

**✓ ALERIE L. BAILEY-RIHN  
CIRCUIT COURT, BR. 3**

STATE OF WISCONSIN

CIRCUIT COURT

DANE COUNTY

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

**FILED**

**NOV 28 2016**

JILL STEIN,  
c/o Emery Celli Brinckerhoff & Abady LLP  
600 Fifth Avenue, 10<sup>th</sup> Floor  
New York, NY 10020,

DANE COUNTY CIRCUIT COURT

Case No.: **16CV3060**

Petitioner,

Case Codes: 30701 (Declaratory Judgment)  
30704 (Other Injunction)

v.

WISCONSIN ELECTIONS COMMISSION,  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707, and

Members of the Wisconsin Elections Commission,  
each and only in his or her official capacity:

MARK L. THOMSEN, ANN S. JACOBS,  
BEVERLY GILL, JULIE M. GLANCEY,  
STEVE KING, and DON M. MILLIS  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707,

Respondents.

---

**SUMMONS**

---

THE STATE OF WISCONSIN, To each person named above as a Respondent:

You are hereby notified that the Petitioner named above has filed a lawsuit or other legal action against you. The Complaint, which is attached, states the nature and basis of the legal action.

Within twenty (20) days of receiving this Summons, you must respond with a written answer, as that term is used in Chapter 802 of the Wisconsin Statutes, to the Complaint. The

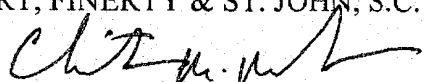
Court may reject or disregard an answer that does not follow the requirements of the statutes. The answer must be sent or delivered to the Court, whose address is Dane County Courthouse 215 South Hamilton Street, Madison, WI 53703-3285, and to Friebert, Finerty & St. John, S.C., Petitioner's attorneys, whose address is 330 East Kilbourn Avenue, Suite 1250, Milwaukee, Wisconsin 53202, ATTN: Christopher M. Meuler, Attorney for Petitioner. You may have an attorney help or represent you.

If you do not provide a proper answer within twenty (20) days, the Court may grant judgment against you for the award of money or other legal action requested in the Complaint, and you may lose your right to object to anything that is or may not be incorrect in the Complaint. A judgment may be enforced as provided by law. A judgment awarding money may become a lien against any real estate you own now or in the future, and may also be enforced by garnishment or seizure of property.

Dated this 28<sup>th</sup> day of November, 2016.

FRIEBERT, FINERTY & ST. JOHN, S.C.

By:

  
Christopher M. Meuler (SBN: 1037971)

EMERY CELLI BRINCKERHOFF & ABADY,  
LLP

By: Matthew D. Brinckerhoff\*  
Debra L. Greenberger\*  
David A. Lebowitz\*

*\*Pro hac vice pending*

Attorneys for Petitioner Jill Stein

P.O. ADDRESS:

330 East Kilbourn Avenue, Suite 1250  
Milwaukee, Wisconsin 53202  
Phone: (414) 271-0130

STATE OF WISCONSIN

CIRCUIT COURT

DANE COUNTY

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

**FILED**

NOV 28 2016

DANE COUNTY CIRCUIT COURT

JILL STEIN  
c/o Emery Celli Brinckerhoff & Abady LLP  
600 Fifth Avenue, 10<sup>th</sup> Floor  
New York, NY 10020

Petitioner,

Case No.:

**16CV3060**

v.

WISCONSIN ELECTIONS COMMISSION  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707, and

Case Codes: 30701 (Declaratory Judgment)  
30704 (Other Injunction)

Members of the Wisconsin Elections Commission,  
each and only in his or her official capacity:

MARK L. THOMSEN, ANN S. JACOBS,  
BEVERLY GILL, JULIE M. GLANCEY,  
STEVE KING, and DON M. MILLIS  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707,

Respondents.

---

**COMPLAINT AND PETITION  
FOR AN ORDER PURSUANT TO WISCONSIN STATUTES §§ 5.90(2) AND 9.01**

---

Jill Stein, by her undersigned attorneys, hereby files this complaint and petition and alleges as follows:

**INTRODUCTION**

Petitioner Jill Stein was a candidate for the office of the President of the United States in an election held on November 8, 2016. On November 25, 2016, Petitioner filed with Respondent

the Wisconsin Elections Commission a verified petition for a recount of all ballots in all wards in the State of Wisconsin pursuant to Wisconsin Statutes § 9.01. Ms. Stein's verified petition requested a hand recount of all ballots, but applicable law affords discretion to the various boards of canvassers throughout the State to recount most ballots cast throughout Wisconsin either by hand or with "automatic tabulating equipment." *See* Wis. Stat. § 5.90(1). However, this court has the power to order a hand recount. Wis. Stat. § 5.90(3). The prospect of a recount performed with "automatic tabulating equipment"—the same equipment Ms. Stein's recount petition explained may have been attacked by foreign government agents seeking to interfere in the presidential race—risks tainting the recount process. Petitioner seeks an order for a hand recount of all optical scan ballots, *i.e.* ballots "distributed to the electors." Wis. Stat. § 5.90(1).

### **PARTIES**

1. Plaintiff Jill Stein was the Green Party nominee for President of the United States in the 2016 election.
2. Respondent Wisconsin Elections Commission ("Elections Commission") is an agency of the State of Wisconsin, which is endowed by statute with the responsibility for the administration of all laws relating to elections and election campaigns. *See* Wis. Stat. § 5.05.
3. Respondents Mark L. Thomsen, Ann S. Jacobs, Beverly Gill, Julie M. Glancey, Steve King, and Don M. Millis, each personally and individually but only in his or her official capacity, are all members of the Wisconsin Elections Commission.

### **JURISDICTION AND VENUE**

4. This Court has jurisdiction over this matter pursuant to Wis. Stat. § 5.90(2)-(3).
5. Venue is proper in this judicial district pursuant to Wis. Stat. § 801.50(5t).

## FACTUAL ALLEGATIONS

### Background

6. On November 25, 2016, Petitioner filed with the Elections Commission a sworn petition for a recount of votes cast in the State of Wisconsin for President of the United States in the 2016 election.

7. The logistics of the recount process depend upon the type of voting equipment used in a particular locality. Of particular relevance here are the two primary electronic voting systems used in Wisconsin: "optical scan" and "direct-recording electronic" ("DRE") voting. An optical scan system uses an electronic scanner to read paper ballots that have been marked by the voters directly and to tabulate the results. DRE machines allow voters to indicate their vote using touchscreens, after which a computer processes their vote records the result in a removable memory component. DRE machines produce a "voter-verified paper audit trail" ("VVPAT") at the time each vote is cast. The VVPAT is a paper record of each vote cast, that is printed out to be inspected and available to be verified by the voter immediately upon casting his or her vote. By contrast, in optical scan voting, a ballot is distributed to each voter, who completes it him- or herself.

8. Under Wisconsin law, where DRE machines are used, "the board of canvassers shall perform the recount using the permanent paper record of the votes cast by each elector, as generated by the machines." Wis. Stat. § 5.90(1). However, "if the ballots are distributed to the electors," as is the case where optical scan voting is used, boards of canvassers have the option of performing the recount "with automatic tabulating equipment," entirely "by hand," or "by hand for only certain wards or election districts." *Id.*

9. Candidates may seek a court order requiring that a recount be done by hand.

Pursuant to Wis. Stat. § 5.90(2):

Any candidate, or any elector when for a referendum, may, by the close of business on the next business day after the last day for filing a petition for a recount under s. 9.01, petition the circuit court for an order requiring ballots under sub. (1) to be counted by hand or by another method approved by the court. The petitioner in such an action bears the burden of establishing by clear and convincing evidence that due to an irregularity, defect, or mistake committed during the voting or canvassing process the results of a recount using automatic tabulating equipment will produce incorrect recount results and 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.

10. Here, where the overall integrity of the election cannot be verified by an automatic recount and popular acceptance of the winner is severely impaired, a hand recount is warranted. The Wisconsin Supreme Court has recognized that courts may relax the standard of outcome-determinativeness generally applied to election irregularities where such irregularities are “so significant in number or so egregious in character as to seriously undermine the appearance of fairness, . . . even when the outcome of the election might not be changed.” *McNally v. Tollander*, 100 Wis. 2d 490, 504, 302 N.W.2d 440 (1981). In post-election proceedings the “primary concern” must be “the protection of the rights and interests of the voters.” *Roth v. Lafarge Sch. Dist. Bd. of Canvassers*, 2004 WI 6, 268 Wis. 2d 335, 349, 677 N.W.2d 599. *See also* Wis. Stat. § 5.01(1) (providing that election laws “shall be construed to give effect to the will of the electors”).

**The Unique Circumstances of the 2016 Presidential Election Require a Hand Recount**

11. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John

Podesta, the chairman of Democratic Party candidate Hillary Clinton's campaign. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. The Department of Homeland Security has stated that senior foreign government officials commissioned these attacks. Attackers attempted to breach election offices in more than 20 other states. *See* Affidavit of J. Alex Halderman ("Halderman Aff."), ¶ 7 & Exs. A, B, C, D, E, F.

12. If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices well in advance to find ways to break into the computers. Next, closer to the election, when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines into some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling. *See* Halderman Aff., ¶ 9.

13. Experts have repeatedly documented in peer-reviewed and state-sponsored research that American voting machines have serious cybersecurity problems. Voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. In just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote. *See* Halderman Aff., ¶ 10. Practically speaking, it is not possible to determine with certainty the absence of malicious

software hiding within what might appear to be many thousands of lines of legitimate software code. *See* Affidavit of Poorvi L. Vora (“Vora Aff.”), ¶ 13.

14. Whether voting machines are connected to the Internet is irrelevant. Sophisticated attackers such as nation-states have developed a variety of techniques for attacking non-Internet-connected systems. Shortly before each election, poll workers copy the ballot design from a regular desktop computer in a government office (or at a company that services the voting machines) and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers infect that computer, they can spread vote-stealing malware to every voting machine in the area. Most voting machines also have reprogrammable software (“firmware”) that can in many cases be manipulated well in advance of the election to introduce vote-sealing malware. Technically sophisticated attackers can accomplish this with ease. Halderman Aff., ¶ 11; *see also* Affidavit of Dan S. Wallach (“Wallach Aff.”), ¶ 7 (“Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems,” and it becomes “entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries’ capabilities”); Affidavit of Ronald L. Rivest (“Rivest Aff.”), ¶ 8 (“We have learned the hard way that almost any computer system can be broken into by a sufficiently determined, skillful, and persistent adversary. There is nothing special about voting systems that magically provides protection against attack.”); Affidavit of Harri Hursti (“Hursti Aff.”), ¶¶ 6-22 (detailing various attack vectors to which optical scan voting systems are vulnerable). AV-OS tabulators—which are among the optical scanners used in Wisconsin—have been proven to be vulnerable to serious



security threats and hacks capable of neutralizing or swapping candidates or reporting results incorrectly. *See Vora Aff.*, ¶ 25 (noting that “one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and without having ever to access the card physically or opening the AV-OS system enclosure”).

15. While the vulnerabilities of American voting machines have been known for some time, states’ responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Wisconsin, continue to use out-of-date machines that are known to be insecure. *Halderman Aff.*, ¶ 12.

16. Procedural safeguards used by Wisconsin and other states to protect their voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack. These inadequate safeguards include tamper evident seals, protective counters, and test decks. Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers. Malware installed on a voting machine can subvert the protective counter by changing its value in the machine’s computer memory. Malware can subvert test decks by refraining from cheating when only a small number of ballots have been scanned (as is the case when a test deck is used), or by only cheating at a specified time of day (electronic voting machines typically have internal clocks). *Halderman Aff.*, ¶ 13.

17. The companies that provide and service election equipment for municipalities are another possible target for attackers. An example of such as a vendor is Command Central Elections, a small business in Minnesota that provides voting machines to approximately 1000 municipalities in Wisconsin. In many municipalities, Command Central is responsible for updating voting machine software and programming ballot designs prior to the election. Such companies provide an attractive target for attackers, since compromising their computer systems

would allow an attack to spread to voting machines over much of the state. An attack on Command Central could affect election in hundreds of jurisdictions statewide by altering the software or election media in malicious ways that could go undetected absent a manual examination of the ballots. Halderman Aff., ¶ 14.

18. A study published by Professor Walter R. Mebane of the University of Michigan finds statistical abnormalities in ward-level vote data from Wisconsin that are consistent with fraud having taken place in the 2016 presidential election. Wards are the smallest aggregation unit at which vote counts are reported in Wisconsin. Mebane, a statistician and political science professor, used election forensics techniques designed to identify electoral fraud. He discovered an “array of anomalies” in the small wards with optical-scan technology which do not occur in the small wards without optical-scan technology. He also discovered some anomalies in specific optical-scan machines in big wards. Mebane concludes that the data published by Wisconsin so far makes it difficult to establish whether or not reported vote counts accurately reflect the intentions of the electors, but that “[a] rigorous audit or a full recount that has humans manually checking the paper ballots can provide convincing evidence about who won the election.” See Affidavit of Philip B. Stark (“Stark Aff.”), ¶ 38 (describing how Mebane’s analysis “raises suspicion about the accuracy of counts in some wards that voted using optical scan voting systems”).

19. Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record

documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks. Halderman Aff., ¶ 15.

20. The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, to count the paper ballots and paper audit trail records, and review the voting equipment, to ensure that the votes cast by actual voters match the results determined by the computers. Halderman Aff., ¶ 17. While Wisconsin law requires reviewing the paper audit trail records from DRE machines, this Petition is necessary to require all counties to count the paper ballots that were initially tabulated by optical scanners.

21. For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, is necessary to reliably detect possible hacking. Using optical scan machines to conduct the recount, even after first evaluating the machines through a test deck, is insufficient to detect potential cyberattacks. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests. Halderman Aff., ¶ 19.

22. If the scanners were attacked by infecting them with malware, such malware might still be active in the machines during the recount. Recounting the ballots using an infected scanner would likely yield the same results as the original count, despite the results being wrong. Halderman Aff., ¶ 20; *see also* Wallach Aff., ¶ 14 (“A purely electronic tally of paper ballots, without some sort of hand-counting or auditing would be unable to detect systematic electronic tampering—the very risk we’re concerned about in this election.”); Stark Aff., ¶ 24 (“Rescanning and retabulating without checking the electronic data against the original paper records cannot confirm that the reported result is correct.”); Hursti Aff., ¶ 4 (“Optical scan machines can be

hacked in a manner that changes election results, and such an attack would likely go undetected during normal pre- and post-election testing. If the scanners are hacked, using them as part of the recount process is likely to result in the same fraudulent election outcome.”).

23. If attackers managed to compromise the count during election day but in a manner that did not persist on the machines, machine recounts would still be insufficient. Attackers who were able to infect the machines before the election likely would be able to attack them again, perhaps using the same methods, prior to the recount. This would result in the scanners producing the same incorrect results when the ballots were scanned again. Halderman Aff., ¶ 21.

24. In contrast to machine recounts, a manual recount, where the paper ballots are inspected by humans, can reliably detect any cyberattack that might have altered the election outcome on the optical scanners. Halderman Aff., ¶ 22.

25. To accurately verify the outcome of software-based voting systems requires a software-independent system, *i.e.*, a system that has a means of verifying the election outcome independent of the software that computed it. *See* Vora Aff., ¶ 14. Securely-stored paper records must be examined to ensure that they are consistent with the election outcomes declared by the voting system software. If they are not examined, any unintentional software bugs, intentional alterations to the vote or to the tally, or procedural errors leading to an incorrect election outcome will not be detected. *Id.*, ¶ 17.

