

IN THE SUPERIOR COURT OF FULTON COUNTY

STATE OF GEORGIA

DONNA CURLING, an individual; DONNA PRICE, an individual; ROCKY MOUNTAIN FOUNDATION, INC., a non-profit corporation organized and existing under Colorado law,

Plaintiffs,

v.

BRIAN P. KEMP, in his official capacity as Secretary of State of Georgia; RICHARD BARRON, in his official capacity as Director of the Fulton County Board of Elections and Registration; MAXINE DANIELS, in her official capacity as Director of Voter Registrations and Elections for DeKalb County; JANINE EVELER, in her official capacity as Director of the Cobb County Board of Elections and Registration,

Defendants.

CIVIL ACTION FILE

NO. 2017CV290630

PLAINTIFFS' EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AND INTERLOCUTORY INJUNCTION, WITH SUPPORTING LEGAL AUTHORITY

COME NOW Plaintiffs in the above-styled case, by and through the undersigned counsel, pursuant to O.C.G.A. § 9-11-65(b) and Uniform Superior Court Rule 6.7, and file this Emergency Motion for Temporary Restraining Order and Interlocutory Injunction, With Supporting Legal Authority, seeking a Court Order restraining and enjoining Defendants Barron, Daniels, and Eveler from using Georgia's federally uncertifiable, unsafe, and inaccurate Direct Recording Electronic ("DRE") voting equipment and its related voting system ("Georgia's DRE-Based Voting System") to conduct the imminent June 20, 2017, runoff (the "Runoff") for the 2017 Special Election in Georgia's Sixth Congressional District in their respective Counties; and requiring these Defendants instead to comply with O.C.G.A. § 21-2-334 and O.C.G.A. § 21-2-

281 by conducting the Runoff using hand-counted paper ballots in the manner provided in O.C.G.A. § 21-2-334 and O.C.G.A. § 21-2, Article 11, Part 2.

STATEMENT OF FACTS

As factual support for this Motion, Plaintiffs rely upon their Verified Complaint for Declaratory and Injunctive Relief and Writ of Mandamus (the “Complaint”), with Exhibits 1–4, filed in this case; and the supplemental Exhibits 5–8 attached hereto.¹ Background facts are thus those that are set forth in the Complaint and in the following documents:

- Exhibit 1: The May 10, 2017, letter sent by a group of Georgia electors to Defendant Kemp, requesting his reexamination of Georgia’s DRE-Based Voting System pursuant to O.C.G.A. § 21-2-379.2(a). Exhibit 1 at 1–6. This Exhibit 1 includes four of its own attachments:
 - Attachment A, (Ex. 1 at 7–9)—the March 15, 2017, letter sent by twenty-one prominent computer scientists inquiring about the FBI’s then-ongoing investigation into a cyberattack on KSU’s Center for Election Systems’ website;
 - Attachment B (Ex. 1 at 10–16)—a peer-reviewed scholarly article examining design issues in relation to the election management software used in Georgia’s DRE-Based Voting System;
 - Attachment C (Ex. 1 at 17–32)—a peer-reviewed scholarly article discussing a security analysis of the Diebold AccuVote-TS voting machine used in Georgia’s DRE-Based Voting System; and

¹ The exhibits attached to this Motion supplement Exhibits 1-4 that were attached to the Verified Complaint for Declaratory and Injunctive Relief and Writ of Mandamus. Accordingly, the first exhibit referenced in this motion and brief is numbered Exhibit 5.

- Attachment D (Ex. 1 at 33)—software versions understood to be currently used in Georgia’s DRE-Based Voting System.
- Exhibit 2: The May 17, 2017, follow-up letter sent to Defendant Kemp by Duncan A. Buell, the technical adviser to the group of Georgia electors who requested reexamination of Georgia’s DRE-Based Voting System. Ex. 2 at 1–6. This Exhibit 2 includes three of its own sub-exhibits:
 - Exhibit A (Ex. 2 at 7–12)—an Incident Report describing the response by KSU’s Center for Election Systems (“CES”) to an intrusion on CES’s systems server that occurred on March 1, 2017, resulting in a data breach affecting voter registration information of 6.7 million individuals.
 - Exhibit B (Ex. 2 at 13–16)—U.S. Election Assistance Commission Advisory 2005-004, explaining how to determine whether a voting system complies with audit capacity requirements in the Help America Vote Act.
 - Exhibit C (Ex. 2 at 17–18)—Fulton County’s letter to the Rocky Mountain Foundation, Inc., requesting advance payment of \$26,000 in order to produce documentation related to Georgia’s DRE-Based Voting System responsive to an Open Records Request.
- Exhibit 3: The May 24, 2017, letter sent to Defendant Kemp by sixteen computer scientists to follow up on the concerns previously expressed and raising concerns about problems with Georgia’s DRE-Based Voting System experienced by Fulton County election officials during the April 18, 2017, Special Election.
- Exhibit 4: A partial transcription of Defendant Barron’s explanation of the April 18 problems to the Fulton County Board of Commissioners.

In further support of the Motion, Plaintiffs also provide:

- Exhibit 5: The Affidavit of Duncan A. Buell (“Buell Aff.”), in which Dr. Buell states, among other things: “[T]he security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems.” Buell Aff., attached hereto as Exhibit 5,² at 4 ¶ 11. Moreover, Dr. Buell attests that, “[A]ll analyses of the ‘standard’ Diebold election system have found major flaws,” a fact that “should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.” *Id.*;
- Exhibit 6: The Affidavit of Edward W. Felten, in which Dr. Felten describes his study of the Diebold voting machines that are core components of Georgia’s DRE-Based Voting System, including the vulnerabilities of those particular machines to malicious software viruses; their susceptibility to surreptitious modification of software by anyone with physical access to the equipment; and the significant vulnerabilities inherent in the design of the equipment, which are not capable of mitigation. Ex. 6 (attached hereto) at 2–5 ¶¶ 4–27;
- Exhibit 7: The Affidavit of Virginia Martin, in which Ms. Martin describes the process of hand counting paper ballots and concludes based on the turnout observed at the April 18 Special Election that, if the Runoff had similar turnout, its results could be tabulated by hand counting of paper ballots in just one and a half hours or less. Ex. 7 (attached hereto) at 2 ¶ 13; and

² The exhibits attached to this brief supplement the exhibits attached to the Verified Complaint for Declaratory and Injunctive Relief and Writ of Mandamus. Accordingly, the first exhibit referenced in this motion and brief is numbered Exhibit 5.

- Exhibit 8: KSU Presentation describing the components and functioning of Georgia’s DRE-Based Voting System. Ex. 8 (attached hereto).

The facts provided to this Court in the foregoing documents show that Georgia’s DRE-Based Voting System suffers from widely known security vulnerabilities. They also show that, this Spring, KSU’s voter registration database was hacked; electronic pollbooks containing voters’ personal identifying information were stolen; system errors occurred during the conduct of the April 18, 2017, Special Election tabulation in Fulton County using Georgia’s DRE-Based Voting System, and these system errors are still under investigation. Ex. 5, Buell Aff., at 5–6 ¶¶ 14–17. Finally, KSU’s CES facility has been revealed by a peer department’s incident review report to be alarmingly deficient in physical security and cybersecurity applicable to Georgia’s DRE-Based Voting System. Ex. 2, at 7–12 (Ex. A). Together with the general environment of escalating cybersecurity threats, such problems have alarmed the public and created widespread public doubt about the integrity of any election conducted using Georgia’s DRE-Based Voting System.

Plaintiffs reserve the right to provide supplemental evidentiary support for this motion.

ARGUMENT

I. Plaintiffs Are Entitled To A TRO And Interlocutory Injunction

A. Legal Standard

“Although an interlocutory injunction is an extraordinary remedy, and the power to grant it must be ‘prudently and cautiously exercised,’ the trial court is vested with broad discretion in making that decision.” *SRB Inv. Servs., LLLP v. Branch Banking & Trust Co.*, 289 Ga. 1, 5, 709 S.E.2d 267, 271 (2011) (internal quotation marks omitted). Among the factors a trial court considers in deciding whether to grant an interlocutory injunction are whether:

(1) there is a substantial threat that the moving party will suffer irreparable injury if the injunction is not granted; (2) the threatened injury to the moving party outweighs the threatened harm that the injunction may do to the party being enjoined; (3) there is a substantial likelihood that the moving party will prevail on the merits of her claims at trial; and (4) granting the interlocutory injunction will not disserve the public interest.