26. A manual recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference. It will also set a precedent that may provide an important deterrent against cyberattacks on future elections. Halderman Aff., ¶ 22; *see also* Wallach Aff. ¶ 7 (“The mere *possibility* of a recount or audit of the paper ballots acts as a deterrent to an electronic attack; it’s much more difficult to tamper

with paper, in bulk, relative to the effort to tamper with purely electronic records as used in many states (but not Wisconsin).”); Rivest Aff. ¶ 36 (“It is important to emphasize that an audit or a recount really *must* look at the paper ballots. Otherwise one is not examining the primary election data (the cast ballots themselves) but only derivative secondary data that may have been corrupted by faulty or malicious software.”)).

27. Indeed, according to a recent Washington Post-ABC News Poll, 18% of Americans surveyed—and 33% of supporters of Democratic Party candidate Hillary Clinton—do not accept Republican candidate Donald Trump’s election as legitimate. Scott Clement, *One-third of Clinton supporters say Trump election is not legitimate, poll finds*, WashingtonPost.com (Nov. 13, 2016).<sup>1</sup> A hand recount is needed to shore up public confidence in the outcome of the election. See Rivest Aff. ¶ 20 (“For our democracy to work well, election systems should produce the best and most convincing evidence that announced election outcomes are correct. One should ask: what will it take to convince a skeptical supporter of a losing candidate that they really lost? Evidence of the form, ‘You must trust the computer here.’ is not likely to be adequate (nor should it be).”).

**A Hand Recount Is Feasible and No More Burdensome than Electronic Retabulation**

28. It is important to note that hand recounts—even for statewide races—are common and practicable.

29. For example, in 2011, Wisconsin conducted a statewide recount of votes cast in the Wisconsin Supreme Court election. According to the Elections Commission, in the initial counting of votes after the election, “90 percent of the ballots were cast on paper and counted by optical scanners, 5 percent were cast on paper and counted by hand, and 5 percent were cast and

---

<sup>1</sup> Available at <https://www.washingtonpost.com/news/the-fix/wp/2016/11/13/one-third-of-clinton-supporters-say-trump-election-is-not-legitimate-poll-finds/>.

tabulated on touch-screen equipment.” See <http://elections.wi.gov/elections-voting/recount/ballot-authenticity>. However, in the recount, “of the 90 percent that were originally counted by voting equipment on Election Night, more than half” were “recounted by hand.” *Id.* As the Elections Commission acknowledged then, hand recounting resulted “in some ballots being counted that the voting equipment may not have attributed a vote due to ballot irregularity, such as the voter circling the candidate name instead of filling in the oval or arrow.” This finding is consistent with expert research on optical scanning, which consistently finds that optical scanners misinterpret votes for various reasons. See, e.g., Vora Aff., ¶ 22; Wallach Aff., ¶¶ 17-21; Stark Aff., ¶¶ 27-32; see generally Affidavit of Douglas W. Jones. Hand counting is therefore also most consonant with Wisconsin’s policy of giving effect to the intent of the voter. See *Roth*, 268 Wis.2d at 329 (“ballots are the best evidence of the intention of voters”).

30. The Elections Commission has itself acknowledged that a hand recount is not necessarily more time-consuming than an electronic retabulation. In a November 25, 2016 message to all of the County Clerks in Wisconsin, Elections Supervisor Ross Hein stated: “In discussions with Wisconsin election officials over the years, a hand-count may not be as timing [sic] consuming as one may think and avoids pre-testing of the equipment and reprogramming of memory devices.” See <http://elections.wi.gov/node/4439>.

31. This statement is consistent with practical experience in other jurisdictions such as Minnesota, where, according to published sources, a hand recount of all of the more than two million votes cast in the 2010 statewide race for Governor was completed in approximately five days.

32. In short, manual recounts are not necessarily more time-consuming than recounting using optical scanners. A manual recount focuses on a single contest, and human

observers typically proceed by sorting the ballots into stacks according to the chosen candidate and then counting the ballots in each stack. This is an efficient and straightforward process. If scanners are used, the scanners must be programmed and tested, and the ballots must be fed into the scanner by humans. These steps are not necessary when hand counting is used. Halderman Aff., ¶ 23.

33. The paper ballots used in Wisconsin can be counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether the voter intended to make a mark. Wisconsin's optically scanned paper ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted efficiently and accurately in a manual recount. *Id.*, ¶ 24.

34. Any contemplated efficiency benefit to an electronic retabulation is especially illusory because, in any locality that proceeds to use optical scanning machines to perform a recount, Petitioner plans to exercise her right to inspect each ballot before it is inserted into the tabulator. See Wisconsin Elections Commission, *Election Recount Procedures*<sup>2</sup> at 12 (Nov. 2016) ("Each ballot . . . may be inspected by the candidates or their representatives before being inserted into the tabulator."); Wis. Stat. § 9.01(b)(11) ("All steps of the recount shall be performed publicly . . . . [A]ll materials and ballots may be viewed and identified by the candidates . . ."). Accordingly, an electronic retabulation will be no faster or more efficient than a hand recount.

---

<sup>2</sup> Available at [http://elections.wi.gov/sites/default/files/publication/65/recount\\_manual\\_11\\_2016.pdf](http://elections.wi.gov/sites/default/files/publication/65/recount_manual_11_2016.pdf) 17034.pdf.

35. Furthermore, Petitioner has paid or will pay all fees associated with the statewide recount. *See* Wis. Stat. § 9.01(1)(ag)(3). The public fisc will therefore be unaffected by any order to conduct a hand recount.

**COUNT 1**

**PETITION**

**FOR AN ORDER PURSUANT TO WISCONSIN STATUTES §§ 5.90(2) AND 9.01**

36. Petitioner repeats and realleges the foregoing paragraphs as if set forth fully herein.

37. Due to an irregularity, defect, or mistake committed during the voting or canvassing process, the results of any recount using automatic tabulating equipment will produce incorrect recount results.

38. There is a substantial probability that recounting the ballots by hand will produce a more correct result and change the outcome of the election.

**WHEREFORE**, Petitioner respectfully requests judgment as follows:

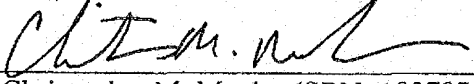
- A. An order to recount all ballots in all wards in the State of Wisconsin by hand.
- B. Such other and further relief as the court may deem just and equitable.



Dated this 28<sup>th</sup> day of November, 2016.

FRIEBERT, FINERTY & ST. JOHN, S.C.

By:

  
Christopher M. Meuler (SBN: 1037971)

EMERY CELLI BRINCKERHOFF & ABADY,  
LLP

By: Matthew D. Brinckerhoff\*  
Debra L. Greenberger\*  
David A. Lebowitz\*

*\*Pro hac vice admission pending*

Attorneys for Petitioner Jill Stein

P.O. ADDRESS:

330 East Kilbourn Avenue, Suite 1250  
Milwaukee, Wisconsin 53202  
Phone: (414) 271-0130



**FRIEBERT, FINERTY & ST. JOHN, S.C.**

ATTORNEYS AT LAW

330 East Kilbourn Ave. • Suite 1250 • Milwaukee, Wisconsin 53202  
Phone 414-271-0130 • Fax 414-272-8191 • www.ffsj.com

WILLIAM B. GUIS

S. TODD FARRIS

TED A. WARPINSKI

LAWRENCE J. GLUSMAN

BRIAN C. RANDALL

CHRISTOPHER M. MEULER

M. ANDREW SKWIERAWSKI

November 28, 2016

**RECEIVED**

**NOV 28 2016**

**VIA MESSENGER**

Clerk of Circuit Court

Dane County Courthouse

215 South Hamilton Street, Room 1000

Madison, WI 53703

**DANE COUNTY CIRCUIT COURT**

ROBERT H. FRIEBERT  
(1938-2013)

EMERITUS  
JOHN D. FINERTY

OF COUNSEL  
THOMAS W. ST. JOHN

Re: *Jill Stein v. Wisconsin Election Commission*

Dear Madam/Sir:

With respect to the above-referenced matter, enclosed for filing, please find the originals and one (1) copy of each of the following documents:

1. Summons with Complaint and Petition for an Order Pursuant to Wisconsin Statutes § 5.90(2);
2. Check in the amount of \$265.50 representing the filing fee;
3. Affidavit of Dan S. Wallach (the original signature page to be filed with the Court upon receipt by this office);
4. Affidavit of Harri Hursti (the original signature page to be filed with the Court upon receipt by this office);
5. Affidavit of Ronald L. Rivest (the original signature page to be filed with the Court upon receipt by this office);
6. Affidavit of J. Alex Halderman (the original signature page to be filed with the Court upon receipt by this office);
7. Affidavit of Poorvi L. Vora (the original to be filed with the Court upon receipt by this office); and
8. Affidavit of Philip B. Stark (the original signature page to be filed with the Court upon receipt by this office).

Also enclosed for filing are the following:

1. Motion to Admit Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz *Pro Hac Vice* (copies of the Applications, letter to the Office of Lawyer Regulation and copies of the checks

Clerk of Circuit Court – Dane County  
November 28, 2016  
Page 2

for the application fees of Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz for admission *Pro Hac Vice* attached);

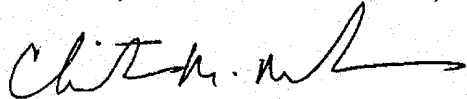
2. Affidavit of Christopher M. Meuler;
3. Affidavit of Matthew D. Brinckerhoff;
4. Affidavit of Debra L. Greenberger;
5. Affidavit of David Lebowitz; and
6. (Proposed) Order Admitting Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz *Pro Hac Vice*.

If the proposed Order meets with the Court's approval, please have the assigned judge sign and return a conformed copy to us in the self-addressed stamped envelope which is enclosed.

Thank you for your attention to this communication.

Very truly yours,

FRIEBERT, FINERTY & ST. JOHN, S.C.



Christopher M. Meuler  
cmm@ffsj.com

CMM/sjf  
Enclosures

cc: Daniel Lennington, Esq. (w/Encs.) – Via Email  
Matthew D. Brinckerhoff, Esq. (w/Encs.) – Via Email

STATE OF WISCONSIN

CIRCUIT COURT

DANE COUNTY

JILL STEIN,

**FILED**

**16CV3060**

Petitioner,

NOV 28 2016

Case No. \_\_\_\_\_

DANE COUNTY CIRCUIT COURT

v

WISCONSIN ELECTIONS COMMISSION,

Respondent.

---

**MOTION TO ADMIT MATTHEW D. BRINCKERHOFF, DEBRA L. GREENBERGER  
AND DAVID LEBOWITZ *PRO HAC VICE***

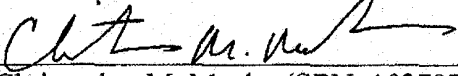
---

TO: Daniel Lennington, Esq.  
Wisconsin Attorney General's Office  
c/o Wisconsin Department of Justice  
17 West Main Street  
PO Box 7857  
Madison, WI 53703-7857

**PLEASE TAKE NOTICE** that Petitioner, Jill Stein, by her counsel, Friebert, Finerty & St. John, S.C., hereby moves the Court for an Order permitting Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz, non-resident attorneys with Emery Celli Brinckerhoff & Abady, LLP, to appear and participate in this action as counsel for the Petitioner based on the grounds set forth in the accompanying Applications for *Pro Hac Vice* of Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz. Pursuant to Supreme Court Rules, attached as proof of payment of the Application fees are copies of a letter and checks to the Office of Lawyer Regulation.

Dated this 28<sup>th</sup> day of November, 2016.

FRIEBERT, FINERTY & ST. JOHN, S.C.  
Attorneys for Petitioner, Jill Stein

  
\_\_\_\_\_  
Christopher M. Meuler (SBN: 1037971)

330 East Kilbourn Avenue – Suite 1250  
Milwaukee, Wisconsin 53202  
Telephone: (414) 271-0130  
[cmm@ffsj.com](mailto:cmm@ffsj.com)



**FRIEBERT, FINERTY & ST. JOHN, S.C.**

ATTORNEYS AT LAW

330 East Kilbourn Ave. • Suite 1250 • Milwaukee, Wisconsin 53202

Phone 414-271-0130 • Fax 414-272-8191 • www.ffsj.com

WILLIAM B. GUIB

S. TODD FARRIS

TED A. WARPINSKI

LAWRENCE J. GLUSMAN

BRIAN C. RANDALL

CHRISTOPHER M. MEULER

M. ANDREW SKWIERAWSKI

November 28, 2016

**VIA MESSENGER**

Office of Lawyer Regulation

110 East Main Street, Suite 315

Madison, WI 53703-3383

**ATTN:** *Pro Hac Vice* Application

RE: *Pro Hac Vice* Applications for Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz

To Whom It May Concern:

Enclosed please find Applications for *Pro Hac Vice* for Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz, along with 3 checks to cover the application fees as follows:

1 check for \$300.00 payable to the Office of Lawyer Regulation

1 check for \$300.00 payable to the Wisconsin Trust Account Foundation, Inc.

1 check for \$150.00 payable to the Wisconsin Access to Justice Commission

Please contact me if you have any concerns.

Very truly yours,

FRIEBERT, FINERTY & ST. JOHN, S.C.

Christopher M. Meuler

cmm@ffsj.com

CMM/sjf

Enclosures

ROBERT H. FRIEBERT  
(1938-2013)

EMERITUS  
JOHN D. FINERTY

OF COUNSEL  
THOMAS W. ST. JOHN

43401

FF&amp;SJ

FRIEBERT, FINERTY & ST. JOHN, S.C.  
ATTORNEYS AT LAW  
330 EAST KILBOURN AVENUE, SUITE 1250  
MILWAUKEE, WI 53202

**PARK BANK**  
DOWNTOWN • CAPITOL DRIVE • BROOKFIELD  
MILWAUKEE, WISCONSIN 53216

EZSolve™ Check Fraud  
Protection for Business

12-66-750

DATE

11/28/16

CHECK

43401

AMOUNT

\*\*\*\*\$300.00

PAY

TO THE  
ORDER  
OF

Office of Lawyer Regulation

\*\*\* THREE HUNDRED &amp; 00/100 DOLLARS

FRIEBERT, FINERTY &amp; ST. JOHN, S.C.

*Will B. Gu*

AUTHORIZED SIGNATURE

⑈043401⑈ ⑆075000666⑆ ⑈61026 9968⑈

Security features. Details on back.



43398

FF&amp;SJ

FRIEBERT, FINERTY & ST. JOHN, S.C.  
ATTORNEYS AT LAW  
330 EAST KILBOURN AVENUE, SUITE 1250  
MILWAUKEE, WI 53202

**PARK BANK**  
DOWNTOWN • CAPITOL DRIVE • BROOKFIELD  
MILWAUKEE, WISCONSIN 53216

EZSolve™ Check Fraud  
Protection for Business

12-66-750

DATE

11/28/16

CHECK

43398

AMOUNT

\*\*\*\*\$300.00

PAY

TO THE  
ORDER  
OF

Wisconsin Trust Account Foundation

\*\*\* THREE HUNDRED &amp; 00/100 DOLLARS

FRIEBERT, FINERTY &amp; ST. JOHN, S.C.

*Will B. Gu*

AUTHORIZED SIGNATURE

⑈043398⑈ ⑆075000666⑆ ⑈61026 9968⑈

Security features. Details on back.