Holton v. Physician Oncology Servs., LP, 292 Ga. 864, 866, 742 S.E.2d 702, 704 (2013) (internal citations omitted). Applying these factors here, Plaintiffs are entitled to and should be granted temporary and interlocutory injunctive relief.

B. Irreparable Injury

Plaintiffs show this Court that each of Plaintiff Curling and the Georgia elector members of Plaintiff RMF who reside in Georgia's Sixth Congressional District will be irreparably harmed in the exercise of their constitutional, fundamental right to vote in the Runoff if Defendants Barron, Daniels, and Eveler are not enjoined from using Georgia's DRE-Based Voting System to conduct the Runoff.

C. Threatened Injury To Plaintiffs Outweighs Harm Any Injunction May Do To Defendants Barron, Daniels, And Eveler

The balance of equities favors the entry of a TRO and interlocutory injunction because the harm to Plaintiffs of allowing the Runoff to be conducted using a demonstrably unsafe and inaccurate voting system is irreparable, whereas there is no harm at all to Defendants Barron, Daniels, and Eveler from being required to conduct the Runoff using hand-counted paper ballots in the manner that Georgia law—specifically O.C.G.A. § 21-2-334 and O.C.G.A. § 21-2, Article 11, Part 2—already contemplates and permits in circumstances where the use of voting equipment is impracticable for any reason.

D. Plaintiffs' Substantial Likelihood of Success On The Merits

Plaintiffs are likely to succeed on the merits of their claims for injunction based on the facts set forth in the Complaint because Georgia's DRE-Based Voting System suffers from widely known, severe safety and accuracy concerns that cannot be timely mitigated. Recent events have revealed to the public the previously unknown severity of pre-existing security issues. This Spring, KSU's voter registration database was hacked; electronic pollbooks containing voters' personal identifying information and software for managing DRE voter access cards were stolen; system errors occurred during the April 18, 2017, Special Election tabulation in Fulton County, which is still under investigation; and KSU's CES facility was revealed by a peer department's incident review report to be alarmingly deficient in security. Together with the general environment of escalating cybersecurity threats, such problems have alarmed the public and render the use of the system at the Runoff to be "not practicable" within the meaning of O.C.G.A. § 21-2-334 and "impracticable" within the meaning of O.C.G.A. § 21-2-281.

E. Granting An Injunction Will Not Disserve The Public Interest

Granting the Plaintiffs injunctive relief will not disserve the public interest, but will rather promote it, by ensuring that the Runoff is not conducted using a voting system that exposes the voters to a real and unacceptably high risk that the result of the Runoff could be compromised by undetectable malfunctions or by malicious actors able to exploit the system's vulnerabilities. Hand counting the votes using paper ballots is necessary for the public to have confidence in the integrity of the Runoff's result, given the public's awareness of recent system problems and security breaches related to Georgia's DRE-Based Voting System.

II. Good Cause Exists For Emergency Proceeding

This Motion is filed as an emergency motion under Uniform Superior Court Rule 6.7 because the commencement of voting in the Runoff is imminent, with advance voting beginning on Tuesday, May 30, 2017.

III. Conclusion

WHEREFORE, Plaintiffs move this Court for a temporary restraining order and an interlocutory injunction restraining and enjoining Defendants Barron, Daniels, and Eveler from using Georgia's DRE-Based Voting System to conduct the Runoff and requiring them instead to comply with O.C.G.A. § 21-2-334 and O.C.G.A. § 21-2-281 by conducting the Runoff using hand-counted paper ballots in the manner provided in O.C.G.A. § 21-2-334 and O.C.G.A. § 21-2, Article 11, Part 2.

Respectfully submitted this 26th day of May, 2017.

/s/ Edward B. Krugman

Edward B. Krugman
Georgia Bar No. 429927
Robert L. Ashe, III
Georgia Bar No. 208077

BONDURANT, MIXSON & ELMORE, LLP
3900 One Atlantic Center
1201 W. Peachtree Street
Atlanta, Georgia 30309
Telephone: 404-881-4100
Facsimile: 404-881-4111
krugman@bmelaw.com
ashe@bmelaw.com

/s/ Robert A McGuire, III

Robert A. McGuire, III
Pending Application for Admission *Pro Hac Vice*

ROBERT MCGUIRE LAW FIRM
2703 Jahn Ave NW, Suite C-7
Gig Harbor, Washington 98335

Telephone: 253-313-5485
Facsimile: 866-352-1051
ram@lawram.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on this day I caused to be served a true and correct copy of the foregoing PLAINTIFFS' EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AND INTERLOCUTORY INJUNCTION, WITH SUPPORTING LEGAL AUTHORITY by filing same with the Court's electronic case management system and also via email upon the following parties:

Brian P. Kemp
Secretary of State of Georgia
214 State Capitol
Atlanta, GA 30334
RHerron@sos.ga.gov

Richard Barron
Director, Fulton County Board of Elections and Registration
130 Peachtree Street, NW
Suite 2186
Atlanta, GA 30303
Richard.Barron@FultonCountyGa.gov

Maxine Daniels
Director of Voter Registrations and Elections for DeKalb County
4380 Memorial Drive
Suite 300
Decatur, GA 30032
MWDaniels@DeKalbCountyGa.gov

Janine Eveler
Director of the Cobb County Board of Elections and Registration
736 Whitlock Avenue, NW
Suite 400
Marietta, GA 30064
Janine.Eveler@CobbCounty.org

Daniel W. White, Esq.
HAYNIE, LITCHFIELD, CRANE & WHITE, PC
222 Washington Avenue
Marietta, GA 30060
dwhite@hlclaw.com

Overtis Hicks Brantley, Esq.
DEKALB COUNTY LAW DEPARTMENT
1300 Commerce Drive
Fifth Floor
Decatur, GA 30030
OvBrantley@DeKalbCountyGa.gov

Christopher Carr, Esq.
GEORGIA ATTORNEY GENERAL
40 Capitol Square, SW
Atlanta, GA 30334
CCarr@law.ga.gov

Deborah Dance, Esq.
COBB COUNTY ATTORNEY'S OFFICE
100 Cherokee Street
Suite 350
Marietta, GA 30090-9689
DDance@CobbCounty.org

Patrise M. Perkins-Hooker, Esq.
FULTON COUNTY ATTORNEY'S OFFICE
141 Pryor Street, SW
Suite 4038
Atlanta, GA 30303
Patrise.Hooker@FultonCountyGa.gov

This 26th day of May, 2017.

/s/ Robert L. Ashe III
Robert L. Ashe III
Georgia Bar No. 208077

EXHIBIT 5

AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of petitions to consider the use of the electronic voting machines in Georgia Congressional District 6 (CD 6) unacceptable based on substantive concerns about security and reliability.

2. In my opinion, the Diebold electronic voting system used by CD 6, is vulnerable to malicious interference and inadvertent error. The Diebold system in general has been put under technical scrutiny several times by technical experts, and each time there have been multiple concerns raised about security and reliability. The possible stamp of approval (for a modified system?) given by the Kennesaw State University (KSU) Center for Election Systems (CES) does not in my opinion mitigate for use in Georgia the known flaws of the system, especially given that the response to the reported hack in Spring 2017 of the CES has not satisfactorily been addressed.

Qualifications and Relevant Employment History

3. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at <http://www.cse.sc.edu/duncanbuell>.

4. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

5. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the U.S. intelligence community.

6. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

7. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

8. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity¹ software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued, in that when the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well.

Basis for My Opinions

9. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

10. I have also used for my opinions a review of the documents surrounding the KSU CES hack in Spring 2017, including the report attached to an email on 24 April 2017 from Stephen Gay to Merle King.

The Diebold Election System Is Unacceptable for Use in the CD6 Election to Be Held 20 June 2017

11. I begin with the fact that the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems. The letter from Georgia citizens to Secretary of State (SoS) Brian Kemp on 10 May 2017 cites the security analysis of Feldman, Halderman, and Felten. The GEMS central server software analysis by Ryan and Hoke, cited in the same letter, shows flaws in the central server. The fact that all analyses of the “standard” Diebold election system have found major flaws should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.

12. It has been well-established in the computer security world that the Diebold election system, as configured for “standard” use, is unfit for use due to security and

reliability concerns. It is not clear to what extent the KSU CES might have modified the “standard” Diebold system (with or without going through the process of federal approval and certification). In my letter/request to Secretary Kemp, serving as a technical advisor to the citizens of Georgia who had petitioned for the non-use of the Diebold systems in the 20 June 2017 election, I asked for responses to the questions of security and reliability. If the standard system had been modified by CES, and that system had been re-certified, and one could rely upon the security credentials of the KSU CES, then one might have some limited confidence in the suitability of the Diebold system for use in elections in Georgia.

13. I have so far received no response from the SoS office. I have, however, seen sufficient documentation to continue my concerns about the suitability and reliability of the Diebold system for use in elections in Georgia.

14. To be specific, the report of 18 April 2017, attached to Mr. Gay’s email to Merle King, is damning in what it says and what it does not say. What we see as “successes” are only that the response to a security incident went well. This is essentially the statement that when law enforcement officials arrived at the barn, they found the door closed, and they found no horses inside the barn, but they had arrived quickly.

15. We see a number of issues in the 18 April 2017 report that indicate that the KSU CES security protocols were insufficient, and we find no commentary on any of those protocols that might have mitigated the damage.

16. I do not see that there are technical comments about successful, or positive, security measures that would have mitigated the damage done by the hack to the CES.

17. We come to the bottom line. We know, because it has been shown repeatedly, that the Diebold system as it is standardly configured, has major flaws. We would believe, based on our knowledge of process in Georgia, that it is the responsibility of the KSU CES to mitigate (or perhaps even remove?) these major flaws. But we do not see, in the report regarding the operational practices of the CES, that there is reason to believe that they have in fact mitigated the known flaws, produced a system that has been federally certified, and provided to the citizens of Georgia an election system in which they can be confident.

18. For these reasons I would argue that the Diebold system ought not be used in the 20 June 2017 CD6 election.

19. I affirm that the foregoing is true and correct.

Duncan Buell 25 May 2017
DUNCAN BUELL Date

Sworn before me this 25 day of May, 2017, in Richland County, S.C.

Donna S. Moses
NOTARY PUBLIC

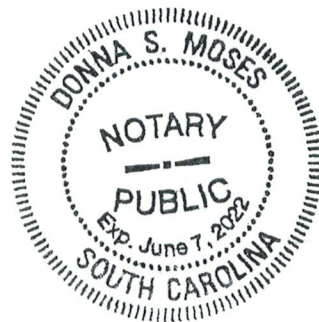


EXHIBIT 6

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual;)
)
DONNA PRICE, an individual;)
)
ROCKY MOUNTAIN FOUNDATION,)
INC., a non-profit corporation organized)
and existing under Colorado law;)
)
Plaintiffs,)

v.)

CIVIL ACTION
FILE NO.:

BRIAN P. KEMP, in his official capacity)
as Secretary of State of Georgia;)
)
RICHARD BARRON, in his official)
capacity as Director of the Fulton County)
Board of Elections and Registration;)
)
MAXINE DANIELS, in her official)
capacity as Director of Voter Registrations)
and Elections for DeKalb County;)
)
JANINE EVELER, in her official)
capacity as Director of the Cobb County)
Board of Elections and Registration;)
)
Defendants.)

AFFIDAVIT

County of Mercer)
) ss.
State of New Jersey)

EDWARD W. FELTEN ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the Director of Princeton's Center for Information Technology Policy. I received my Ph.D. in Computer Science and Engineering from the University of Washington in 1993. I am a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

2. From 2015 until January 2017, I served in the White House as Deputy United States Chief Technology Officer. During that time I advised the President and his senior advisors on policy issues relating to computer science, including issues relating to the security and reliability of elections and electronic voting systems.

3. A copy of my curriculum vitae is attached as Exhibit A.

Inherent risks of paperless electronic voting machines

4. Before turning to the specific systems and circumstances of this matter, I will provide a brief summary of cybersecurity issues relating to voting machines.

5. The voting machines at issue in this matter are a type of so-called Direct Recording Electronic (DRE) machine. DREs are voting machines that are designed to record a voter's ballot directly in electronic storage, without creating any record of the ballot that can be directly verified by the voter.

6. DREs can be contrasted with other voting technologies in which there is a record of the voter's ballot, typically on paper, the accuracy of which can be verified directly by the voter in the polling place, and which is collected at the polling place as a record of the voter's intent. The most common examples of voter-verifiable ballots include paper ballots. The simplest way to tabulate paper ballots is by hand counting.

7. The lack of a voter-verifiable ballot creates special risks associated with any DRE voting system. For this reason, computer scientists and cybersecurity experts typically recommend against the use of DREs. I concur with this general recommendation against the use of DREs.

8. The hardware of a DRE—the physical equipment comprising the computer—is much like a standard desktop computer, often installed into a different physical enclosure. Like a standard computer, a DRE will do whatever the software installed in it directs it to do. If anyone changes the software, whether through malice or error, the DRE may do something other than accurately recording and tabulating votes.

9. A malicious modification to a DRE's software would likely cause the DRE to modify ballots silently. The modified software could be designed to report on the machine's display screen, to voters and election officials, that all was well. It could also be designed to falsify all of the logs and records kept by the voting machine.

10. My students and I have modified the software on many types of DREs. For example, my students modified a (now decommissioned) New York DRE to turn it into a kiosk for playing the popular arcade game Pac-Man. We have also created, installed, and tested software for multiple DRE models that would silently modify election results. (For obvious reasons, these latter tests were done in secure laboratories.)

My team's study of Diebold voting machines

11. I led a team of researchers that studied the Diebold AccuVote TS voting machine system. We published a peer-reviewed paper summarizing our analysis, which is attached as Exhibit B.

12. As part of our research we demonstrated that it was possible to create a voting machine virus: a computer virus that infected the voting machines, spreading from machine to machine by infecting the memory cards that are used to transport election and ballot information between the machines and central tabulation offices. The virus, having infected a voting machine, would modify election results, without leaving any trace in the logs or records kept by the machine. We created and tested such a virus in our secure laboratory.

13. I did a live demonstration of this election-stealing virus, including showing the casting of votes and mis-reporting of the vote counts by the machine, during live testimony at a hearing of a committee of the U.S. House of Representatives. My students and I did a similar demonstration twice on live television, on CNN and Fox News.

14. The TS machine we studied allowed modified (and possibly malicious) software to be installed by anyone who could open a small metal access door on the side of the machine. The door was locked by an ordinary file cabinet type of lock. Because the very same key that is used for the access door on the AccuVote TS is also used widely on office furniture, jukeboxes, and hotel minibars, the keys are easily purchased. I bought a gross of these keys (i.e., 144 keys) from a vendor on the Internet. The lock is also easily picked—a member of our team who studies locks as hobby was able to pick the access door lock consistently in less than 15 seconds.

15. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes.

16. Our peer reviewed paper listed a number of other security problems with the AccuVote TS system. Some of these problems could in principle be fixable by improving the software of the TS, but others are inherent in the machine's hardware and therefore not fixable by any software update.

17. As described in our peer reviewed paper, it is inherent in the hardware design of the TS that a person who can get physical access to the inside of the machine can install any software they like on the machine.

18. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes. This problem is inherent in the hardware design of the TS machine.

19. Subsequent to the publication of our paper, we studied the AccuVote TSX system and found that it had similar security problems.

Need for software verification

20. One cannot know that any DRE machine, including a TS or TSX, will accurately record or tabulate votes, unless one is certain as to which software is installed on that machine. Because of the ease of malicious modification of the software, it is not enough to know which software is supposed to be installed—one must inspect the machine to verify which software is actually installed.

21. Verifying which software is actually installed is technically very difficult, because one cannot rely on the software itself to report its own status accurately. Malicious software can simply misreport its own status, reporting that everything is normal. Relying on the software to report whether it has been tampered with is like trying to determine whether a person is honest by asking him, “Are you honest?” An answer of “yes” is not reliable evidence.

22. Unfortunately, the standard methods for inspecting the software version installed in a machine rely on the machine’s software in one way or another, so they fail to avoid this pitfall and should not be trusted. Special protocols, typically involving the use of specialized equipment, must be designed and used to perform such inspections, and rigorous chain-of-custody controls are necessary after the inspection to make sure no tampering with the machine’s software could have occurred after the inspection.

23. Unless all of these steps are followed, with respect to a particular DRE machine, one cannot be confident in its ability to accurately record or tabulate votes.

Need for secure facilities

24. I understand that Georgia voting machines are tested and configured in the Center for Election Systems (CES) at Kennesaw State University (KSU). Because my team’s research has demonstrated the propagation of malicious software during these types of activities, any security breach at CES, or failure to implement adequate cybersecurity precautions at CES, could have created an opportunity for a malicious party to modify software in voting machines and related systems.

25. The security breach at CES, and KSU’s response to it, are indications that cybersecurity precautions at CES may not have been adequate. It is especially significant that KSU’s response to the breach included steps to change how cybersecurity and system administration were managed at CES, so that CES personnel were no longer managing these functions on their own.