43397

FF&amp;SJ

FRIEBERT, FINERTY & ST. JOHN, S.C.  
ATTORNEYS AT LAW  
330 EAST KILBOURN AVENUE, SUITE 1250  
MILWAUKEE, WI 53202

**PARK BANK**  
DOWNTOWN • CAPITOL DRIVE • BROOKFIELD  
MILWAUKEE, WISCONSIN 53216

EZSolve™ Check Fraud  
Protection for Business

12-66-750

DATE

11/28/16

CHECK

43397

AMOUNT

\*\*\*\*\$150.00

PAY

TO THE  
ORDER  
OF

Wisconsin Access to Justice Commission

\*\*\* ONE HUNDRED FIFTY &amp; 00/100 DOLLARS

FRIEBERT, FINERTY &amp; ST. JOHN, S.C.

*Will B. Gu*

AUTHORIZED SIGNATURE

⑈043397⑈ ⑆075000666⑆ ⑈61026 9968⑈

Security features. Details on back.



STATE OF WISCONSIN, CIRCUIT COURT, DANE COUNTY

For Official Use

Case Caption: JILL STEIN v. WISCONSIN  
ELECTIONS COMMISSION, et al.  
ADMISSION MATTHEW D. BRINCKERHOFF

**Application for  
Pro Hac Vice**


Case No. \_\_\_\_\_

**I DECLARE UNDER PENALTY OF PERJURY:**

1. That I seek to appear pro hac vice in order to represent Petitioner, Jill Stein in the above-captioned matter;
2. That I am admitted to practice law in the highest court(s) of the state(s) or country(ies) of New York;
3. That there are no disciplinary complaints filed against me for violation of the rules of those courts (if so, please explain): \_\_\_\_\_;
4. That I am not suspended or disbarred from practice for disciplinary reasons or reason of medical incapacity in any jurisdiction (if yes, please explain): \_\_\_\_\_;
5. That I am associated with Attorney Christopher M. Meuler, State Bar No. 1037971, an active member of the State Bar of Wisconsin (name the member of the State Bar of Wisconsin and provide his/her Member Number);
6. That I do not practice or hold out to practice law in the State of Wisconsin;
7. That I acknowledge the jurisdiction of the courts of the State of Wisconsin over my professional conduct, and I agree to abide by the rules of the relevant division of the Circuit Court of the State of Wisconsin, the Wisconsin Court of Appeals, the Wisconsin Supreme Court, and the Rules of Professional Conduct for Attorneys, if I am admitted pro hac vice;
8. That I have complied fully with SCR Rule 10.03 (4);
9. That I am applying for admission pro hac vice for the following reasons:  
to appear on behalf of Petitioner, Jill Stein, in the above-captioned matter.

I have applied for admission pro hac vice in the courts of the State of Wisconsin zero times previously in this calendar year.

I attach hereto evidence of my payment or prior payment of the pro hac vice fee to the Office of Lawyer Regulation.

|   |                                    |
|---|------------------------------------|
| Signature of Attorney<br> | Telephone Number<br>(212) 763-5000 |
| Name Printed<br>Matthew D. Brinckerhoff   |                                    |
| Address of Principal Office<br>600 Fifth Avenue, 10 <sup>th</sup> Floor<br>New York, New York 10020           |                                    |



STATE OF WISCONSIN, CIRCUIT COURT, DANE COUNTY

For Official Use

Case Caption: JILL STEIN v. WISCONSIN  
ELECTIONS COMMISSION, et al.  
ADMISSION DEBRA L. GREENBERGER

**Application for  
Pro Hac Vice**

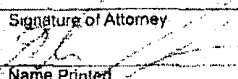
Case No. \_\_\_\_\_

**I DECLARE UNDER PENALTY OF PERJURY:**

1. That I seek to appear pro hac vice in order to represent Petitioner, Jill Stein in the above-captioned matter;
2. That I am admitted to practice law in the highest court(s) of the state(s) or country(ies) of New York;
3. That there are no disciplinary complaints filed against me for violation of the rules of those courts (if so, please explain): \_\_\_\_\_;
4. That I am not suspended or disbarred from practice for disciplinary reasons or reason of medical incapacity in any jurisdiction (if yes, please explain): \_\_\_\_\_;
5. That I am associated with Attorney Christopher M. Meuler, State Bar No. 1037971, an active member of the State Bar of Wisconsin (name the member of the State Bar of Wisconsin and provide his/her Member Number);
6. That I do not practice or hold out to practice law in the State of Wisconsin;
7. That I acknowledge the jurisdiction of the courts of the State of Wisconsin over my professional conduct, and I agree to abide by the rules of the relevant division of the Circuit Court of the State of Wisconsin, the Wisconsin Court of Appeals, the Wisconsin Supreme Court, and the Rules of Professional Conduct for Attorneys, if I am admitted pro hac vice;
8. That I have complied fully with SCR Rule 10.03 (4);
9. That I am applying for admission pro hac vice for the following reasons:  
to appear on behalf of Petitioner, Jill Stein, in the above-captioned matter.  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I have applied for admission pro hac vice in the courts of the State of Wisconsin zero times previously in this calendar year.

I attach hereto evidence of my payment or prior payment of the pro hac vice fee to the Office of Lawyer Regulation.

|  |                                    |
|--|------------------------------------|
| Signature of Attorney<br> | Telephone Number<br>(212) 763-5000 |
| Name Printed<br>Debra L. Greenberger   |                                    |
| Address of Principal Office<br>600 Fifth Avenue, 10 <sup>th</sup> Floor<br>New York, New York 10020          |                                    |

STATE OF WISCONSIN, CIRCUIT COURT, DANE COUNTY

For Official Use

Case Caption: JILL STEIN v. WISCONSIN  
ELECTIONS COMMISSION, et al.  
ADMISSION DAVID LEBOWITZ

**Application for  
Pro Hac Vice**

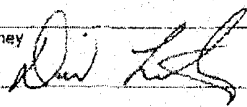
Case No. \_\_\_\_\_

**I DECLARE UNDER PENALTY OF PERJURY:**

1. That I seek to appear pro hac vice in order to represent Petitioner, Jill Stein in the above-captioned matter;
2. That I am admitted to practice law in the highest court(s) of the state(s) or country(ies) of New York;
3. That there are no disciplinary complaints filed against me for violation of the rules of those courts (if so, please explain): \_\_\_\_\_;
4. That I am not suspended or disbarred from practice for disciplinary reasons or reason of medical incapacity in any jurisdiction (if yes, please explain): \_\_\_\_\_;
5. That I am associated with Attorney Christopher M. Meuler, State Bar No. 1037971, an active member of the State Bar of Wisconsin (name the member of the State Bar of Wisconsin and provide his/her Member Number);
6. That I do not practice or hold out to practice law in the State of Wisconsin;
7. That I acknowledge the jurisdiction of the courts of the State of Wisconsin over my professional conduct, and I agree to abide by the rules of the relevant division of the Circuit Court of the State of Wisconsin, the Wisconsin Court of Appeals, the Wisconsin Supreme Court, and the Rules of Professional Conduct for Attorneys, if I am admitted pro hac vice;
8. That I have complied fully with SCR Rule 10.03 (4);
9. That I am applying for admission pro hac vice for the following reasons:  
to appear on behalf of Petitioner, Jill Stein, in the above-captioned matter.  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I have applied for admission pro hac vice in the courts of the State of Wisconsin zero times previously in this calendar year.

I attach hereto evidence of my payment or prior payment of the pro hac vice fee to the Office of Lawyer Regulation.

|   |                                    |
|---|------------------------------------|
| Signature of Attorney<br> | Telephone Number<br>(212) 763-5000 |
| Name Printed<br>David Lebowitz  |                                    |
| Address of Principal Office<br>600 Fifth Avenue, 10 <sup>th</sup> Floor<br>New York, New York 10020           |                                    |

NOV 28 2016

DANE COUNTY CIRCUIT COURT

DANE COUNTY

**16CV3060**

Case No. \_\_\_\_\_

V.

### Respondents.

**AFFIDAVIT OF DAVID LEBOWITZ**

STATE OF NEW YORK )  
 ) SS.  
NEW YORK COUNTY )

DAVID LEBOWITZ, being first duly sworn on oath, deposes and states as follows:

1. Pursuant to Wisconsin Supreme Court Rules, Chapter 10.03(4), I hereby request leave of the Court to appear in the above-entitled action *pro hac vice* as counsel for Petitioner, Jill Stein.

2. Petitioner has retained Emery Celli Brinckerhoff & Abady, LLP to represent her in this matter. I am an associate in Emery Celli Brinckerhoff & Abady, LLP working in its offices located at 600 Fifth Avenue, 10<sup>th</sup> Floor, New York, New York 10020.

3. I have been admitted to practice law in the State of New York. I am also a member in good standing of the United States District Courts for the Southern and Eastern Districts of New York and the United States Court of Appeals for the Second Circuit. I am a

member in good standing of each court, and no disciplinary or grievance proceeding has ever been filed against me.

4. I have never been denied admission to any state or federal court to which I have applied.

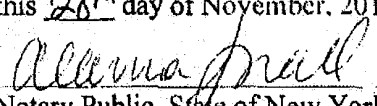
5. I request that I be admitted *pro hac vice* to appear on behalf of Petitioner in the above-captioned case.

6. I will abide by the Dane County Circuit Court rules.

7. I make this request in connection with local counsel for Petitioner, Friebert, Finerty & St. John, S.C., located at 330 East Kilbourn Avenue, Suite 1250, Milwaukee, Wisconsin 53202.

  
David Lebowitz

Subscribed and sworn to before me  
this 28<sup>th</sup> day of November, 2016.

  
Notary Public, State of New York  
My Commission: \_\_\_\_\_

ALANNA SMALL  
NOTARY PUBLIC-STATE OF NEW YORK  
No. 02SM8340924  
Qualified in New York County  
My Commission Expires 04-26-2020

STATE OF WISCONSIN

CIRCUIT COURT

DANE COUNTY

JILL STEIN,

Petitioner,

Y.

WISCONSIN ELECTIONS COMMISSION,  
et al.,

### Respondents.

Case No. **16CV3060**

**FILED**

NOV 28 2016

DANE COUNTY CIRCUIT COURT

# AFFIDAVIT OF DEBRA L. GREENBERGER

STATE OF NEW YORK )  
 ) SS.  
NEW YORK COUNTY )

DEBRA L. GREENBERGER, being first duly sworn on oath, deposes and states as follows:

1. Pursuant to Wisconsin Supreme Court Rules, Chapter 10.03(4), I hereby request leave of the Court to appear in the above-entitled action *pro hac vice* as counsel for Petitioner, Jill Stein.

2. Petitioner has retained Emery Celli Brinckerhoff & Abady, LLP to represent her in this matter. I am a partner in Emery Celli Brinckerhoff & Abady, LLP working in its offices located at 600 Fifth Avenue, 10<sup>th</sup> Floor, New York, New York 10020.

3. I have been admitted to practice law in the State of New York. I am also a member in good standing of the United States District Courts for the Southern and Eastern Districts of New York, the United States Court of Appeals, Second Circuit, and the United States

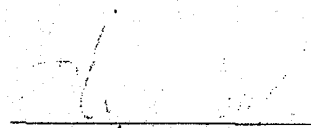
Supreme Court. I am a member in good standing of each court, and no disciplinary or grievance proceeding has ever been filed against me.

4. I have never been denied admission to any state or federal court to which I have applied.

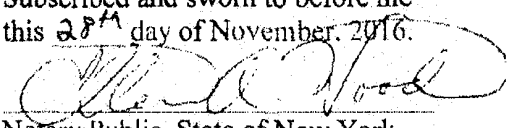
5. I request that I be admitted *pro hac vice* to appear on behalf of Petitioner in the above-captioned case.

6. I will abide by the Dane County Circuit Court rules.

7. I make this request in connection with local counsel for Petitioner, Friebert, Finerty & St. John, S.C., located at 330 East Kilbourn Avenue, Suite 1250, Milwaukee, Wisconsin 53202.

  
Debra L. Greenberger

Subscribed and sworn to before me  
this 28<sup>th</sup> day of November, 2016.

  
Notary Public, State of New York  
My Commission: No. 01WO6251860

ELLEN A. WOOD  
NOTARY PUBLIC-STATE OF NEW YORK  
No. 01WO6251860  
Qualified in Kings County  
My Commission Expires November 21, 2019

NOV 28 2016

**16CV3060**

Case No. \_\_\_\_\_

Respondents.

**AFFIDAVIT OF MATTHEW D. BRINCKERHOFF**

STATE OF NEW YORK )  
 ) SS.  
NEW YORK COUNTY )

MATTHEW D. BRINCKERHOFF, being first duly sworn on oath, deposes and states as follows:

1. Pursuant to Wisconsin Supreme Court Rules, Chapter 10.03(4), I hereby request leave of the Court to appear in the above-entitled action *pro hac vice* as counsel for Petitioner, Jill Stein.
2. Petitioner has retained Emery Celli Brinckerhoff & Abady, LLP to represent her in this matter. I am a partner in Emery Celli Brinckerhoff & Abady, LLP working in its offices located at 600 Fifth Avenue, 10<sup>th</sup> Floor, New York, New York 10020.
3. I have been admitted to practice law in the State of New York. I am also a member in good standing of the United States District Courts for the Southern and Eastern Districts of New York, the United States Court of Appeals, Second, Third and Ninth Circuits,

and the United States Supreme Court. I am a member in good standing of each court, and no disciplinary or grievance proceeding has ever been filed against me.

4. I have never been denied admission to any state or federal court to which I have applied.

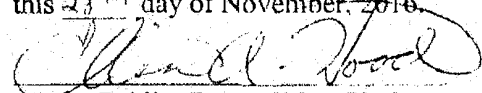
5. I request that I be admitted *pro hac vice* to appear on behalf of Petitioner in the above-captioned case.

6. I will abide by the Dane County Circuit Court rules.

7. I make this request in connection with local counsel for Petitioner, Friebert, Finerty & St. John, S.C., located at 330 East Kilbourn Avenue, Suite 1250, Milwaukee, Wisconsin 53202.

  
Matthew D. Brinckerhoff

Subscribed and sworn to before me  
this 28<sup>th</sup> day of November, 2016.

  
Notary Public, State of New York  
My Commission: No. 01WO6251860

**ELLEN A. WOOD**  
**NOTARY PUBLIC-STATE OF NEW YORK**  
**No. 01WO6251860**  
**Qualified in Kings County**  
**My Commission Expires November 21, 2019**



STATE OF WISCONSIN

CIRCUIT COURT

DANE COUNTY

JILL STEIN,

Petitioner,

v

WISCONSIN ELECTIONS COMMISSION,

Respondent.

**FILED**

NOV 28 2016

DANE COUNTY CIRCUIT COURT

**16CV3060**

Case No. \_\_\_\_\_

**AFFIDAVIT OF CHRISTOPHER M. MEULER**

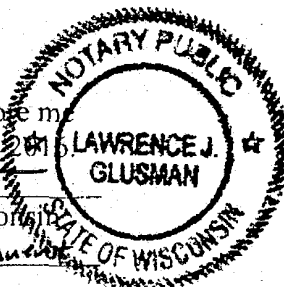
STATE OF WISCONSIN     )  
  ) SS.  
MILWAUKEE COUNTY     )

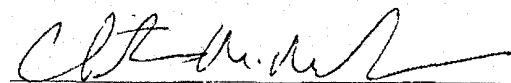
CHRISTOPHER M. MEULER, being first duly sworn on oath, deposes and states as follows:

1. I am one of the attorneys representing the Petitioner, Jill Stein, in the above-captioned matter.
2. I am an attorney in the law firm of Friebert, Finerty & St. John, S.C. and am a member in good standing of the State Bar of Wisconsin.
3. I believe that Matthew D. Brinckerhoff, Debra L. Greenberger and David Lebowitz of Emery Celli Brinckerhoff & Abady, LLP are competent to represent Petitioner in a Wisconsin court and that they are willing to abide by the Rules of Professional Conduct for Attorneys and the Rules of Decorum of the Court.