26. The most sophisticated cyberattackers are especially skilled not only at gaining unauthorized access to systems, but also at maintaining access. So-called Advanced Persistent Threat actors specialize in gaining access and maintaining that access over time, while avoiding detection and waiting for the best moment to strike. Once they are in a system, it can be

extraordinarily difficult to find them. As a result, very stringent measures may be necessary to render a facility safe after a period of vulnerability—and especially when highly skilled actors may have been motivated to compromise that facility.

27. Because of the vulnerability of the DRE voting machines to software manipulation, and because of intelligence reports about highly skilled cyber-actors having attempted to affect elections in the United States, such precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism.

28. Further Affiant sayeth not.

 May 26, 2017
Edward W. Felten



EMMA MARSHALL
NOTARY PUBLIC OF NEW JERSEY
I.D. # 2434585
My Commission Expires 5/30/2018

Edward W. Felten

Education

Ph.D. in Computer Science and Engineering, University of Washington, 1993.

Dissertation title: "Protocol Compilation: High-Performance Communication for Parallel Programs." Advisors: Edward D. Lazowska and John Zahorjan.

M.S. in Computer Science and Engineering, University of Washington, 1991.

B.S. in Physics, with Honors, California Institute of Technology, 1985.

Employment

Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University, 2013-present

Deputy United States Chief Technology Officer, The White House, Office of Science and Technology Policy, 2015-2017

Professor of Computer Science and Public Affairs, Princeton University, 2006-2013.

Chief Technologist, U.S. Federal Trade Commission, 2011-2012.

Professor of Computer Science, Princeton University, 2003-2006.

Associate Professor of Computer Science, Princeton University, 1999-2003.

Assistant Professor of Computer Science, Princeton University, 1993-99.

Senior Computing Analyst, Caltech Concurrent Computing Project, California Institute of Technology, 1986-1989.

Director, Center for Information Technology Policy, Princeton University, 2005-present.

Elysium Digital LLC and various law firms. Consulting and expert testimony in technology litigation, 1998-2015

U.S. Federal Trade Commission: consulting regarding spam policy and investigation, 2004, 2006.

U.S. Dept. of Justice, Antitrust Division: consulting and testimony in Microsoft antitrust case, 1998-2002..

Electronic Frontier Foundation. Consulting in intellectual property / free speech lawsuits, 2001-2010.

Certus Ltd.: consultant in product design and analysis, 2000-2002.

Cigital Inc.: Technical Advisory Board member, 2000-2007.

Cloakware Ltd.: Technical Advisory Board member, 2000-2003.

Propel.com: Technical Advisory Board member, 2000-2002.

NetCertainty.com: Technical Advisory Board member, 1999-2002.
FullComm LLC: Scientific Advisory Board member, 1999-2001.
Sun Microsystems: Java Security Advisory Board member, 1997-2001.
Finjan Software: Technical Advisory Board member, 1997-2002.
International Creative Technologies: consultant in product design and analysis, 1997-98.
Bell Communications Research: consultant in computer security research, 1996-97.

Honors and Awards

National Academy of Engineering, 2013.
Alumni Achievement Award, University of Washington, 2013.
American Academy of Arts and Sciences, 2011.
E-Council Teaching Award, School of Engineering and Appl. Sci., Princeton, 2010.
ACM Fellow, 2007.
EFF Pioneer Award, 2005.
Scientific American Fifty Award, 2003.
Alfred P. Sloan Fellowship, 1997.
Emerson Electric, E. Lawrence Keyes Faculty Advancement Award, Princeton University School of Engineering, 1996.
NSF National Young Investigator award, 1994.
Outstanding Paper award, 1997 Symposium on Operating Systems Principles.
Best Paper award, 1995 ACM SIGMETRICS Conference.
AT&T Ph.D. Fellowship, 1991-93.
Mercury Seven Foundation Fellowship, 1991-93.

Research Interests

Information security. Privacy. Technology law and policy. Internet software.
Intellectual property policy. Using technology to improve government. Operating systems. Distributed computing. Parallel computing architecture and software.

Professional Service

Professional Societies and Advisory Groups

ACM U.S. Public Policy Council, Chair, 2014-2015.
ACM U.S. Public Policy Committee, Vice Chair, 2008-2010, 2012-2014.
DARPA Privacy Panel, 2010-2012.
Transportation Security Administration, Secure Flight Privacy Working Group, 2005.
National Academies study committee on Air Force Information Science and Technology Research, 2004.
Electronic Frontier Foundation, Advisory Board, 2004-2007.
ACM U.S. Public Policy Committee, 2004-present (Executive Committee, 2005-present)

ACM Advisory Committee on Security and Privacy, 2002-2003.
DARPA Information Science and Technology (ISAT) study group, 2002-2004.
Co-chair, ISAT study committee on “Reconciling Security with Privacy,” 2001-2002.
National Academy study committee on Foundations of Computer Science, 2001-2004.

Program Committees

World Wide Web Conference, 2006.
USENIX General Conference, 2004.
Workshop on Foundations of Computer Security, 2003.
ACM Workshop on Digital Rights Management, 2001.
ACM Conference on Computer and Communications Security, 2001.
ACM Conference on Electronic Commerce, 2001.
Workshop on Security and Privacy in Digital Rights Management, 2001.
Internet Society Symposium on Network and Distributed System Security, 2001.
IEEE Symposium on Security and Privacy, 2000.
USENIX Technical Conference, 2000.
USENIX Windows Systems Conference, 2000.
Internet Society Symposium on Network and Distributed System Security, 2000.
IEEE Symposium on Security and Privacy, 1998.
ACM Conference on Computer and Communications Security, 1998.
USENIX Security Symposium, 1998.
USENIX Technical Conference, 1998.
Symposium on Operating Systems Design and Implementation, 1996.

Boards

Verified Voting, Advisory Board, 2013-present.
Electronic Privacy Information Center, Advisory Board, 2013-present.
Electronic Frontier Foundation, Board of Directors, 2007-2010.
DARPA Information Science and Technology study board, 2001-2003.
Cigital Inc.: Technical Advisory Board (past).
Sun Microsystems, Java Security Advisory Council (past).
Cloakware Ltd.: Technical Advisory Board (past).
Propel.com: Technical Advisory Board (past).
Finjan Software: Technical Advisory Board (past).
Netcertainty: Technical Advisory Board (past).
FullComm LLC: Scientific Advisory Board (past).

University and Departmental Service

Council on Teaching and Learning, 2014-2015.
School of Engineering and Appl. Sci., Strategic Plan Steering Committee, 2014-2015
Committee on Online Courses, 2012-2013.
Director, Center for Information Technology Policy, 2005-present.
Committee on the Course of Study, 2009-present.
SEAS Strategic Planning, 2004.
 Member, Executive Committee
 Co-Chair, Interactions with Industry area.

Co-Chair, Engineering, Policy, and Society area.
Faculty Advisory Committee on Policy, 2002-present.
Council of the Princeton University Community, 2002-present (Executive Committee)
Faculty Advisory Committee on Athletics, 1998-2000.
Computer Science Academic Advisor, B.S.E. program, class of 1998 (approx. 25 students)
Faculty-Student Committee on Discipline, 1996-98.
Faculty-Student Committee on Discipline, Subcommittee on Sexual Assault and Harrassment, 1996-98.

Students Advised

Ph.D. Advisees:

Harlan Yu (Ph.D. 2012). Dissertation: Designing Software to Shape Open Government Policy. Founder, Upturn Partners.

Ariel J. Feldman (Ph.D. 2012). Dissertation: Privacy and Integrity in the Untrusted Cloud. Assistant Professor of Computer Science, University of Chicago.

Joseph A. Calandrino (Ph.D. 2012). Dissertation: Control of Sensitive Data in Systems with Novel Functionality. Consulting Computer Scientist, Elysium Digital.

William B. Clarkson (Ph.D. 2012). Dissertation: Breaking Assumptions: Distinguishing Between Seemingly Identical Items Using Cheap Sensors. Technical staff member at Google.

Matthias Jacob (Ph.D. 2009). Technical staff member at Nokia.

J. Alex Halderman (Ph.D. 2009). Dissertation: Security Failures in Non-traditional Computing Environments. Associate Professor of Computer Science, University of Michigan.

Shirley Gaw (Ph.D. 2009). Dissertation: Ideals and Reality: Adopting Secure Technologies and Developing Secure Habits to Prevent Message Disclosure. Technical staff member at Google.