Subscribed and sworn to before me  
this 25<sup>th</sup> day of November, 2016.

Notary Public, State of Wisconsin  
My Commission: is permanent



  
Christopher M. Meuler

FILED

NOV 28 2016

DANE COUNTY CIRCUIT COURT

**AFFIDAVIT OF POORVI L. VORA**

POORVI L. VORA, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is Poorvi L. Vora. I am a Professor of Computer Science at The George Washington University (GW) in Washington, DC. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Wisconsin.
2. I have Ph. D. and Master's degrees in Electrical Engineering from North Carolina State University, Raleigh, NC, a Master's degree in Mathematics from Cornell University and a Bachelor's degree in Electrical and Electronics Engineering from the Indian Institute of Technology, Bombay, India. My CV is attached as Exhibit A.
3. My research in the last dozen or so years has focused on computer security and privacy, with a special focus on secure electronic voting systems.
4. I have published peer-reviewed research on the design of secure end-to-end-verifiable (E2E-V) voting systems which are software-independent voting systems that enable voters and observers to perform especially powerful election audits. I have also helped the National Institute of Standards and Technology develop definitions of E2E-V system properties.
5. With my students and collaborators, I contributed to the design and deployment of an E2E-V voting system called Scantegrity in the municipal elections of the City of Takoma Park in 2009 and 2011. 2009 marked the first time an E2E-V system was used in a government election. We also designed accessible and absentee voting variants of Scantegrity, which were used by Takoma Park in 2011.

6. I was an invited contributor to the Open Vote Foundation study: "The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study" which concluded that secure internet voting is not possible at this time.
7. I have recently been providing public comment in person at meetings of the State Board of Elections in Maryland to urge Maryland to carry out an election audit using its voter-verified paper ballots.
8. I have been on program committees of several conferences and review panels for National Science Foundation research awards. I have been an Associate Editor for the IEEE Transactions on Information Forensics and Security, and Guest Editor, special issue on electronic voting, IEEE Transactions on Information Forensics and Security, December 2009.
9. I regularly teach a course on Cryptography (mathematical techniques that enhance computer security and are used in the design of secure voting systems and secure electronic commerce) for undergraduate and graduate students. I also often teach a more general course on Computer Security, and a course on Advanced Cryptography.
10. It is, of course, important for a voting system to produce the correct tallies. The system should also be designed to enable voters and observers to verify that it produced the correct tallies once the election is over.
11. When votes are cast on paper ballots which are hand counted, the verification is performed through public observation of the counting process. When counts are computed using inherently unobservable software-based systems, the verification of the tallies has not always been possible.

12. Software-based voting systems are very complex and may consist of hundreds of thousands of lines of code<sup>1</sup>.
13. It is hence not possible to find all bugs in voting system software; nor is it possible to completely characterize its behavior in all possible scenarios. For the same reasons, it is not possible to determine with certainty the absence of malicious software hiding within what might appear to be many thousands of lines of legitimate software code. Additionally, it is not possible to confirm with certainty that the code running on the machines is the code that was examined.
14. One approach to dealing with this fundamental challenge of verifying the outcome of software-based voting systems is the notion of software-independence,<sup>2,3</sup> as described by Rivest and Wack. A software-independent voting system is one in which an undetected change in the voting system software will not cause an undetected change in election outcome. Note that a software-independent system is not one that does not use software. It is a system that has a means of verifying the election outcome, independent of the software that computed it (because that software could have bugs and malicious code that have not been detected).
15. One way of achieving software-independence is through the use of voter-verified paper records (VVPRs) securely stored and used to audit the election after it is completed.

---

<sup>1</sup> For example, the Everest study, ("EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing", Final report, December 2007, <http://www.patrickmcdaniel.org/pubs/everest.pdf>) states that the team was provided with "670,000 lines of code, encompassing twelve programming languages and five hardware platforms" for its study of the ES&S system, which includes a version of the Model 100 scanner used in some Wisconsin jurisdictions this year.

<sup>2</sup> Ronald L. Rivest and John P. Wack. "On the notion of 'software independence' in voting systems." Prepared for the TGDC, and posted by NIST at the given url. (2006-07-28) <https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf>

<sup>3</sup> Ronald L. Rivest. "On the notion of 'software independence' in voting systems." *Philosophical Transactions of The Royal Society A* 366,1881 (2008) pp. 3759--3767.

VVPRs may consist of (a) printouts from Direct-Recording Electronic (DRE) machines, verifiable by voters as correctly representing their votes or (b) paper ballots completed by voters and fed into optical scanners that tabulate the votes.

16. As a general principle, both optical scanners and DREs are computers running software and hence vulnerable to the same problems—bugs, malware, intentional alterations, etc.—as all software.<sup>4</sup>
17. Hence the mere act of recording a vote on paper is not sufficient for software independence. The securely-stored paper records need to be examined to ensure that they are consistent with the election outcomes declared by the voting system software. If they are not examined, any unintentional software bugs, intentional alterations to the vote or to the tally, or procedural errors leading to an incorrect election outcome will not be detected.
18. A voter using a DRE enters her vote with guidance from the user interface. The DRE prints out a record of her choices. If she approves it, her vote is cast on the DRE, and the paper record is stored securely. Assuming the voter examined the system's representation of her vote carefully before approving it, the voter knows the system understood her vote for what it was intended to be.
19. A voter using an optical scanner marks a paper ballot and feeds it into the scanner. She does not know if it has read her votes correctly.

---

<sup>4</sup> From the Everest study: "... although they do not appear the same as your typical desktop or laptop computer, all the components of the ES&S system are fully programmable computers capable of running arbitrary software stored in easily modifiable memory. Therefore use of the term "firmware" to refer to the software controlling the hardware components of the ES&S system is somewhat misleading. The code running on the iVotronic [DRE] or Model 100 [optical scanner] is in no way less susceptible to bugs, tampering, or co-option than any other part of the Unity system."

20. The scanner uses light measurements to determine what ballot positions have marks on them, and may store the images thus generated as ballot scans. While the scans do originate through a physical process, they are not like photographs. They are computer data, stored as ones and zeroes and handled by computer software. As a general principle, though the specifics may vary with the specific op-scan system, they can be deleted, replaced or tampered with like any other computer data.
21. Once the scanner has obtained the scan data, it uses instructions regarding the order and position of the various contests and options to determine the votes on a ballot. These ballot programming instructions are delivered, shortly before every election, generally through a removable memory device.
22. A scanner may misinterpret a vote for various reasons: a voter may not have marked the oval as expected to—she may check the oval or circle the candidate's name; a voter may make very light marks on the ballot that are not detected; the voter may enter a write-in vote thinking she needs to both mark the oval next to her candidate and write-in the name; some optical scanners may not detect red ink<sup>5</sup>; ballot programming errors or intentional hacking can lead to votes being swapped among candidates. Newer scanners use more sophisticated techniques to deal with light marks and some identify problem ballots for humans to adjudicate. However, one cannot rely on scanners to do so without error. And scanners cannot detect programming errors or intentional attacks.
23. Logic and Accuracy testing (L&A testing) is intended to test for some of the above problems before the elections, but human error can result in the tests not being correctly completed and equipment malfunction can result in the equipment behaving differently

---

<sup>5</sup> In 2004, in Napa County, CA, a primary election lost 6,000 votes because the scanner was not calibrated to read all types of ink. See: Kim Zetter, "E-Vote Snafu in California County," *Wired*, 2004. <http://archive.wired.com/politics/security/news/2004/03/62721>.

on Election Day. Further, a competent attacker would have the system behave as expected when tested, and maliciously during the election<sup>6</sup>.

24. Once the DRE or the optical scanner obtains the vote—whether after confirmation by the voter using a DRE or after the votes are read by an optical scanner—the votes are tabulated electronically by software.

25. In principle, at any point in the above process, software can alter the votes or the tallies

The University of Connecticut Center for Voting Technology Research (VoTeR Center) evaluated the security of AV-OS tabulators, a model also used in Wisconsin, on the request of the Connecticut Secretary of the State (SOTS) Office, in 2011. They reported<sup>7</sup>: “the memory cards used with AV-OS can be tampered with, thus proving the seriousness of the Hursti Hack. VoTeR Center also discovered new security vulnerabilities of AV-OS. We note that if the memory cards or the AV-OS tabulators are left unattended — within or without the tabulator — they can be tampered with in a matter of minutes. The effects of tampering with the AV-OS and memory cards on the election outcome can be devastating: votes cast on ballots can be reassigned to arbitrary candidates, leading to invalid election results. Subsequent reports by VoTeR Center document additional integrity issues with AV-OS systems. In particular, we determined that even if the memory card is sealed and pre-election testing is performed, one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and

---

<sup>6</sup> Volkswagen's 2L Diesel cars were found to use more emission controls when they were being tested than during normal use. On examination, it was found that their software was written to detect when a test was underway. See: [https://en.wikipedia.org/wiki/Volkswagen\\_emissions\\_scandal](https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal) In our case, software manipulated without vendor knowledge could also provide testers with the results they expected to see. Then the software could perform differently when used in the election.

<sup>7</sup> VoTeR Center: UConn Center for Voting Technology Research, “Technological Audits of Optical Scan Voting Systems: Summary for 2007 to 2010 Connecticut Elections”, Kiayias et al, reference. October 19, 2011, Version 1.1. <https://voter.engr.uconn.edu/voter/wp-content/.../VC-TechAudits-2007-2010c.pdf>

without having ever to access the card physically or opening the AV-OS system enclosure. For example, the attacks can lead to the following: Neutralizing candidates: The votes cast for a candidate are not recorded; Swapping candidates: The votes cast for two candidates are swapped; Biased Reporting: The votes are counted correctly by the terminal, but they are reported incorrectly using conditionally-triggered biases.” I am not aware if the systems have been modified to resist these specific attacks since they were discovered; regardless, they illustrate the general principle that op-scan systems of this kind are very vulnerable.

26. The method of delivery of the malicious code depends on the type of scanner used. In older op-scan systems, the removable memory used to store counts also stores a computer program to print the results that can be manipulated to print different results.<sup>89</sup> In newer op-scan systems such as the Model 100 also used in WI, the removable memory also delivers software updates, and can be used as a means of delivering malicious code<sup>10</sup>.
27. Note that one cannot depend on detecting the above types of alteration without a manual review of the paper votes (or, potentially, a forensic audit) because the software process is unobservable and because it is possible for a competent attacker to erase their tracks.
28. In the event that an election outcome were incorrect, the only way to detect this with high certainty is to manually examine the paper votes cast. Rescanning and retabulation of the ballots, even if by another scanner, could lead to the same error or malware, delivered by the same source, having the same influence on the retabulated election outcome.

---

<sup>8</sup> The “Hursti Hack”, [https://en.wikipedia.org/wiki/Hursti\\_Hack](https://en.wikipedia.org/wiki/Hursti_Hack)

<sup>9</sup> See Doug Jones’ comments on Andrew Appel’s blog post at: <https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/>

<sup>10</sup> Andrew Appel, “Which voting machines can be hacked through the internet?”, blog post, Freedom to Tinker, September 20, 2016. <https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/>



Moreover, where the same scanner is used, as I understand the Wisconsin recount procedures permit, the problem is exacerbated because any attack on the scanner's software (software that is often referred to as "firmware") would make the recount vulnerable as well. Manual examination of securely-stored paper ballots can greatly increase certainty in the outcome.

29. For the above reasons, it is important to make the election audit a standard part of the election process and, where there is no audit procedure, to perform a recount of paper ballots. When paper ballots are available, they provide very reliable independent evidence about voter intent.
30. Given the unhealthy interest demonstrated by foreign powers in influencing the 2016 presidential election, I believe we would send the incorrect signal if we were not to review the voter-verified paper records of the election. We would be making very clear to a potential future attacker how to go about attacking the system. In contrast, if we review the voter-verified paper records from this election, it will serve as an important deterrent to dissuade potential cyberattackers in future elections.

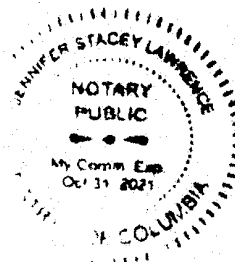
This affidavit was executed on the 28th day of November, 2016 in the District of Columbia

Poorvi Vora  
POORVI L. VORA

Sworn to before me this 28th day of November, 2016.

Jeff Stacey Lawrence  
Notary Public

My Commission Expires: Oct. 31 2021



**Exhibit A**

## Poorvi L. Vora

Department of Computer Science  
The George Washington University  
Washington D.C. 20052

202 994 1864  
poorvi@gwu.edu  
<http://www.seas.gwu.edu/~poorvi>

### Major Research Interests:

Electronic voting, cryptology, privacy, game theory, information theory, color imaging

### Education

Ph.D., Electrical Engineering. North Carolina State University (1993)

*Dissertation Title: Optimization Criteria and Numerical Analysis in the Design of Colour Scanning Filters*

*Dissertation Adviser: H. Joel Trussell*

M.S., Mathematics. Cornell University (1990)

M.S., Electrical Engineering. North Carolina State University (1988)

*Thesis Topic: Bounds on the Improvement of Restoration Using Spatial a priori Information*

*Thesis Adviser: H. Joel Trussell*

B. Tech., Electrical and Electronics Engineering. Indian Institute of Technology, Bombay (1986)

### Positions

*Professor, AY 2015-current*

Department of Computer Science, The George Washington University

*Board of Advisers, 2015-current*

Verified Voting Foundation

*Associate Professor, AY 2009-2015*

Department of Computer Science, The George Washington University

*Visiting Associate Professor, AY 2011-2012, on sabbatical*

Department of Computer Science and Engineering, Indian Institute of Technology-Bombay

*Assistant Professor, AY 2003-AY 2009*

Department of Computer Science, The George Washington University

*Faculty Computer Scientist – Intermittent Appointment, 2008-2011*

Security Technology Group, National Institute of Standards and Technology

At Hewlett-Packard Co. (Oct. 1995-July 2003)

- *Security Architect*, Office of the CTO, Imaging and Printing, Oct. 2002 - Aug. 2003

- *Senior Technical Contributor*, Hewlett-Packard Labs., Jan. 2001-Oct. 2002

- *Project Manager*, Mar. 2000-Jan. 2001

- *Member Tech. Staff and Project Scientist*, Hewlett-Packard Labs., Oct. 1995 - Mar. 2000

*Assistant Professor, Fall 1994 - Fall 1995*

School of Biomedical Engineering, Indian Institute of Technology-Bombay

Lecturer, Summer 1994

Department of Electrical Engineering, Indian Institute of Technology-Delhi

Research Scientist, Nov. 1993 - May 1994

Ravi Database Consultants (RDC), Bombay, India

### Awards

- School of Engineering and Applied Science Outstanding Teacher Award for Associate/Full Professors, 2015 "in recognition of her demonstrated ability to greatly improve student learning in difficult courses in her field, and her exceptional student advising and mentoring approach"
- ACM Teacher of the Year Award, 2009. Shared with Bhagirath Narahari "for having greatly impacted the life of the students of the Class of 2009"

### Doctoral Students

1. Sarah Alzakari (current)
2. Hua Wu (current)
3. Reham Almukhlifi (current)
4. Kerry A. McKay, 2011  
Dissertation Title: *Analysis Of ARX Round Functions In Secure Hash Functions*  
Now at NIST  
Funded in part by NSF
5. Benjamin Hosp (ARCS Scholar: 2005-06; 2006-07), 2011  
Dissertation Title: *The Privacy And Verifiability of Voting Systems: Measures and Limits*  
Now at Progeny  
Funded in part by NSF
6. Stefan Popoveniuc, 2009 (co-advised by David Chaum)  
Dissertation Title: *A Framework For Secure Electronic Voting*  
Now at Amazon.com  
Funded in part by NSF
7. Yu-An Sun, 2009  
Dissertation Title: *The Second Chance Offer: Optimal Strategies for Sellers and Bidders*  
Now at PARC

### Thesis Master's Students

1. Darakhshan Mir, *Related-key linear cryptanalysis of DES*. 2006.  
Ph.D., Rutgers University, 2013.  
Now tenure-track Assistant Professor and Jane W. Griffith Faculty Fellow at Bucknell.
2. Rajat Bhatt, *Related-key attacks on pseudo-random number generators*. 2005.  
Now at Microstrategy.

### Supervised Undergraduate Research

1. Katherine Walker, current.  
Funded in part by NSF.
2. Brannon McGraw (B.S., 2015, now at Visa)  
Funded in part by SUPER.

3. John Wittrock (B.S., 2013, SEAS Distinguished Scholar, now at AppNexus)  
Funded in part by NSF. Co-author on one paper.
4. Tyler Kaczmarek (B.S., 2013, now in doctoral program at U.C. Irvine)  
Funded in part by NSF and GW-SEAS Summer Undergraduate Program in Engineering Research (SUPER). Co-author on one paper.
5. Jan Rubio (B. S., 2011, Freudenthal Award, Pelton Award Second Prize, now at oPower)  
Funded in part by NSF. Co-author on two papers.
6. Alex Florescu (B.S., 2010, Arnold P. Meltzer Award for Best Computer Science Senior Design Project (2010), M. S., 2011, now at YPlan, UK; )  
Funded in part by NSF. Co-author on two papers.
7. Jacob Alperin-Sheriff (B.S., 2010, Ph. D., Georgia Tech., 2015, now at NIST).  
Funded in part by NSF.

#### Post-Doctoral Researchers Supervised

1. Filip Zagórski, October 2010-November 2011  
now Assistant Professor, Wroclaw University of Technology, Poland  
Fully-funded by NSF
2. Mridul Nandi, December 2009-August 2010  
now Assistant Professor, Indian Statistical Institute  
Fully-funded by NSF

#### Visiting Faculty Hosted

Ronald L. Rivest, Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science, MIT, October 2009

Ricardo Custodio, Dept. of Computer Science, Universidade Federal de Santa Catarina (UFSC), Brazil, AY 2006-07

#### Research Sponsorship

1. Poorvi L. Vora (PI) and Michael R. Clarkson, "TWC: TTP Option: Small: Open-Audit Voting Systems—Protocol Models and Properties".  
*National Science Foundation CNS-1421373. \$688,554*  
September 1, 2014-August 31, 2017
2. Poorvi L. Vora, "Reasoning about Protocols with Human Participants".  
*National Security Agency*, Subaward on Prime Award to University of Maryland, College Park (UMCP)<sup>1</sup>.  
Estimated total award: \$305,642  
February 7, 2014-February 6, 2017; currently granted for first two years, renewed annually
3. Poorvi Vora (PI), Gabriel Parmer. "RAPID: Secure Bulletin Boards and Absentee Voting in Real-World Independently-Verifiable Elections".  
*National Science Foundation CNS-0937267. \$99,673.*  
July 1, 2011-June 30, 2013.
4. Poorvi Vora. "EAGER: Electronic End-to-End Independently Verifiable (E2E) Voting Systems".  
*National Science Foundation CNS-0937267. \$239,767.*  
October 1, 2009-September 30, 2012.

---

<sup>1</sup>UMCP PI: Jonathan Katz.

5. Poorvi Vora. "Statistical cryptanalysis of block ciphers as channel communication".  
*National Science Foundation CCF-0830576*. \$141,643.  
September 1, 2008-August 31, 2011.
6. Poorvi Vora. "CT-ISG: The Privacy and Verifiability of Practical Voting Systems".  
*National Science Foundation CNS-0831149*. \$180,478.  
September 1, 2008-August 31, 2011.
7. Poorvi Vora (PI), Jonathan Stanton, Rahul Simha. "SGER: A Performance Ratings Framework for the Evaluation of Electronic Voting Systems".  
*National Science Foundation IIS-0505510*. \$85,582.  
March 1, 2005-August 31, 2006.
8. Poorvi Vora.  
*Research Gift, Hewlett-Packard Co.* \$30,000.  
AY 2004-2005
9. Poorvi Vora (PI) and Sumit Joshi. "Randomized Auctions and the Economic Value of Privacy".  
*GW Dilthey Award*. \$12,129.  
July-August 2004.
10. Poorvi Vora. Workshop Co-sponsorship: Threat Analyses for Voting System Categories: A Workshop on Rating Voting Methods (VSRW) 2006.  
*National Institute for Standards and Technology (NIST)*. Approximately \$10,000.  
Summer 2006.

## Pedagogy

### • Classes Taught

#### At GW

- Computer Security
- Cryptography
- Advanced Cryptography
- Discrete Structures II.

#### *Guest Lectures:*

- Econ 8303, Microeconomics III: Fall 2013, four weeks
- CSci 147, Team Project Development & Professional Ethics: Spring 2007, 2008
- CSci 01, Computer Science Orientation: Fall 2006, 2007
- CSci 178, Database Systems I: Fall 2003, 2004; Spring 2007
- CSci 297, Electronic Voting: Fall 2004
- CSci 41, Introduction to Computer Science: Fall 2004, 2005

#### At IIT-Bombay

*Medical Signal and Image Processing*, AY 1994-1995

*Partial Differential Equations*, AY 1994-1995

*Computational Algebra and Number Theory*, AY 2011-2012

At Cornell University (While in graduate program — I had independent charge and was instructor for my section)

*Calculus I*

*Calculus II*

*Pre-freshman Mathematics*

### • Curriculum Development

- Director of CSIA graduate certificate program: Fall 2005-2011 (joint with former faculty member Jonathan Stanton until Fall 2008)
- Course Director
  - \* Computer Security (graduate—6531/283—and undergraduate—4531/172)
  - \* Cryptography (graduate—6331/284—and undergraduate—4331/162)
  - \* Advanced Cryptography (graduate: 8331/381)
- Courses Proposed and Designed.
  - \* CSCI 8331/381, Advanced Cryptography
  - \* CSCI 2312/124, Discrete Structures II (co-proposer: Abdou Youssef).
- Courses Designed
  - \* CSCI 4331/162, Cryptography

### Selected Service

#### • Professional

- Invited Participation, Technical Team, End-to-End Verifiable Internet Voting Project of the Overseas Vote Foundation, 2014–2015
- Associate Editor: *IEEE Transactions on Information Forensics and Security*, 2010-2013
- Guest Editor: *IEEE Transactions on Information Forensics and Security*, special issue on electronic voting, December 2009.  
With: Ronald L. Rivest (Lead GE), David Chaum, Bart Preneel, Aviel D. Rubin, Donald G. Saari
- Program Committees: *Voting*, 2016; *Vote-ID*, 2013, 2015; *WIFS*, 2012; *WOTE or EVT/WOTE*, 2006, 2007, 2011; *ICISS*, 2008, 2010; *CANS*, 2010; *NIST End-to-End Voting Workshop*, 2009; *RE-Vote*, 2009; *EVOTE*, 2008; *VoComp*, 2007; *ACM CCS*, 2006.
- Invited external expert, Selection Committee (faculty hiring and promotion), DAIICT, Gandhinagar, India: 2012, 2013
- Invited Participant:
  - \* 2010 NSF Workshop on the Future of Trustworthy Computing, October 27-29, 2010, Arlington, VA
  - \* US-EU workshop on "International Co-operation in Trustworthy Systems: Security, Privacy and Trust in Large-Scale Global Networks & Services as Part of the Future Internet", Madrid, Spain, March 30-April 1, 2009, organized by the National Science Foundation and the European Union.
  - \* *DIMACS/Portia Working Group on Privacy in Data Mining*, 2004
- Invited expert at meeting on New Currency Designs, Bureau of Engraving and Printing, Dept. of the Treasury, US Govt. Fall 2004
- Reviewer for *IEEE Trans. Info. Security and Forensics*, *IEEE Trans. Computers*, *IEEE Trans. Image Proc.*, *IEEE Trans. Signal Processing*, *IEEE Trans. Knowledge and Data Engineering*, *IEEE Security and Privacy*, *Electronic Imaging*, *Journal Optical Society of America - A*.

- Departmental
  - Undergraduate Adviser, AY 2013-current
  - MS Adviser, AY 2003-current
  - Faculty Mentor for Assistant Professor Claire Monteleoni, AY 2011-current
  - Curriculum Committee: AY 2004; AY 2009-2011; AY 2014-current
  - Graduate Applications and Support Committee: AY 2003-2008; AY 2014-2015
  - Women in Computer Science (WiCS): AY 2003-2004 (introduced and managed); AY 2009 - 2011 (managed); AY 2012-2014
  - Director, graduate certificate program in Computer Security and Information Assurance: AY 2005-2011. (Co-director with Prof. Jonathan Stanton, 2005-2008)
  - Undergraduate Recruiting: several lectures at Chantilly Academy, part of the Fairfax County High School system.
- School of Engineering and Applied Science (SEAS)
  - Pelton Award (Best Senior Design Project) Judge: 2014, 2015
  - R&D Showcase – co-Chief Judge, 2015, 2016
  - Promotion & Tenure Subcommittee (elected for two year term: 2016-2018)
- Community
  - Testimony to State Board of Elections, MD, September 2016
  - Member of the Scantegrity project, which deployed a voting system for Takoma Park city elections, 2009 and 2011
  - Guest Lectures on cryptography, Chantilly Academy, Fairfax County High Schools: Spring 2007, 2008, 2010
  - Chantilly Academy Award “in recognition and grateful appreciation of exceptional leadership support”: 2007 and 2008.
  - Guest lecture on Pakistani poet Faiz Ahmed Faiz, Hunter College, NY. Course on *Partition Literatures*.

## Publications

From 2004 onwards, I have attempted to list authors in alphabetical order in my publications. Those authors who are (intentionally) not listed alphabetically are marked with \*.

Co-authors who were my students or post-docs at the time the work was done are marked with †.

Click on the paper title in the electronic copy of the CV to link to a copy of the paper.

## Journal Papers Appeared (including Periodicals)

1. Sumit Joshi\* and Poorvi L. Vora. “Weak and Strong Multimarket Bidding Rings”. *Economic Theory*, vol. 53, no. 3, pp. 657-696, June 2012.
2. Sumit Joshi, Yu-An Sun† and Poorvi L. Vora. “Price Discrimination and Privacy: a Note”. *International Journal of Game Theory*, vol. 13, no. 1, pp. 83-92, March 2011.
3. David Chaum\* , Richard T. Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc†, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, Alan T. Sherman, and Poorvi L. Vora. “Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes”. *IEEE Transactions on Information Forensics and Security*. Special issue on electronic voting. Vol. 4, No. 4, Part I, pp 611-627, December 2009.



4. Yu-An Sun<sup>†</sup> and Poorvi L. Vora. "Auctions and Differential Pricing: Optimal Seller and Bidder Strategies in Second-Chance Offers". *Computational Economics*, Vol. 34, No. 3, pp. 243-271, October 2009.
5. David Chaum, Ben Hosp<sup>†</sup>, Stefan Popoveniuc<sup>†</sup> and Poorvi L. Vora. "Accessible Voter Verifiability". *Cryptologia*, Vol. 33, No. 3, pp. 283-291, July 2009.
6. Stefan Popoveniuc<sup>†</sup> and Poorvi L. Vora. "A framework for secure electronic voting". *Cryptologia*, Vol. 34, No. 3, pp. 236-257, June 2010.
7. Rahul Simha and Poorvi L. Vora. "Vote Verification using Hard AI Problems". *Journal of Information Assurance and Security*, Vol. 3, No. 4, pp. 270-278, 2008.
8. Ben Hosp<sup>†</sup> and Poorvi L. Vora. "An information-theoretic model of voting systems". *Mathematical and Computer Modelling*, special issue on: Mathematical Modeling of Voting Systems and Elections: Theory and Applications. Vol. 48, Nos.9-10, pp. 1628-1645, November 2008.
9. David Chaum\*, Aleks Essex\*, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, Poorvi Vora. "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting". *IEEE Security and Privacy*, special issue on electronic voting, Vol 6., No. 3, pp. 40-46, May/June 2008.
10. Poorvi L. Vora. "An Information-Theoretic Approach to Inference Attacks on Random Data Perturbation and a Related Privacy Measure". *IEEE Transactions on Information Theory*, Vol. 53, No. 8, pp 2971-2977, August 2007.
11. P.L. Vora\*, B. Adida, R. Bucholz, D. Chaum, D.L. Dill, D. Jefferson, D.W. Jones, W. Lattin, A.D. Rubin, M.I. Shamos, and M. Yung. "Evaluation of Voting Systems". Inside Risks Column. *Communications of the ACM*, vol. 47, no. 11, pp. 144, November 2004.
12. K. Gopalakrishnan, Nasir D. Memon and Poorvi Vora. "Protocols for Watermark Verification". *IEEE MultiMedia*, special issue on Multimedia and Security, vol. 8, no. 4, pp. 66-70, October-December 2001.
13. Poorvi L. Vora. "Inner Products and Orthogonality in Color Recording Filter Design". *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 632-642, April 2001.
14. Poorvi L. Vora, Joyce E. Farrell, Jerome D. Tietz, David H. Brainard. "Image Capture: Simulation of Sensor Responses from Hyperspectral Images". *IEEE Transactions on Image Processing*, vol. 10, no. 2, pp. 307-316, February 2001.
15. Poorvi L. Vora and H. Joel Trussell. "Mathematical Methods for the Analysis of Color Scanning Filters". *IEEE Transactions on Image Processing*, vol. 6, no. 2, pp. 321-327, February 1997.
16. Poorvi L. Vora and H. Joel Trussell. "Mathematical Methods for the Design of Color Scanning Filters". *IEEE Transactions on Image Processing*, vol. 6, no. 2, pp. 312-320, February 1997.
17. Poorvi L. Vora and H. Joel Trussell. "Measure of goodness of a set of color scanning filters". *Journal of the Optical Society of America-A*, vol. 10, no. 7, pp. 1499-1508, July 1993.

#### Journal Papers in Preparation

1. Filip Zagórski, Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, Jonathan Katz and Poorvi L. Vora, "The Remotegrity Protocol and its Properties".
2. Kerry McKay<sup>†</sup> and Poorvi L. Vora. "Analysis of ARX Functions: Pseudo-linear Cryptanalysis and a Diffusion Metric".