Brent Waters (Ph.D. 2004). Dissertation: Security in a World of Ubiquitous Recording Devices. Professor of Computer Science, University of Texas.

Robert A. Shillingsburg (Ph.D. 2004). Dissertation: Improving Distributed File Systems using a Shared Logical Disk. Retired; previously a technical staff member at Google.

Michael Schneider (Ph.D. 2004). Dissertation: Network Defenses against Denial of Service Attacks. Researcher, Supercomputing Research Center, Institute for Defense Analyses.

Minwen Ji (Ph.D. 2001). Dissertation: Data Distribution for Dynamic Web Content. Researcher, HP Labs.

Dirk Balfanz (Ph.D. 2000). Dissertation: Access Control for Ad Hoc Collaboration. Technical staff member at Google.

Dan S. Wallach (Ph.D. 1998). Dissertation: A New Approach to Mobile Code Security. Professor of Computer Science, Rice University.

Significant Advisory Role:

Drew Dean (Ph.D. 1998). Advisor: Andrew Appel. Research Scientist, SRI International.

Stefanos Damianakis (Ph.D. 1998). Advisor: Kai Li. President and CEO, Netrics, Inc.

Pei Cao (Ph.D. 1996). Advisor: Kai Li. Technical staff at Facebook.

Lujo Bauer (Ph.D. 2003). Advisor: Andrew Appel. Associate Professor, School of Computer Science, Carnegie Mellon University.

Publications

Books and Book Chapters

- [1] The Economics of Bitcoin, or Bitcoin in the Presence of Adversaries. Joshua A. Kroll, Ian Davey, and Edward W. Felten. To appear, Lecture Notes in Computer Science series.
- [2] Enabling Innovation for Civic Engagement. David G. Robinson, Harlan Yu, and Edward W. Felten. In *Open Government*, Daniel Lathrop and Laurel Ruma, eds., O'Reilly, 2010.
- [3] *Securing Java: Getting Down to Business with Mobile Code*. Gary McGraw and Edward W. Felten. John Wiley and Sons, New York 1999.
- [4] *Java Security: Web Browsers and Beyond*. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz. In "Internet Besieged: Countering Cyberspace Scofflaws," Dorothy E. Denning and Peter J. Denning, eds. ACM Press, New York, 1997.
- [5] *Java Security: Hostile Applets, Holes and Antidotes*. Gary McGraw and Edward Felten. John Wiley and Sons, New York, 1996
- [6] *Dynamic Tree Searching*. Steve W. Otto and Edward W. Felten. In "High Performance Computing", Gary W. Sabot, ed., Addison Wesley, 1995.

Journal Articles

- [7] *Accountable Algorithms*. Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. *University of Pennsylvania Law Review*, Vol. 165, 2017. *Forthcoming. 2016 Future of Privacy Forum Privacy Papers for Policymakers Award*.
- [8] *Government Data and the Invisible Hand*. David Robinson, Harlan Yu, William Zeller, and Edward W. Felten. *Yale Journal of Law and Technology*, vol. 11, 2009.
- [9] *Mechanisms for Secure Modular Programming in Java*. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. *Software – Practice and Experience*, 33:461-480, 2003.
- [10] *The Digital Millennium Copyright Act and its Legacy: A View from the Trenches*. *Illinois Journal of Law, Technology and Policy*, Fall 2002.
- [11] *The Security Architecture Formerly Known as Stack Inspection: A Security Mechanism for Language-based Systems*. Dan S. Wallach, Edward W. Felten, and Andrew W. Appel. *ACM Transactions on Software Engineering and Methodology*, 9:4, October 2000.

- [12] Statically Scanning Java Code: Finding Security Vulnerabilities. John Viega, Tom Mutdosch, Gary McGraw, and Edward W. Felten. IEEE Software, 17(5), Sept./Oct. 2000.
- [13] Client-Server Computing on the SHRIMP Multicomputer. Stefanos N. Damianakis, Angelos Bilas, Cezary Dubnicki, and Edward W. Felten. IEEE Micro 17(1):8-18, February 1997.
- [14] Fast RPC on the SHRIMP Virtual Memory Mapped Network Interface. Angelos Bilas and Edward W. Felten. IEEE Transactions on Parallel and Distributed Computing, February 1997.
- [15] Implementation and Performance of Integrated Application-Controlled File Caching, Prefetching and Disk Scheduling. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. ACM Transactions on Computer Systems, Nov 1996.
- [16] Virtual Memory Mapped Network Interface Designs. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, Kai Li, and Malena Mesarina. IEEE Micro, 15(1):21-28, February 1995.

Selected Symposium Articles

- [17] Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. IEEE Symposium on Security and Privacy, 2015.
- [18] A Precautionary Approach to Big Data Privacy. Edward W. Felten, Joanna Huey, and Arvind Narayanan. Conference on Privacy and Data Protection, 2015.
- [19] On Decentralizing Prediction Markets and Order Books. Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Mill, and Arvind Narayanan. Workshop on Economics of Information Security, May 2014.
- [20] Mixcoin: Anonymity for Bitcoin with Accountable Mixes. Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. Proceedings of Financial Cryptography, February 2014.
- [21] Privacy Concerns of Implicit Security Factors for Web Authentication. Joseph Bonneau, Edward W. Felten, Prateek Mittal, and Arvind Narayanan. Adventures in Authentication: WAY Workshop, 2014.
- [22] The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Joshua Kroll, Ian Davey, and Edward W. Felten. Workshop on the Economics of Information Security, 2013.
- [23] Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2012.
- [24] Bubble Trouble: Off-Line De-Anonymization of Bubble Forms. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2011

- [25] You Might Also Like: Privacy Risks of Collaborative Filtering. Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov. Proc. IEEE Symposium on Security and Privacy, May 2011.
- [26] SPORC: Group Collaboration Using Untrusted Cloud Resources. Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. Proc. Symposium on Operating Systems Design and Implementation, 2010.
- [27] SVC: Selector-Based View Composition for Web Frameworks. William Zeller and Edward W. Felten. Proc. USENIX Conference on Web Application Development, 2010.
- [28] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmet Witchel. Proc. 17th Network and Distributed System Security Symposium, 2010.
- [29] Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham, Proc. Electronic Voting Technology Workshop, 2009.
- [30] Some Consequences of Paper Fingerprinting for Elections. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2009.
- [31] Software Support for Software-Independent Auditing. Gabrielle A. Gianelli, Jennifer D. King, Edward W. Felten, and William P. Zeller. Proc. Electronic Voting Technology Workshop, 2009.
- [32] Fingerprinting Blank Paper Using Commodity Scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Proc. ACM Symposium on Security and Privacy, May 2009.
- [33] Lest We Remember: Cold Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Proc. Usenix Security Symposium, 2008.
- [34] In Defense of Pseudorandom Sample Selection. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2008.
- [35] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.
- [36] Machine-Assisted Election Auditing. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.
- [37] Lessons from the Sony CD DRM Episode. J. Alex Halderman and Edward W. Felten. Proc. Usenix Security Symposium, 2006.

- [38] A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. Proc. 14th World Wide Web Conference, 2005.
- [39] New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent R. Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. ACM Conference on Computer and Communications Security. November 2004.
- [40] Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. 3rd Workshop on Privacy in Electronic Society. November 2004.
- [41] Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Edward W. Felten, and Amit Sahai. ACM Conference on Computer and Communications Security. November 2003.
- [42] Attacking an Obfuscated Cipher by Injecting Faults. Matthias Jacob, Dan Boneh, and Edward W. Felten. ACM Workshop on Digital Rights Management, November 2002.
- [43] A General and Flexible Access-Control System for the Web. Lujo Bauer, Michael A. Schneider, and Edward W. Felten. 11th USENIX Security Symposium, August 2002.
- [44] Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Batya Friedman, Daniel C. Howe, and Edward W. Felten. Hawaii International Conference on System Sciences, January 2002. (Best Paper award, organizational systems track.)
- [45] Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, John P. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. USENIX Security Symposium, August 2001.
- [46] Cookies and Web Browser Design: Toward Realizing Informed Consent Online. Lynette I. Millett, Batya Friedman, and Edward W. Felten. Proc. of CHI 2001 Conference on Human Factors in Computing Systems, April 2001.
- [47] Timing Attacks on Web Privacy. Edward W. Felten and Michael A. Schneider. Proc. of 7th ACM Conference on Computer and Communications Security, Nov. 2000.
- [48] Archipelago: An Island-Based File System for Highly Available and Scalable Internet Services. USENIX Windows Systems Symposium, August 2000.
- [49] Proof-Carrying Authentication. Andrew W. Appel and Edward W. Felten. Proc. of 6th ACM Conference on Computer and Communications Security, Nov. 1999.
- [50] An Empirical Study of the SHRIMP System. Matthias A. Blumrich, Richard D. Alpert, Yuqun Chen, Douglas W. Clark, Stefanos, N. Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, Margaret Martonosi, Robert A. Shillner, and Kai Li. Proc. of 25th International Symposium on Computer Architecture, June 1998.
- [51] Performance Measurements for Multithreaded Programs. Minwen Ji, Edward W. Felten, and Kai Li. Proc. of 1998 SIGMETRICS Conference, June 1998.