#### Guest Editor, Special Issue

1. Ronald L. Rivest\*, David Chaum, Bart Preneel, Aviel D. Rubin, Donald G. Saari, Poorvi L. Vora. *IEEE Transactions on Information Forensics and Security*, vol 4, no. 4, Part I, December 2009. "Guest editorial".

#### Book Chapters

1. Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, Poorvi L. Vora, John Wittrock, and Filip Zagorski, The Scantegrity Voting System and its Use in the Takoma Park Elections, Real-World Electronic Voting: Design, Analysis and Deployment, Feng Hao and Peter Ryan, CRC Press, Taylor & Francis Group, *in press*.
2. Ian Dickinson, Dave Reynolds, Dave Banks, Steve Cayzer, and Poorvi Vora. "User profiling with privacy: a framework for adaptive information agents". *Intelligent Information Agents: An AgentLink Perspective*, Chp. 4. Editors: Matthias Klusch, Sonia Bergamaschi, Pete Edwards, Paolo Petta. Springer Verlag, LNAI 2586, 2003.

#### Refereed Conference and Workshop Papers With Published Proceedings

Acceptance rates are mentioned where available.

1. Dawid Gawel, Maciej Kosarzewski, Poorvi Vora, Hua Wu<sup>†</sup>, Filip Zagórski. "Apollo—End-to-end Verifiable Internet Voting with Recovery from Vote Manipulation", *E-Vote-ID*, 2016.
2. Tyler Kaczmarek\*<sup>†</sup>, John Wittrock\*<sup>†</sup>, Richard Carback, Alex Florescu<sup>†</sup>, Jan Rubio<sup>†</sup>, Noel Runyan, Poorvi L. Vora, Filip Zagórski<sup>†</sup>. "Dispute Resolution in Accessible Voting Systems: The Design and Use of Audiotegrity". *Vote-ID 2013*, Guildford, UK, 17-19 July, 2013. Springer LNCS vol. 7985, pp. 127-141. Acceptance Rate: 12/26  $\approx$  0.46
3. Richard Carback, David Chaum, Jeremy Clark, Aleksander Essex, Poorvi L. Vora, Filip Zagórski<sup>†</sup>, "Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System". *ACNS 2013*, Banff, Canada, 25-28 June, 2013. Springer LNCS vol. 7954, pp. 441-457. Acceptance Rate: 33/150  $\approx$  0.22
4. David Chaum, Alex Florescu<sup>†</sup>, Mridul Nandi<sup>†</sup>, Stefan Popoveniuc<sup>†</sup>, Jan Rubio<sup>†</sup>, Poorvi L. Vora, Filip Zagórski<sup>†</sup>. "Paperless Independently-Verifiable Voting". *VoteID 2011*, Tallinn, Estonia, 28-30 September 2011. Springer LNCS vol. 7187, pp 140-157. Acceptance Rate: 15/33  $\approx$  0.45
5. Mridul Nandi<sup>†</sup>, Stefan Popoveniuc, Poorvi L. Vora. "Stamp-It: A Method for Enhancing the Universal Verifiability of E2E Voting Systems". *ICISS 2010*, Gandhinagar, India, 15-19 December 2010. Springer LNCS vol. Volume 6503, pp. 81-95. Acceptance Rate: 14/51  $\approx$  0.27
6. Richard Carback\*, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc<sup>†</sup>, Ronald L. Rivest, Emily Shen, Alan T. Sherman, Poorvi L. Vora. "Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy". *USENIX Security*, Washington, D.C., 11-13 August, 2010. Acceptance Rate: 30/202  $\approx$  0.15
7. Stefan Popoveniuc, John Kelsey, Andrew Regenscheid, Poorvi Vora. "Performance Requirements for End-to-End Verifiable Elections". *EVT/WOTE 2010*, held in conjunction with USENIX Security, Washington, D.C., 9-10 August, 2010. Acceptance Rate: 15/38  $\approx$  0.39
8. Alan T. Sherman\*, Richard Carback\*, David Chaum, Jeremy Clark, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc<sup>†</sup>, Ronald L. Rivest, Emily Shen, Bimal Sinha, Poorvi Vora. "Scantegrity Mock Election at Takoma Park". *EVOTE2010*, Bregenz, Austria, 21-24 July 2010. Acceptance Rate < 0.5

- An abstract on this material was presented earlier with a slightly different author list, in a conference without published proceedings. This abstract is listed in a later section in this CV, and is mentioned here for completeness. Alan T. Sherman\*, Richard Carback\*, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Harrison, Travis Mayberry, Stefan Popoveniuc†, Ronald L. Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, Poorvi Vora. "Scantegrity Mock Election at Takoma Park". *NIST End-to-End Voting Systems Workshop*, Washington DC, 13-14 October, 2009
- 9. Sumit Joshi, Yu-An Sun† and Poorvi L. Vora. "Privacy In A Multi-Stage Game – An Evolutionary Programming Approach". *Eproceedings of 10th Joint Conference on Information Sciences, 6th International Conference on Computational Intelligence in Economics & Finance*, Salt Lake City, Utah, 18-24 July 2007, pp 529-535.
- 10. Sumit Joshi, Yu-An Sun† and Poorvi Vora. "Randomization as a Strategy for Sellers During Price Discrimination, and Impact on Bidders' Privacy". Short paper, *5th ACM Workshop on Privacy in the Electronic Society (WPES)* held in association with ACM CCS, Alexandria, VA, 30 October, 2006, pp. 73-76. Acceptance Rate:  $16/39 \approx 0.41$
- 11. Poorvi L. Vora\* and Darakhshan J. Mir†. "Related-Key Linear Cryptanalysis". *IEEE International Symposium on Information Theory (ISIT)*, Seattle, WA, 9-14 July, 2006, pp. 1609-1613.
- 12. Sumit Joshi, Yu-An Sun†, Poorvi L. Vora. "The Privacy Cost of the Second-Chance Offer". *2005 ACM Workshop on Privacy in the Electronic Society (WPES)* held in association with ACM CCS, Alexandria, VA, 7 November, 2005, pp. 97-106. Acceptance Rate:  $15/40 \approx 0.38$
- 13. Poorvi L. Vora. "Information Theory and the Security of Binary Data Perturbation". *INDOCRYPT 2004*, Chennai, India, 20-22 December, 2004. Springer LNCS 3348, pp. 136-147. Acceptance Rate:  $30/147 \approx 0.20$
- 14. Cormac Herley\*, Poorvi Vora and Shawn Yang. "Detection and Deterrence of Counterfeiting of Valuable Documents". *IEEE International Conference on Image Processing (ICIP)*, Singapore, 24-27 Oct. 2004, vol. 4, pp. 2423-2426.
- 15. Nasir D. Memon, Poorvi L. Vora, Boon-Lock Yeo, and Minerva M. Yeung. "Distortion-bounded authentication techniques". *SPIE Conference on Security and Watermarking of Multimedia Contents II*, San Jose, CA, 24-26 January 2000, vol. 3971, pp. 164-74.
- 16. K. Gopalakrishnan, Nasir D. Memon and Poorvi Vora. "Protocols for Watermark Verification". *Multimedia and Security Workshop of ACM International Multimedia Conference*, Orlando, Florida, GMD Report No. 85, Oct. 1999, pp. 91-94. (This paper was invited to a special issue of IEEE Multimedia, see section on journals and periodicals).
- 17. Poorvi L. Vora. "Robust Watermarking Using Argument Modulation". *PICS (Image Processing, Image Quality, Image Capture Systems)*, Savannah, Georgia, April 1999, p. 290-294.
- 18. Richard L. Baer, William D. Holland, Jack M. Holm, and Poorvi L. Vora. "A Comparison of Primary and Complementary Color Filters for CCD-based Digital Photography". *IS&T/SPIE Conference on Sensors, Cameras, and Applications for Digital Photography*, San Jose, CA, 27 January 1999, vol. 3650, pp. 16-25.
- 19. Nasir D. Memon and Poorvi L. Vora. "Authentication Techniques for Multimedia Content". *SPIE Conference on Multimedia Systems and Applications, Photonics East*, Boston, MA, 2 November 1998, vol. 3528, pp. 412-422.
- 20. Poorvi Vora and Cormac Herley. "Trade-offs Between Color Saturation and Noise Sensitivity in Image Sensors". *IEEE International Conference on Image Processing (ICIP)*, Chicago, IL, 4-7 October 1998, vol. 1, pp. 196-200.

21. Poorvi L. Vora, Joyce E. Farrell, Jerome D. Tietz and David H. Brainard. "Linear Models for Digital Cameras". *IS&T's 50th Annual Conference*, Cambridge, MA, 18-23 May 1997, pp. 377-382.
22. Poorvi L. Vora, Michael L. Harville, Joyce E. Farrell, Jerome D. Tietz, and David H. Brainard. "Image capture: synthesis of sensor responses from multispectral images". *SPIE/IS&T Conference on Color Imaging: Device Independent Color, Color Hard Copy, and Graphic Arts II*, 10 February 1997, San Jose, CA, vol. 3018, pp. 2-11.
23. Bhaskar Bhumkar<sup>†</sup>, Poorvi L. Vora, B. Chandna and K. Shankar. "A set-theoretic approach to image reconstruction from projections". *IEEE International Conference on Image Processing (ICIP)*, Lausanne, Switzerland, 16-19 September 1996, vol. 2, pp. 737-740.
24. Poorvi L. Vora, H. Joel Trussell and Lawrence S. Iwan. "Design Results for a Set of Thin Film Color Scanning Filters". *IS&T/SPIE Symposium on Electronic Imaging, Science and Technology*, San Jose, CA, 6-10 February 1995, vol. 2414, pp. 70-75.
25. Poorvi L. Vora, H. Joel Trussell, and Lawrence S. Iwan. "Mathematical method for designing a set of color scanning filters". *SPIE and IS&T Conference on Color Hard Copy and Graphic Arts II*, San Jose, CA, 31 January-5 February 1993, vol. 1912, pp. 322-329. 1993.
26. H. J. Trussell and P. L. Vora. "On the Accuracy of Scanning Color Images". *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, San Francisco, CA, 23-26 March 1992, vol. 3, pp. 161-164.
27. Poorvi L. Vora and H. Joel Trussell. "Measures of Goodness of a Set of Color Scanning Filters". *SPIE and IS&T Conference on Color Hard Copy and Graphic Arts*, San Jose, CA, 11-14 February 1992, vol. 1670, pp. 344-352.
28. H. Joel Trussell and Poorvi L. Vora. "Bounds on restoration quality using a priori information". *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, New York, NY, 11-14 April 1988, vol. 3, pp. 1758-1761.

#### Refereed/Lightly-Refereed Conference and Workshop Papers Without Formal Proceedings

Many of these conferences allow the resubmission of these papers to other venues; further, many of these conferences also allow the submission of work published elsewhere.

1. Kerry A. McKay<sup>†</sup>, Poorvi L. Vora. "Pseudo-Linear Approximations for ARX Ciphers With an Application to Threefish-256". Second SHA-3 Candidate Conference, Santa Barbara, CA, 23-24 August 2010. Also available as IACR ePrint, see below.
2. David Chaum, Stefan Popoveniuc<sup>†</sup>, Poorvi L. Vora. "eTegrity and ePunchScan". *NIST End-to-End Voting Systems Workshop*, Washington DC, 13-14 October, 2009.
3. Stefan Popoveniuc<sup>†</sup> and Poorvi L. Vora. Similar or identical versions presented at:
  - Presented as "Remote ballot casting with Captchas". *3rd Benelux Workshop on Information and System Security (WISSEC)*, Eindhoven, The Netherlands, 13-14 November, 2008.
  - Presented as "Secure voting using infected computers". 8th Annual Security Conference, Las Vegas, Nevada, April 2009.
4. Stefan Popoveniuc<sup>†</sup> and Poorvi L. Vora. "A framework for secure electronic voting". *WOTE 2008*, held in conjunction with *8th Privacy Enhancing Technologies Symposium (PET)*, Leuven, Belgium, July 22-23, 2008.
5. Rahul Simha and Poorvi L. Vora. "Vote Verification using CAPTCHA-like Primitives". *WOTE 2007*, held in conjunction with *7th Workshop on Privacy Enhancing Technologies (PET)*, Ottawa, Canada, June 20-June 21, 2007. (Extended Abstract)

6. Ben Hosp<sup>†</sup> and Poorvi L. Vora. "An Information-Theoretic Model of Voting Systems". Similar or identical versions presented at:
  - *IAVoSS Workshop on Trustworthy Elections (WOTE)*, held in conjunction with *6th Workshop on Privacy Enhancing Technologies (PET)*, Cambridge, UK, June 29-June 30, 2006.
  - *Threat Analyses for Voting System Categories. A Workshop on Rating Voting Methods (VSRW)*, Washington, DC, 8-9 June 2006.
  - *Frontiers of Electronic Voting*, Dagstuhl Seminar Series, 2008. (This venue was unrefereed).

#### Abstracts

1. Alan T. Sherman\*, Richard Carback\*, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc<sup>†</sup>, Ronald L. Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, Poorvi Vora. "Scantegrity Mock Election at Takoma Park". *NIST End-to-End Voting Systems Workshop*, Washington DC, October 13-14, 2009
2. Poorvi Vora. "The channel coding theorem and the security of binary randomization". *IEEE International Symposium on Information Theory (ISIT)*, Yokohama, Japan, 29 June-4 July 2003, pp. 306. (With Proceedings)

#### Invited Paper

1. Yu-An Sun and Poorvi L. Vora. "From eBay's Second Chance Offer to B2B Service Pricing: Similarity and Challenges". *Invited Paper*, 2009 IEEE International Conference on Service Operations, Logistics and Informatics. Chicago, July 2009.

#### Patent Applications Granted

1. Poorvi L. Vora and Verna E. Knapp. "Anonymous transactions based on distributed processing". US 7187772. Issued 6 March 2007.
2. Cormac Herley, Xuguang Yang, Poorvi Vora. "Detection and deterrence of counterfeiting of documents having a characteristic color". US 6748100. Issued June 8, 2004.
3. Xuguang Yang, Poorvi L. Vora and Cormac Herley. "Multi-level detection and deterrence of counterfeiting of documents with reduced false detection". US 6516078. Issued February 4, 2003.
4. Poorvi L. Vora, Verna E. Knapp and Umesh V. Vazirani. "Probabilistic Privacy Protection". US 6470299. Issued October 22, 2002.
5. Poorvi L. Vora. "Robust watermarking for digital objects". US 6463162. Issued October 8, 2002.
6. Cormac Herley and Poorvi Vora. "Detection and deterrence of counterfeiting of two-sided documents". US6335794. Issued January 1, 2002. (The US government has shown interest in using this to prevent counterfeit)

#### Presentations by my Research Undergraduate Students at Undergraduate Student Conferences

1. Alex Florescu<sup>†</sup>, Stefan Popoveniuc<sup>†</sup>, Poorvi L. Vora. "Accessible Voting Interface Using an Interactive Voice System Model", *20th Annual Argonne Symposium for Undergraduates in Science, Engineering and Mathematics*, Argonne National Laboratory, 13 November 2009.
2. Jan Michael Rubio<sup>†</sup>, Ben Hosp<sup>†</sup>, Poorvi L. Vora. "Comparing Privacy Properties of Mixnet Audits used by End-to-End Voting Systems", *20th Annual Argonne Symposium for Undergraduates in Science, Engineering and Mathematics*, Argonne National Laboratory, 13 November 2009.

### Relevant Selected Recent Invited Presentations on Secure Electronic Voting

- Remote Voting Conference, CDAC under the aegis of Department of Electronics and Information Technology (DeitY), Govt. of India, June 2015
- DC Area Privacy and Security Seminar (DC-APS), April, 2013
- National Institute of Standards and Technology, Gaithersburg, MD, May 2011
- Indian Institute of Technology, Bombay, January 2011
- Indian Institute of Technology, Hyderabad, January 2011
- Information Systems Seminar, Princeton University, April 2010
- Hewlett-Packard Labs., Princeton, NJ, April 2010

### Selected Media Coverage

- *Wired*. March 21, 2016. Issie Lapowsky. "Utah's Online Caucus Gives Security Experts Heart Attacks".
- *Washington Post* April 6, 2015. "Can you vote for the next president on your smartphone? Not just yet" By Amrita Jayakumar.
- *Electionline Weekly* June 16, 2011. "Takoma Park, Md. tests online absentee voting". By Kristi Tousignant.
- *FairVote Blog* June 9, 2011. "Internet Voting 2.0 and Other Advances in Election Technology in Takoma Park". By Melanie Kiser.
- *WAMU News* (WAMU Radio is the DC NPR Affiliate). 4 November 2009. "Takoma Park Voters Use New System". By Matt Bush.
- *WAMU News* 3 November 2009. "New Voting Technology Makes Debut In Takoma Park". By Matt Bush.
- *WAMU News*. 21 October 2008. "George Washington University Helps Devise New Voting System". By Matt Bush.
- *NPR Morning Edition*. March 7, 2008. "Shift Back to Paper Ballots Sparks Disagreement". By Pam Fessler.
- *IEEE Spectrum*. January 2007. "Making Every E-Vote Count". By Steven Cherry
- *C-SPAN* November 1, 2004. "George Washington Univ. Panel on Electronic Voting Machines".
- *CNET News.com*. June 08, 2004. "High hopes for unscrambling the vote". By Declan McCullagh.
- *SIAM News* Volume 37, Number 3, April 2004. "Works in progress: trustworthy cryptographic voting systems". By Sara Robinson.
- *New York Times* March 2, 2004. Science Edition. "Did your vote count? New coded ballots may prove it did". By Sara Robinson.

FILED

NOV 28 2016

DANE COUNTY CIRCUIT COURT

## AFFIDAVIT OF RONALD L. RIVEST

RONALD L. RIVEST, being duly sworn, deposes and says the following under penalty of perjury:

## BACKGROUND

1. My name is *Ronald L. Rivest*. I am an Institute Professor at the Massachusetts Institute of Technology in Cambridge, Massachusetts. I have been employed by MIT since the fall of 1974. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Wisconsin.
2. My CV and list of publications are available on my website:  
<http://people.csail.mit.edu/rivest>.
3. At MIT, my home department is the Department of Electrical Engineering and Computer Science. I have taught courses in computer programming, computer algorithms, cryptography, theoretical computer science, network and computer security, and elections and voting technology.
4. I am a co-author of the best-selling textbook "*Introduction to Algorithms*" (co-authored with Cormen, Leiserson, and Stein).
5. My research interests include algorithms, theoretical computer science, cryptography, machine learning, security, election integrity, and statistical methods for election auditing. I have published numerous research papers, books, and book chapters on these topics.
6. I am perhaps best known for the invention (with Adi Shamir and Len Adleman) of the *RSA public-key cryptosystem*, based on the difficulty of factoring the product of large prime numbers. This cryptosystem is widely used today to provide secure browsing and secure electronic commerce.
7. I have commercialized some of my innovations, founding companies *RSA Security*, *Verisign*, and *Peppercoin* in the security and digital payments spaces.
8. I have received numerous awards, including the prestigious ACM Turing Award (joint with Adi Shamir and Len Adleman); this award is considered by many to be the "Nobel Prize of Computer Science" (there is no actual Nobel Prize in this area).
9. I am member of the National Academy of Engineering and the National Academy of Science.
10. I have supervised graduate and undergraduate theses in many areas, including novel systems for secure voting.

11. I am on the Board of Verified Voting, a non-profit organization devoted to election integrity.
12. I am member of the *CalTech-MIT Voting Technology Project*, which has been working towards improved voting systems since 2001.
13. I am co-founder of the *Workshop on Trustworthy Elections* workshop series (WOTE, now merged with Electronic Voting Technology).
14. I have been a member of the *Technical Guidelines Development Group* (TGDC), an advisory group to the U.S. Elections Assistance Commission for the purpose of developing certification standards for election systems. I chaired the *Security and Transparency* subgroup of the TGDC.
15. I am a co-author and co-inventor (with John Wack) of the notion of "*software independence*" of a voting system: the notion that a voting system should not be vulnerable to suffering undetectable changes in the election outcome due to errors or misbehavior by the voting system software.
16. I am part of the team that fielded the "*Scantegrity*" voting system for two elections in Takoma Park, Maryland. Scantegrity is a novel voting system of the "end-to-end verifiable" type: voters can check on a website after the election to confirm that their ballot was included and counted as intended, without thereby being able to sell their votes(!).
17. I am an advisor to the *StarVote* project in Travis County (Austin) Texas, which will provide high-integrity voting systems to that county, based on both advanced cryptographic operations and statistical auditing methods.
18. I am a collaborator and co-author on the recent report "*The Future of Voting: End-to-End Verifiable Internet Voting --- Specification and Feasibility Study*", produced by the Overseas Vote Foundation.

## OPINION

19. I feel strongly that the security of voting systems is essential to our democracy—a voting system should accurately reveal the choice of the voters (collectively, not individually!), otherwise our democracy is lost.
20. Moreover, a voting system should not only be *accurate*, it should be *demonstrably accurate*. A voting system should produce *evidence* that is sufficient to convince a loser (and his/her supporters) that he/she lost fair and square.  
 Recounts and statistical post-election audits are two powerful tools for examining evidence (paper ballots) to produce a convincing proof that an announced outcome is correct. (Or, if the unofficial outcome is incorrect, for producing a convincing proof that another candidate is the correct winner.)



For our democracy to work well, election systems should produce the best and most convincing evidence that the announced election outcomes are correct. One should ask: what will it take to convince a skeptical supporter of a losing candidate that they really lost?

Evidence of the form, "You must trust the computer here." is not likely to be adequate (nor should it be).

21. I am a strong believer that *all* elections should be based on voter-verified paper ballots, and that statistical post-election audits should be used to check that the announced outcome is consistent with the cast paper ballots.
22. Professor Philip B. Stark and I have recently published an OpEd in USA Today (Nov. 18, 2016, entitled "Still Time for an Election Audit") arguing that performing statistical audits in every state (where possible) for the 2016 U.S. Presidential election would be good practice, and would not be very expensive.
23. I would recommend statistical audits for checking the correctness of the announced election outcome everywhere that paper ballots are used. The nature of the underlying statistics makes these audits quite cheap, except when the margin is very small.
24. When a statistical audit is not possible (say for reasons having to do with election law), then a full recount of the paper ballots can provide the desired assurances.
25. Voting machines are computers, and subject to the same security issues facing any computer system (and more, since privacy of the ballot must also be enforced).
26. We have learned the hard way that almost any computer system can be broken into by a sufficiently determined, skillful, and persistent adversary. There is nothing special about voting systems that magically provides protection against attack.

The computer systems of voting systems vendors and of election officials must be included in any list of potentially vulnerable systems.

An attacker may be able to place malware in the source code of a voting system before it is compiled and delivered to an election jurisdiction. (This may be for the firmware of the voting system, or for other election-specific software.) Current voting system certification procedures are not adequate to detect sophisticated injection of malware into a voting system. It is not possible, even in principle, to have a certification procedure that can detect whether a voting system will ever produce an erroneous result (this is due to a powerful result known as Rice's Theorem). The voting system software *when delivered* may contain malware capable of affecting the announced election outcome.

This malware may be set to be triggered when a particular event occurs---perhaps something based on the date, the jurisdiction, or the pattern of choices made in an early-cast "trigger" vote. The malware may lay dormant during so-called "logic and accuracy" testing, only to be activated during the actual election.

While such an attack may naively seem unlikely or implausible, it is not the sort of attack that is beyond the resources of a powerful nation-state, and may be likely or plausible today depending on political circumstances. The "Stuxnet" attack on Iranian nuclear facilities demonstrated that even computers that are not connected to the internet may be successfully attacked.

27. Voting system software may be maliciously designed, may contain bugs, or may be changed or replaced at some point during the pre-election roll-out of equipment.

28. It is important to realize that *it is not feasible to verify the correct operation of voting system software, even given the source code.*

Certification source code review and pre-election logic and accuracy testing are useful but weak tools for uncovering errors and bugs. These tools provide no proofs of correct operation, particularly when the errors or bugs may be maliciously devised to avoid detection.

Perhaps someday this situation will improve here. But current voting systems are only partially tested, and in general unverified, for correct operation.

29. Even if we had correctly operating software, the following fact gives one pause. It is important to realize that *current voting systems are not designed to allow election officials to verify that the software running on their voting systems is indeed the software that is supposed to be running on those voting systems.*

While I was serving on the TGDC, we contemplated rules that would have required voting systems to allow such checks, but abandoned the effort due to their cost and complexity.

There is no way with current scanners and voting systems to easily "read out" the loaded software and confirm that it is the intended software. (And a corrupt system may even lie about what software has been loaded.)

30. One is thus forced to the conclusion that *one can not really trust voting system software very far.* One is reminded of the Reagan maxim, "*Trust but verify.*"

In order to verify that an election outcome is correct, one is forced to abandon putting any trust in the voting system itself, and instead work directly with the "primary inputs" to the election: the cast paper ballots.

31. It is important to note that when the election is close (as WI appears to be), changing just a few votes in every precinct may suffice to swing the election. An attack need not make dramatic changes—it may suffice for the attacker's purpose just to "put one's thumb on the scale a bit".
32. Beyond the general principles enunciated above, there are aspects of the current 2016 U.S. Presidential election that seem sufficient to cause concern, and thus to increase the motivation to double-check that the voting systems have operated correctly.
33. 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. While pre-election polls and post-election polls may seem to some to be particularly suspicious to count as sufficient evidence, for me the best and only real evidence would derive from the examination of the paper ballots via a post-election statistical audit or recount.
34. The extent to which Russian hackers have allegedly attempted to access U.S. election-related systems gives one reason for being especially careful. In the past, vendors and election officials may have felt comfortable that their systems were secure against the "script kiddies" that vandalized insecure computer systems. (A "script kiddie" is an inexperienced hacker who knows only how use attack scripts he has found on the internet.) Being secure today against a sophisticated nation-state is an entirely different matter.
35. A statistical post-election audit (or, if that is impossible, a recount) of the paper ballots provides really the only effective way to determine whether an announced election outcome is correct.
36. It is important to emphasize that an audit or a recount really *must* look at the paper ballots. Otherwise one is not examining the primary election data (the cast ballots themselves) but only derivative secondary data that may have been corrupted by faulty or malicious software.
37. A hand-count of paper ballots, as part of a recount or statistical audit, is the only way to ensure that faulty software has not corrupted the announced election outcome.
38. Re-running the same software on the cast ballots does nothing to help confirm the announced election outcome. One would expect a faulty system running on the same inputs to produce the same faulty outcome.
39. There may be other valid motivations for performing a recount or statistical audit of the paper ballots, such as providing a deterrent to adversaries in the future. For the present purposes, however, one should focus on checking that the announced outcome for the current election is correct.

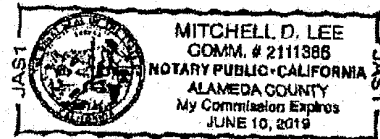
This affidavit was executed on the 28th  
day of November, 2016 in

Berkeley, California

Ronald L. Rivest  
RONALD L. RIVEST

Sworn to before me this 28th day of November, 2016.

[Signature]  
Notary Public



My Commission Expires: Jun 10 2019

**FILED**

**NOV 28 2016**

DANE COUNTY CIRCUIT COURT

**AFFIDAVIT OF HARRI HURSTI**

**16CV3060**

I declare under penalty of false swearing under the law of Wisconsin that the foregoing is true and correct, and that I am physically located outside the geographic boundaries of the United States, Puerto Rico, the United States Virgin Islands, and any territory or insular possession subject to the jurisdiction of the United States.

1. In 2005, I developed the Hursti Hack(s), a series of four tests in which I demonstrated how voting results produced by the Diebold Election Systems voting machines could be altered. I submit this Affidavit in support of a hand recount of all ballots in Wisconsin.

2. I have been a consultant and a co-author of several studies commissioned or funded by various U.S. states and the federal government on computer security. In the area of election security, I am the co-author of several peer-reviewed and state-sponsored studies of election system vulnerabilities. Most notably, I was a co-author of the EVEREST commissioned by the Secretary of State of Ohio (<http://hursti.net/docs/everest.pdf>), a study of vulnerabilities in Sequoia AVC voting machines (<http://hursti.net/docs/princeton-sequoia.pdf>), and a study of the Estonian Internet voting system (<http://hursti.net/docs/ivoting-ccs14.pdf>). I have served as an expert on electronic voting issues in consultations to officials, legislators, and policy makers in five countries. I received the EFFI Winston Smith Award 2008, and the EFF Pioneer Award 2009 for my research and work on election security, data security and data privacy. I recently founded Nordic Innovation Labs to advise governments around the world on election

vulnerabilities. My qualifications and experience are further detailed at the following website:

<https://nordicinnovationlabs.com/team/harri-hursti/>.

### **Opinion**

3. Many of the models of voting machines and other election infrastructure used in Wisconsin were previously analyzed by state-sponsored security reviews, including the EVEREST report (<http://hursti.net/docs/everest.pdf>) commissioned by the Secretary of State Ohio, and were shown to be vulnerable to demonstrated attacks. Due to the shortness of time, I have not been able to verify which of these attacks are feasible on the systems used in one or many of the Wisconsin jurisdictions. It is possible that critical parts of the election infrastructure are processed with equipment which has never been submitted for certification.

4. Optical scan machines can be hacked in a manner that changes election results, and such an attack would likely go undetected during normal pre- and post-election testing. If the scanners are hacked, using them as part of the recount process is likely to result in the same fraudulent election outcome. The only reliable way to detect attacks on the scanners is to recount the paper ballots by hand and compare the results to the electronic tallies.

5. The following attack vectors expose optical scan election results to potential hacking

### **Attacks on Precinct Scanners**

6. Optical scan voting machines can be manipulated by attackers who are able to modify the election-specific settings on the memory card (sometimes called the "mobile ballot box"). Manipulation of the memory card can either be persistent or "one-time", meaning that if the card is reset but not reprogrammed, the card will be "clean" and the hack will not work until the card is reprogrammed again.

7. Optical scan machines can also be attacked by manipulating the software and operating system in their internal memory (which is sometimes also contained on a memory card, though a separate card from the election data). Manipulation of this kind would afford the attacker total control over the system. To recover from such an attack, the software memory would need to be cleanly reprogrammed, or if the software is stored on a removable memory card, that memory card would have to be physically removed from the scanner and replaced with a known-to-be-secure one. Wisconsin recount procedures do not call for these steps to be performed before scanners are used.

#### **Attack on Vote Aggregation**

8. In some jurisdictions only a single report of votes cast is transmitted and/or published. Common practice to accomplish that is to aggregate votes from other machines used in the precinct to a single machine, and that machine is used to report the results. In this case, if the single aggregation machine is attacked, it can influence votes from all the scanners.