- [52] Understanding Java Stack Inspection. Dan S. Wallach and Edward W. Felten. Proc. of 1998 IEEE Symposium on Security and Privacy, May 1998.
- [53] Extensible Security Architectures for Java. Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Proc. of 16th ACM Symposium on Operating Systems Principles, Oct. 1997. Outstanding Paper Award.
- [54] Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Proc. of 20th National Information Systems Security Conference, Oct. 1997.
- [55] Reducing Waiting Costs in User-Level Communication. Stefanos N. Damianakis, Yuqun Chen, and Edward W. Felten. Proc. of 11th Intl. Parallel Processing Symposium, April 1997.
- [56] Stream Sockets on SHRIMP. Stefanos N. Damianakis, Cezary Dubnicki, and Edward W. Felten. Proc. of 1st Intl. Workshop on Communication and Architectural Support for Network-Based Parallel Computing, February 1997. (Proceedings available as Lecture Notes in Computer Science #1199.)
- [57] Early Experience with Message-Passing on the SHRIMP Multicomputer. Richard D. Alpert, Angelos Bilas, Matthias A. Blumrich, Douglas W. Clark, Stefanos Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, and Kai Li. Proc. of 23rd Intl. Symposium on Computer Architecture, 1996.
- [58] A Trace-Driven Comparison of Algorithms for Parallel Prefetching and Caching. Tracy Kimbrel, Andrew Tomkins, R. Hugo Patterson, Brian N. Bershad, Pei Cao, Edward W. Felten, Garth A. Gibson, Anna R. Karlin, and Kai Li. Proc. of 1996 Symposium on Operating Systems Design and Implementation.
- [59] Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten, and Dan S. Wallach. Proc. of 1996 IEEE Symposium on Security and Privacy.
- [60] Integrated Parallel Prefetching and Caching. Tracy Kimbrel, Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1996 SIGMETRICS Conference.
- [61] Software Support for Virtual Memory-Mapped Communication. Cezary Dubnicki, Liviu Iftode, Edward W. Felten, and Kai Li. Proc. of Intl. Parallel Processing Symposium, April 1996.
- [62] Protected, User-Level DMA for the SHRIMP Network Interface. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996
- [63] Improving Release-Consistent Shared Virtual Memory using Automatic Update . Liviu Iftode, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996
- [64] Synchronization for a Multi-Port Frame Buffer on a Mesh-Connected Multicomputer. Bin Wei, Gordon Stoll, Douglas W. Clark, Edward W. Felten, and Kai Li. Parallel Rendering Symposium, Oct. 1995.

- [65] A Study of Integrated Prefetching and Caching Strategies. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1995 ACM SIGMETRICS Conference. Best Paper award.
- [66] Evaluating Multi-Port Frame Buffer Designs for a Mesh-Connected Multicomputer. Gordon Stoll, Bin Wei, Douglas W. Clark, Edward W. Felten, Kai Li, and Patrick Hanrahan. Proc. of 22nd Intl. Symposium on Computer Architecture.
- [67] Implementation and Performance of Application-Controlled File Caching. Pei Cao, Edward W. Felten, and Kai Li. Proc. of 1st Symposium on Operating Systems Design and Implementation, pages 165-178, November 1994.
- [68] Application-Controlled File Caching Policies. Pei Cao, Edward W. Felten, and Kai Li. Proc. of USENIX Summer 1994 Technical Conference, pages 171-182, 1994.
- [69] Virtual Memory Mapped Network Interface for the SHRIMP Multicomputer. Matthias A. Blumrich, Kai Li, Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Jonathan S. Sandberg. Proc. of Intl. Symposium on Computer Architecture, 1994.
- [70] Performance Issues in Non-Blocking Synchronization on Shared-Memory Multiprocessors. Juan Alemany and Edward W. Felten. Proceedings of Symposium on Principles of Distributed Computing, 1992.
- [71] Improving the Performance of Message-Passing Applications by Multithreading. Edward W. Felten and Dylan McNamee. Proceedings of Scalable High-Performance Computing Conference (SHPCC), 1992.
- [72] A Highly Parallel Chess Program. Edward W. Felten and Steve W. Otto. 1988 Conference on Fifth Generation Computer Systems.

Selected Other Publications

- [73] Testimony for Privacy and Civil Liberties Oversight Board hearing on “Defining Privacy”. November 2014. Written testimony submitted December 2014.
- [74] Heartbleed Shows Government Must Lead on Internet Security. Edward W. Felten and Joshua Kroll. *Scientific American*, July 2014.
- [75] How the NSA Piggy-Backs on Third-Party Trackers. Edward Felten and Jonathan Mayer. *Slate*, Dec. 13, 2013.
- [76] Testimony for Senate Judiciary Committee hearing on “Continued Oversight of the Foreign Intelligence Surveillance Act,” October 2, 2013.
- [77] The Chilling Effects of the DMCA. Edward Felten. *Slate*, March 29, 2013.
- [78] CALEA II: Risks of Wiretap Modifications to Endpoints. [20 authors]. Submitted to a White House working group.
- [79] Strangers in a Strange Land. Review of *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*, by Abelson, Ledeen, and Lewis. *American Scientist*, 97:4. July/August 2009.

- [80] Lest We Remember: Cold-Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Communications of the ACM*, 52(5):91-98. May 2009.
- [81] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Sept. 2006.
- [82] Digital Rights Management, Spyware, and Security. Edward W. Felten and J. Alex Halderman, *IEEE Security and Privacy*, Jan./Feb. 2006.
- [83] Inside RISKS: DRM and Public Policy. Edward W. Felten. *Communications of the ACM*, 48:7, July 2005.
- [84] Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks? Edward W. Felten. *IEEE Security and Privacy*, May 2003.
- [85] A Skeptical View of DRM and Fair Use. Edward W. Felten. *Communications of the ACM* 46(4):56-61, April 2003.
- [86] Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace. Testimony before U.S. Senate Commerce Committee. September 2003.
- [87] Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. Submitted for publication, 2003.
- [88] An Efficient Heuristic for Defense Against Distributed Denial of Service Attacks using Route-Based Distributed Packet Filtering. Michael A. Schneider and Edward W. Felten. Submitted for publication, 2003.
- [89] Written testimony to House Commerce Committee, Subcommittee on Courts, the Internet, and Intellectual Property, oversight hearing on "Piracy of Intellectual Property on Peer to Peer Networks." September 2002.
- [90] Written testimony to Senate Judiciary Committee hearings on "Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creativity?" March 2002.
- [91] Informed Consent Online: A Conceptual Model and Design Principles. Batya Friedman, Edward W. Felten, and Lynette I. Millett. Technical Report 2000-12-2, Dept. of Computer Science and Engineering, University of Washington, Dec. 2000.
- [92] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Technical Report CS-TR-603-99, Department of Computer Science, Princeton University, July 1999.
- [93] A Java Filter. Dirk Balfanz and Edward W. Felten. Technical Report 567-97, Dept. of Computer Science, Princeton University, October 1997.
- [94] Inside RISKS: Webware Security. Edward W. Felten. *Communications of the ACM*, 40(4):130, 1997.
- [95] Simplifying Distributed File Systems Using a Shared Logical Disk. Robert A. Shillner and Edward W. Felten. Princeton University technical report TR-524-96.

- [96] Contention and Queueing in an Experimental Multicomputer: Analytical and Simulation-based Results. Wenjia Fang, Edward W. Felten, and Margaret Martonosi. Princeton University technical report TR-508-96.
- [97] Design and Implementation of NX Message Passing Using SHRIMP Virtual Memory Mapped Communication. Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Kai Li. Princeton University technical report TR-507-96.
- [98] Protocol Compilation: High-Performance Communication for Parallel Programs. Edward W. Felten. Ph.D. dissertation, Dept. of Computer Science and Engineering, University of Washington, August 1993.
- [99] Building Counting Networks from Larger Balancers. Edward W. Felten, Anthony LaMarca, and Richard Ladner. Univ. of Washington technical report UW-CSE-93-04-09.
- [100] The Case for Application-Specific Communication Protocols. Edward W. Felten. Univ. of Washington technical report TR-92-03-11.
- [101] A Centralized Token-Based Algorithm for Distributed Mutual Exclusion. Edward W. Felten and Michael Rabinovich. Univ. of Washington technical report TR-92-02-02.
- [102] Issues in the Implementation of a Remote Memory Paging System. Edward W. Felten and John Zahorjan. Univ. of Washington technical report TR-91-03-09.

EXHIBIT 7

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual;)
)
DONNA PRICE, an individual;)
)
ROCKY MOUNTAIN FOUNDATION,)
INC., a non-profit corporation organized)
and existing under Colorado law;)
)
Plaintiffs,)

v.)

CIVIL ACTION
FILE NO.:

BRIAN P. KEMP, in his official capacity)
as Secretary of State of Georgia;)
)
RICHARD BARRON, in his official)
capacity as Director of the Fulton County)
Board of Elections and Registration;)
)
MAXINE DANIELS, in her official)
capacity as Director of Voter Registrations)
and Elections for DeKalb County;)
)
JANINE EVELER, in her official)
capacity as Director of the Cobb County)
Board of Elections and Registration;)
)
Defendants.)

AFFIDAVIT

County of Columbia)

) ss.

State of New York)

VIRGINIA MARTIN ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am the Democratic Election Commissioner in Columbia County, New York. I submit this affidavit in support of petitions to use paper ballots to conduct the Runoff in Georgia Congressional District 6 (CD6) on June 20, 2017.

2. I have been employed as election commissioner since 2008. I hold a BA in English and Communication from Skidmore College and an MS and a PhD in Communication and Rhetoric from Rensselaer Polytechnic Institute. I serve on the advisory board of the National Election Defense Coalition.

3. Because of my extensive experience in hand counting paper ballots, I have taught hand-counting workshops to other election officials and election-integrity experts.

4. Since 2010, the Columbia County Board of Elections, comprising myself and my Republican counterpart Jason Nastke, has run 23 elections on Dominion ImageCast optical scan voting machines, followed by a hand-count process which I oversee with Commissioner Nastke.

5. I have a great deal of experience overseeing the reconciliation and hand counting of paper ballots. In most cases, multiple races were counted on each ballot. In every election, the hand counts were completed efficiently and in a reasonable time frame.

6. The number of ballots cast in the 2016 presidential election was more than 31,000. The number of ballots cast in the 2014 gubernatorial election was more than 21,000. The number of ballots cast in the 2012 presidential election was more than 29,000. The number of ballots cast in the 2010 gubernatorial election was more than 24,000.

7. The number of races on the above ballots was as many as nine in 2016, 13 in 2014, eight in 2012, and 11 in 2010.

8. All of the paper ballots cast in the 23 elections run in this county beginning in 2010 were then physically accounted for.

9. Most of the votes on the paper ballots cast in the 23 elections run in this county beginning in 2010 have additionally been counted by hand, in a transparent and verifiable process, subsequent to being tabulated by optical scanners.

10. The New Hampshire Assistant Secretary of State produced a report in 2007 concerning the hand counting of paper ballots, asserting that the state has considerable experience in hand counting. Using the sort and stack method of ballot counting, their data showed that a team of three people could count one vote in six seconds. Data showed that more experienced teams could count one vote in four to five seconds. The report is attached.


11. At the rate of six seconds per vote, a team of three can be expected to count 600 votes in one hour.

12. Each ballot in the Runoff will have a single race.

13. On election day, April 18, 2017, the average in-person voter turnout per precinct was 634 voters. If turnout on June 20, 2017 is similar, in my estimation it is reasonable to believe that the average precinct could hand count, in a transparent and verifiable process, all the ballots cast in one and one-half hours or less.

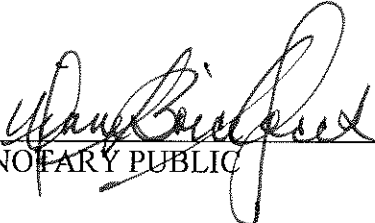
14. I affirm that the foregoing is true and correct.

15. Further Affiant sayeth not.



Virginia Martin

Sworn before me this 26th day of May, 2017, in Columbia County, New York.



NOTARY PUBLIC

DIANE BOICE YORCK
Notary Public, State of New York
Reg. No. 01BO5029553
Qualified in Columbia County
Commission Expires June 20, 2018



Hand Counting Paper Ballots

Address to Democracy Fest
Annual National Convention
June 10, 2007
Sheraton Wayfarer, Bedford, NH

By Anthony Stevens
Assistant Secretary of State
New Hampshire

Focus of this Presentation

Election
Night Hand
Counting



Why New Hampshire is relevant for hand counts

- NH has perhaps the highest volume of hand recounts conducted at state level in the nation.
 - 10-32 recounts per election cycle
 - 50-136 candidates involved per cycle
- Current Secretary of State has been involved in over 300 hand-counted recounts.
- In the 2004 general election, there were 7 hand counting polling places with over 2,500 persons registered to vote.
 - Each counted over 2,000 ballots, or over 3 X the ballots cast in an average-sized US precinct.

Counting in New Hampshire

Approx. ballots counted:
80% optical scan; 20% hand count

- 139 polling places (45%) in NH rely on hand counting
- 170 polling places (55%) in NH rely on optical scanning machines

- 138 jurisdictions (58%) in NH rely on hand counting
- 98 jurisdictions (42%) in NH rely on optical scanning machines

Wide range of situations calls for different solutions

- Individual New Hampshire polling places served as few as 18 registered voters and as many as 18,974 registered voters in 2006.
- New Hampshire has 7 polling places with over 10,000 registered voters, which is over 6 X the national average polling place size.
- Size of polling place affects decisions regarding counting methods.
- One size does not fit all.

New Hampshire Secretary of State

- Supports hand counting and optical scanning counting methods.
- Seeks to identify best practices, recognizing that all ballot counting methods are under scrutiny and will need improvement over time.
- Continues to learn from local officials and promote best practices in counting using hand counting and optical scanning methods.
- Recognizes that there is probably more than one way to count ballots correctly.

In appreciation

- **Recognition to:**
 - All those election workers who give their time, often for little or no pay, to ensure democracy works

- **Special thanks to:**
 - Ernest D. Vose, Moderator, Walpole
 - David Westover, Assistant Moderator
 - Walter Fries, Moderator, Danville

Purpose of hand counts

- Testing of voting machines
- Election night counting
- Parallel counting on election night
- Audits
- Recounts

National use of hand counting on election night EAC: 2004 Election Day Survey

1,734 hand count jurisdictions (26.4%)
among 6,568 jurisdictions nationwide

Hand counting used for about 1% of ballots in nation

Significant hand count states:

Wisconsin, Maine, Vermont,
New Hampshire, Texas, Massachusetts, Nebraska,
Montana, Kansas.

In New Hampshire

Selection of counting method

- **Based on a local decision – often a town meeting warrant article.**
- **Decision to use a vote counting machine is subject to NH Ballot Law Commission approval**

Focus on Sort and Stack Method

- Secretary of State indicates a preferred method in NH Election Procedure Manual
- Use of sort-and-stack method based on observation in recounts - operating hypothesis
- Many steps similar to the read-and-mark method, also used heavily in NH
- Sort-and-stack method is not used by the SOS in recounts for multi-seat races
 - Although the method can be used by treating every candidate as a separate contest.
- Sort-and-stack method may not be used widely in New Hampshire on election night

Overview of Sort and Stack Method

- **Ballots are sorted into piles**
- **One pile for different categories**
 - Each candidate or alternative on a question
 - Overvotes (defective in that contest)
 - Undervotes (skipped races)
 - Write-ins
 - Judgment calls for the moderator (local election manager)

Hand Counting Steps

- Planning
- Recruiting
- Knowing your method & how to present it
- Preliminary organizational work
- Training
- Oath of office
- Opening ballot box, counting and distributing ballots
- Tallying votes in contests
- Entering on tally sheet
- Moderator (local election manager) review
- Dealing with discrepancies

Recruiting counters & observers

- Cost estimates of \$10 per hour here are on the high side. Many counters in NH work for between \$0 and \$5 per hour and are justly proud of their contribution.
- Locations paying \$0-\$5 per hour are some of the most effective at inspiring and recruiting good election night counters of all ages.
- Plan on using a second shift for counting. This makes it easier to recruit :
 - people with day jobs
 - students
- High school students are now required to contribute community service hours and log them.
 - 17-year olds qualify in NH & other states.
- Seek a balanced mix.
 - Managers
 - Numbers person
 - Young people
 - Middle aged
 - Older people

Recruiting

- Count your contest equivalents on the ballot.
- Know your method.
- Estimate your target number of counters & observers at each table.
- Estimate the number of sets of eyes per ballot.
- Consider using people who have worked all day as observers.