9. With certain voting system vendors it is a recommended practice that all optical scan machines be aggregated into a disabled voter DRE machine before reporting. In this setup, the DRE reserved for a low number of disabled voters actually can influence all the optical scan votes too.

#### **Attacks on Election Media Processors**

10. Election media processors are computers which read and/or write many memory cards simultaneously. The EVEREST study cited above found out that a memory card can infect the media processor. An attacker who infects the election media processor in this way can spread the attack to all, or nearly all, scanners that use memory cards written by the processor.

11. Election media processors are typically used by larger jurisdictions and by election services companies that are contracted to program memory cards for many jurisdictions. Attacks on election media processors are therefore likely to affect large numbers of votes.

12. Election media processors have not been certified as of 2008 by the federal Election Assistance Commission or the Federal Election Commission (or, in the case of Ohio by the state), under the legal theory that they are not "vote acting" equipment.

13. These factors make election media processors a particularly dangerous attack vector.

#### **Attacks on High speed Scanners**

14. High-speed scanners are typically used to count ballots from many polling places at a central location. They too face a number of dangerous attack vectors.

15. The controller units of the scanners are typically normal PCs and are subject to a wide array of attacks, including the potential for vote-stealing malware to alter results.

16. The scanner units may be optical mark recognition scanners or digital imaging scanners. Both are hackable. Optical mark recognition scanners can be hacked to misinterpret the ballot and change the recorded vote. A digital imaging scanner can be programmed to manipulate the ballot image. In either case, the recorded vote will not match the voter's intent.

17. There are two major ways high speed scanners are used in an election environment: as scanners producing images into staging areas from which the votes are typically transmitted into a central tabulator over a local area network, or by directly connecting the scanners to a central tabulator.

18. If ballots are transmitted over a local area network, the chain-of-custody of the images is not provable, and images may be manipulated in transmission by network-based attacks.



19. When the scanner is directly connected to the central tabulator, at least one vendor uses special bar codes on the ballots which are commands to the tabulator. Typical commands are "begin batch", "end batch", and "override precinct code". These commands can be transmitted to the machine by ballots that appear under casual human inspection to be normal votes. If an attacker injects them into the set of ballots to be scanned, this can cause real ballots to not be counted, or to be reported in an incorrect jurisdiction.

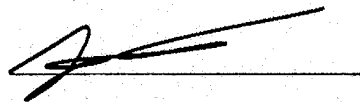
#### **Attacks on Central Tabulators**

20. Central tabulators are normal PCs and are subject to a wide array of attacks, including vote-stealing malware.

21. Tabulator software typically has many features to adjust the vote totals, and these software interfaces can be manipulated by malicious software to alter the reported results.

22. For all these reasons, optical scan votes face a serious threat of being hacked in ways that can alter the outcome of an election. Ballots that are recounted using optical scanners face most of the same threats. The only way to reliably detect such attacks on the election results is to recount the ballots manually, without reliance on potentially hacked election equipment.

Executed on the 28th day of November, 2016 in Helsinki, Finland.

A handwritten signature in black ink, appearing to be 'Harri Hursti', written over a horizontal line.

**HARRI HURSTI**

**16CV3060**

**FILED**

**NOV 28 2016**

**AFFIDAVIT OF DAN S. WALLACH**

**DANE COUNTY CIRCUIT COURT**

DAN S. WALLACH, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is Dan S. Wallach. I am a Professor in the Department of Computer Science and a Rice Scholar at the Baker Institute for Public Policy at Rice University, where I have been for 18 years. My research considers a variety of topics in computer security. I also served as a member of the Air Force Science Advisory Board (2011-2015) and the USENIX Association Board of Directors (2011-2013). I've published over 100 papers in the field. I earned my M.A. (1995) and PhD (1999) from Princeton University, advised by Profs. Edward Felten and Andrew Appel. I earned my B.S. EE/CS from the University of California, at Berkeley (1993). My complete curriculum vita is attached as Exhibit A. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Wisconsin.
2. I've maintained a research interest in electronic voting systems starting with their widespread adoption in the early 2000s. Notably, I served as the director of an NSF-funded multi-institution research center, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), from 2005-2011. I also participated in the 2007 California "Top to Bottom Review" of its electronic voting systems, where we found unacceptable security vulnerabilities in every system we studied<sup>1</sup>; those systems were replaced in California with more secure, paper-based systems but are still being used elsewhere and are likely still quite vulnerable. One of my ongoing projects is helping the Travis County (Austin, Texas) Clerk's office design a new electronic voting system to replace their current, aging system<sup>2</sup>. In short, my experience makes me very familiar with how our election systems are vulnerable, how our adversaries might seek to exploit them, and how we can engineer better election systems for the future.
3. My main message is that our election systems face credible cyber-threats generally, and in this election year those threats are magnified in light of the persuasive evidence of state-sponsored attacks against our elections. Recounts and audits, particularly in tight races, are appropriate measures to take against these threats.

---

<sup>1</sup> <http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/>

<sup>2</sup> <https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell>

## Background and threat analysis

4. In September 2016, I was invited by the Congressional Space, Science, and Technology Committee to testify about possible cyber threats against our elections.<sup>3</sup> At the time, my primary concern was attacks against voter registration databases, driven by news reports of nation-state attacks against these facilities in at least two states (Arizona and Illinois). I was and remain concerned as well about attempts to tamper with other computers systems, including those facing the voter (precinct-based optical ballot scanners and/or paperless electronic voting systems) as well as those used to do vote tabulation and reporting. I am including my Congressional testimony and post-testimony questions & answers as Exhibits B and C<sup>4</sup>. My testimony speaks to the possible motives and capabilities of our nation-state adversaries toward attacking our election systems and the defenses that we have in place as well as what sort of contingency planning might be appropriate in light of these threats. I'm including some excerpts from my testimony below:
5. **How serious is the threat?** We've learned that foreign nation-state actors, likely Russian, broke into DNC computers and released documents for expressly partisan purposes<sup>5</sup>. So far as we know, they did this to manipulate the outcome of November's election. We must ask ourselves the same sorts of questions that arise in any security analysis. Does the adversary have the *means, motive, and opportunity* to have their desired effect, and do we have the necessary *defenses* and/or *contingency plans* to mitigate these threats?
6. **This has happened in elections before.** Russian hackers, who may or may not have been government-affiliated, committed "wanton destruction" upon Ukrainian election systems in 2014, arranging for the vote tallying system to report incorrect results<sup>6</sup>. The Ukrainians were lucky to catch this; it's not uncommon for nation-state computer attacks to go unnoticed for months or years. Like the Ukrainians in 2014, we face similar vulnerabilities today.

---

<sup>3</sup> My written testimony:

<https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf>

My written answers to questions posed afterward:

<http://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-qa-17oct2016.pdf>

<sup>4</sup> <http://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-13sept2016.pdf>

<http://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-qa-17oct2016.pdf>

<sup>5</sup> See, e.g., Lichtblau's article in the *New York Times* (July 29, 2016).

<http://www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html>

<sup>6</sup> Clayton, "Ukraine election narrowly avoided wanton destruction from hackers", *Christian Science Monitor* (June 2014),

<http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video>

7. **Can our adversaries get malware into our voting machines, or our vote tabulation**

**computers?** The U.S. military protects its important secrets by keeping them on distinct networks and servers, physically separated from the Internet. This “air gap” defense is also used to protect voting machines. Despite this, voting machines still interact with normal computers as part of their initialization phase (loading software and ballot definitions) and the tabulation phase (extracting cast-vote records and computing the totals); these computers are not necessarily “air gapped” (see Paragraph 11, below). Even if the whole process is designed to be “air gapped” from the Internet (and it absolutely must be air-gapped), nation-state adversaries have devised a variety of workarounds. The Stuxnet malware, for example, was engineered specifically to damage nuclear centrifuges in Iran, even though those centrifuges were never connected to the Internet. We don’t know exactly how the Stuxnet malware got in, but it did nonetheless<sup>7</sup>.

Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems, and especially if we consider the possibility of insider threats, then yes, it’s entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries’ capabilities. The best mitigations we have for systems that we use today are only feasible where we have paper ballots. The mere *possibility* of a recount or audit of the paper ballots acts as a deterrent to an electronic attack; it’s much more difficult to tamper with paper, in bulk, relative to the effort to tamper with purely electronic records as used in many states (but not Wisconsin).

8. **Does an adversary need to attack everywhere?** Our adversaries understand how the American political system works. They know about “battleground states”. They can focus their efforts on states where a small nudge might have a large impact. Wisconsin has one of the smallest margins of victory in the Presidential race. This makes it a logical target.

**Vote tabulation, auditing, and recounting: Validating the correct winner of the race**

9. I wish to tackle a seemingly straightforward question: if there’s a risk that a nation-state attacker might have compromised some or all of the computers used in Wisconsin’s election systems, what steps might be appropriate to mitigate against such threats and ensure a correct election tally?
10. The bulk of Wisconsin votes were marked by hand on paper, and tabulated through electronic systems. What if those electronic tabulation systems were corrupt? Manual (hand) tabulation can

---

<sup>7</sup> For more details, see, e.g., Langner et al. (2013).

<http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>

validate the correctness of the electronic tally, since no amount of electronic tampering can overwrite paper ballots in a ballot box nor can electronic tampering compromise a team of human tabulators.

11. Why not just conduct an electronic tally? While many election officials maintain that there is “no way” their computers could have been electronically tampered, this is inconsistent with the skills available to our nation-state adversaries. For example, we know that “ballot programming” and other forms of electronic information regularly cross any “air gap” there might be around an election administrator’s computer. “Ballot programming” is the process of defining all of the candidates and races for a given election, and copying that data to the voting machines, precinct-count optical scanners, and the back-end tabulation computers. While copied around on USB sticks or other kinds of storage devices, those storage devices can also serve as a conduit for malware. (Back in the days before the Internet, PC viruses spread in exactly this fashion.)
12. It’s also a common and undesirable practice for election administrators to have their computers behind a network firewall of some sort, which is to say, there’s no actual air in the air gap. So long as there are wires between the Internet and an election administration computer, then there’s an opportunity for an adversary to break the firewall and attack the computers behind it. (Adversarial techniques to breach network firewalls are widely known to nation-state cyber attackers.)
13. Can an attacker compromise the computer inside of a precinct-based optical scanner? Unfortunately, this is well within the capabilities of a nation-state attacker. These computers are potentially vulnerable to malware that can be introduced as part of the pre-election ballot programming, wherein malware might hitch a ride along with legitimate ballot data being loaded into the scanner. There might be other vulnerabilities as well. Similar vulnerabilities were discovered as part of the California “Top to Bottom” review and the Ohio “EVEREST” studies, and we have no reason to believe that election equipment vendors have taken the engineering steps to defend against this class of attacker.
14. A purely electronic tally of paper ballots, without some sort of hand-counting or auditing would be unable to detect systematic electronic tampering--the very risk we’re concerned about in this election.

15. I have advocated and continue to support the use of “risk-limiting audits,”<sup>8</sup> which have been piloted in California, Ohio, and Colorado.<sup>9</sup> In short, by selecting a small number of ballots at random and then comparing the physical paper ballot with its electronic analogue, we can reach a very high degree of statistical confidence in the correctness of the election outcome. A risk-limiting audit samples a suitable number of ballots to ensure that there is no systematic error large enough to change the outcome. However, as a pragmatic matter, a risk-limiting audits is not an alternative to the full hand recount that I believe is appropriate here. Because risk-limited audits are not currently a standard practice in Wisconsin, their introduction would require some effort to agree on suitable procedures, to implement those procedures, and to train staff on those procedures to ensure the audit occurs properly. It is unlikely such procedures can be developed and implemented in the short time period at issue here.
16. I understand that a relatively small fraction of Wisconsin voters cast their ballots electronically, using touch-screen computers rather than hand-marked paper ballots, and that Wisconsin’s touch-screen devices include a printed paper trail which the voter sees while voting. Such “voter verifiable paper audit trails” (VVPAT) provide an opportunity to verify the correctness of the electronic results. It’s already the standard procedure in Wisconsin to examine these VVPAT printouts manually during a recount, which mitigates against electronic corruption or tampering in the voting machine in the same way that examining hand-marked paper ballots by hand mitigates against electronic corruption or tampering in the optical scanner and tabulation system.

#### **Intent of the voter and the accuracy of a recount**

17. Even aside from the concerning issue of computer hacking, a hand recount is important to determine the “intent of the voter,” even if the voter did not correctly mark his or her ballot. While most voters indeed follow the instructions, many don’t.
18. There are many circumstances where an optical scanner will accept a ballot that might otherwise be rejected. For example, if the voter signed or otherwise made personally distinguishing marks on his or her ballot, then the ballot should be properly removed from the tally, yet optical scanners will still accept it. (Ballots must be anonymous, otherwise voters will be subject to bribery or coercion.) Similarly, a voter might have filled in the bubble for one candidate, recognized the error, and then drawn arrows to indicate that a different candidate was his or her

---

<sup>8</sup> See, e.g., <https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf>  
[http://www.commoncause.org/democracy-wire/new-post-election-audits-promise-more-accurate-election-res](http://www.commoncause.org/democracy-wire/new-post-election-audits-promise-more-accurate-election-results.html)  
[ults.html](http://www.commoncause.org/democracy-wire/new-post-election-audits-promise-more-accurate-election-results.html)

<sup>9</sup> [http://bcn.boulder.co.us/~neal/elections/corla/Risk-Limiting\\_Audit\\_Report-Final\\_20140331.pdf](http://bcn.boulder.co.us/~neal/elections/corla/Risk-Limiting_Audit_Report-Final_20140331.pdf)

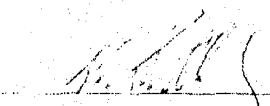
preference. In these cases, a machine will have difficulties determining the "intent of the voter." Only a human vote counter can make these judgments. Other issues that might confuse a scanner include "stray marks" which a scanner sees and a human observer would clearly discount.

19. Broadly speaking, a human ballot tabulator can learn a voter's style, i.e., how they typically fill in bubbles. If most bubbles are marked in a heavy hand, it's easier to reject a light "stray mark" that a machine might otherwise count. If, on the other hand, all the bubbles are marked with light single lines, a machine might not see any of them and treat the whole ballot as if nothing were marked. A human tabulator would know that the voter used this specific style and would be able to correctly interpret the voter's intent where a machine could not.
20. The correct interpretation of voter intent for individual ambiguous ballots became a point of contention in Minnesota's 2008 Senate race between Al Franken and Norm Coleman<sup>10</sup>, and similar issues might be important this year in Wisconsin as well.
21. *By conducting manual tallies, a recount will produce a tally that more accurately represents the intent of Wisconsin's voters than an electronic tally. A manual tally is particularly necessary here given the concerning evidence of Russian-sponsored hacking and the vulnerabilities of our election machinery. Luckily, Wisconsin is a state that has paper records of each vote which can be used to verify the election results. I believe the only appropriate recount in this circumstance is one that manually tallies those paper records.*

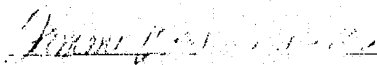
---

<sup>10</sup> [http://minnesota.publicradio.org/features/2008/11/19\\_challenged\\_ballots/](http://minnesota.publicradio.org/features/2008/11/19_challenged_ballots/)

This affidavit was executed on the 28th day of November, 2016 in Houston, Texas.

  
\_\_\_\_\_  
DAN S. WALLACH

Sworn to before me this 28th day of November, 2016.

  
\_\_\_\_\_  
Notary Public

My Commission Expires: 3-10-19