Contests per ballot

- The number of contests per ballot varies widely.
- In NH, the typical range on a primary or general election ballot is 12 contests, plus questions.
- The NH state representative contest normally is a multiple-seat race, with as many as 26 candidates running for 13 seats in the same district.
 - We would count this example as 13 contest equivalents. When added to 11 other contests on the ballot, the contest equivalents on this ballot should be estimated as $13 + 11 = 24$ contests.
- The following estimates should be adjusted according to how many contests or contest equivalents appear on the ballot.

Team availability on election night

- 3 hours available (8 PM to 11 PM) X 60 minutes X 60 seconds = 10,800 seconds per team available in one night.

Assumptions:

- Second shift (8-11 PM) brings in fresh counters.
- 20 minutes of training is included in 3 hours

Estimating hand counting staff

- Average U.S. precinct in 2006 = 936 registered voters X 67% turnout in general election = 627 ballots X 20 contests/ballot = 12,540 contests to count.
- Assumptions:
 - In NH, general election ballots may contain contests for as few as 12 positions per ballot and contests for as many as 25 position equivalents.
 - Multi-seat races are harder to count than races with single outcomes.

Estimating hand counting staff

- 12,540 contests to count X 6 seconds for a team to count a contest in NH experience = 75,240 seconds required on election night, divided by 10,800 (3-member) team seconds available per night = 7 teams needed.
- Assumption: It takes approximately 6 seconds to hand count a contest on a ballot.
 - This is based on:
 - Videos and interviews with towns that conduct hand counts efficiently
 - Secretary of State experience with hand counting
 - Experienced towns average 4 - 5 seconds to count each contest on a ballot, including training time, sorting, stacking and counting.

Estimating hand counting staff

- 7 teams X (2 counters + 1 observer = 3 persons per team)
= 21 counters/observers
+ 3 managers = 24 total staff

Estimated staff costs

21 counters/observ. X 3 hours @ \$10/hr = \$630

3 managers X 4 hours @ \$20/hr = \$240

Total **\$870**

Using 3 person counting teams:

\$870 per polling place/627 ballots counted

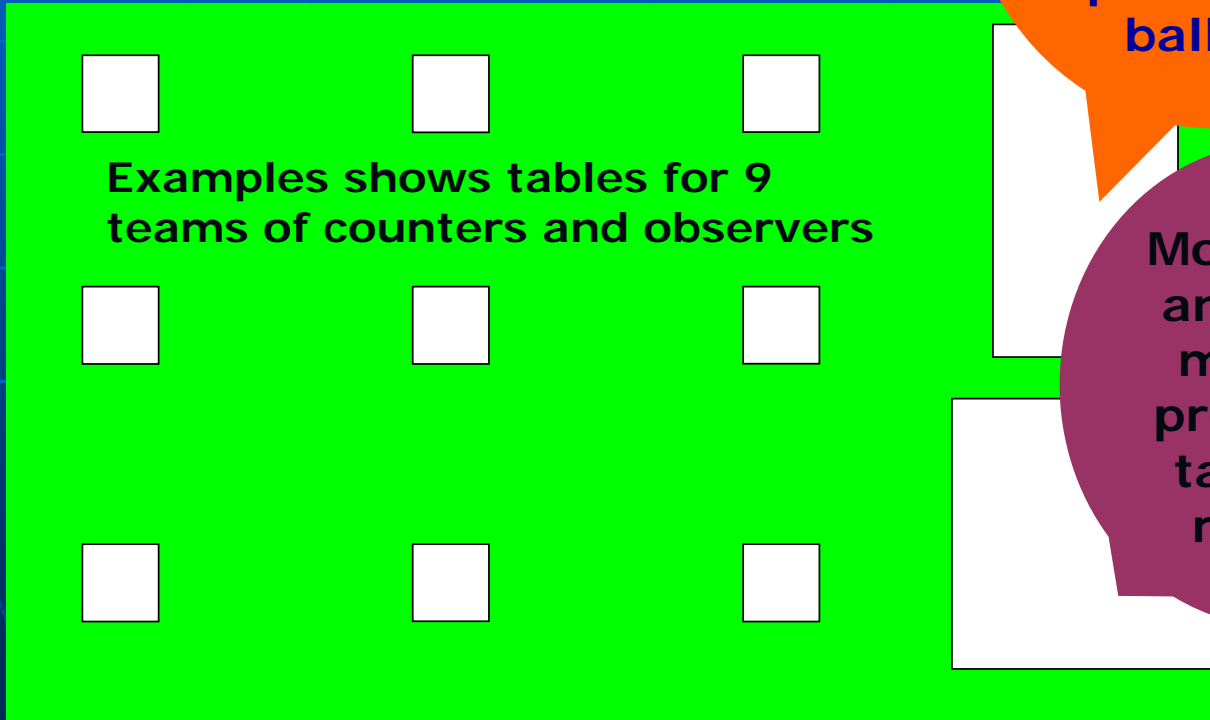
@ 20 contests/ballot =

- \$1.39/ballot, or
- \$0.07/contest on a ballot

Hand counting steps

- **Close the polls**
- **Verify all absentee ballots processed**
- **Rearrange the polling place for counting**

Ballot counting table layout



Examples shows tables for 9 teams of counters and observers

Checklist (pollbook) supervisors count those who have picked up ballots

Moderator and clerk manage process & tabulate results

Advantage of sort and stack method

- Counters and observers are looking at only one candidate or question on the ballot.
- Counters' and observers' eyes do not have to move to different locations on the ballot and on the tally sheet.
- Counters and observers have to focus on getting only one thing right. When looking for evidence of only one mark on one precise location on the ballot, it is harder to make mistakes.
- Recording the number of votes for a candidate or question is done when the stack is counted.
- Other methods rely on a separate mark on a tally sheet being made with each ballot. This requires more sets of eyes to track accurately.

Rule of thumb: 3 sets of eyes per contest per ballot

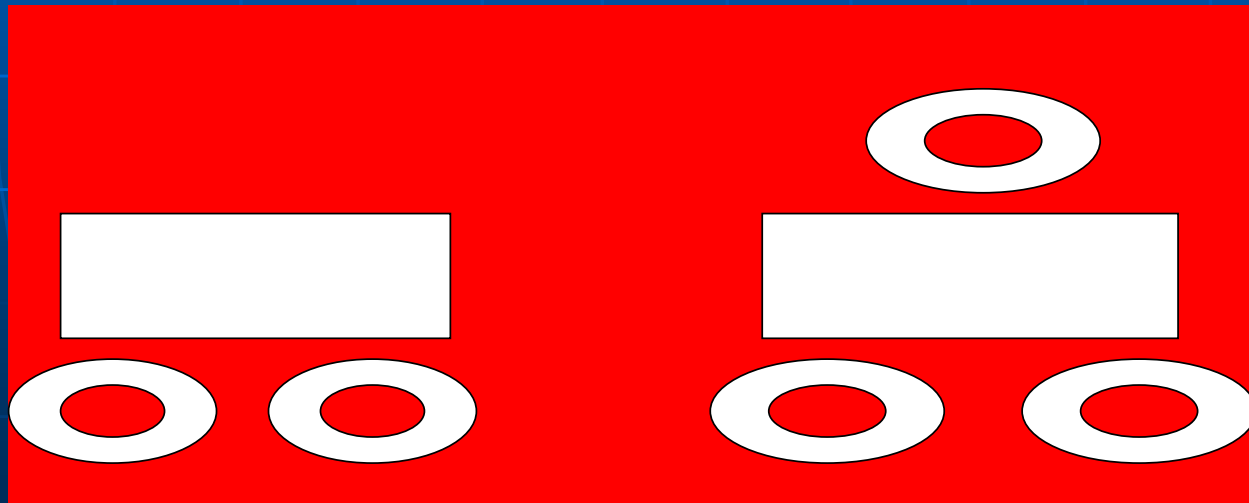
- **Aim for at least 3 sets of eyes on each ballot, and each vote recording.**
- **Using a 2-person team, that might mean that both members watch as one member sorts the ballots.**
 - **At least one member checks the marks again when counting the number of ballots in the stack.**
- **Both members count each pile and record and check the sum on the tally sheet.**

Choosing # of observers

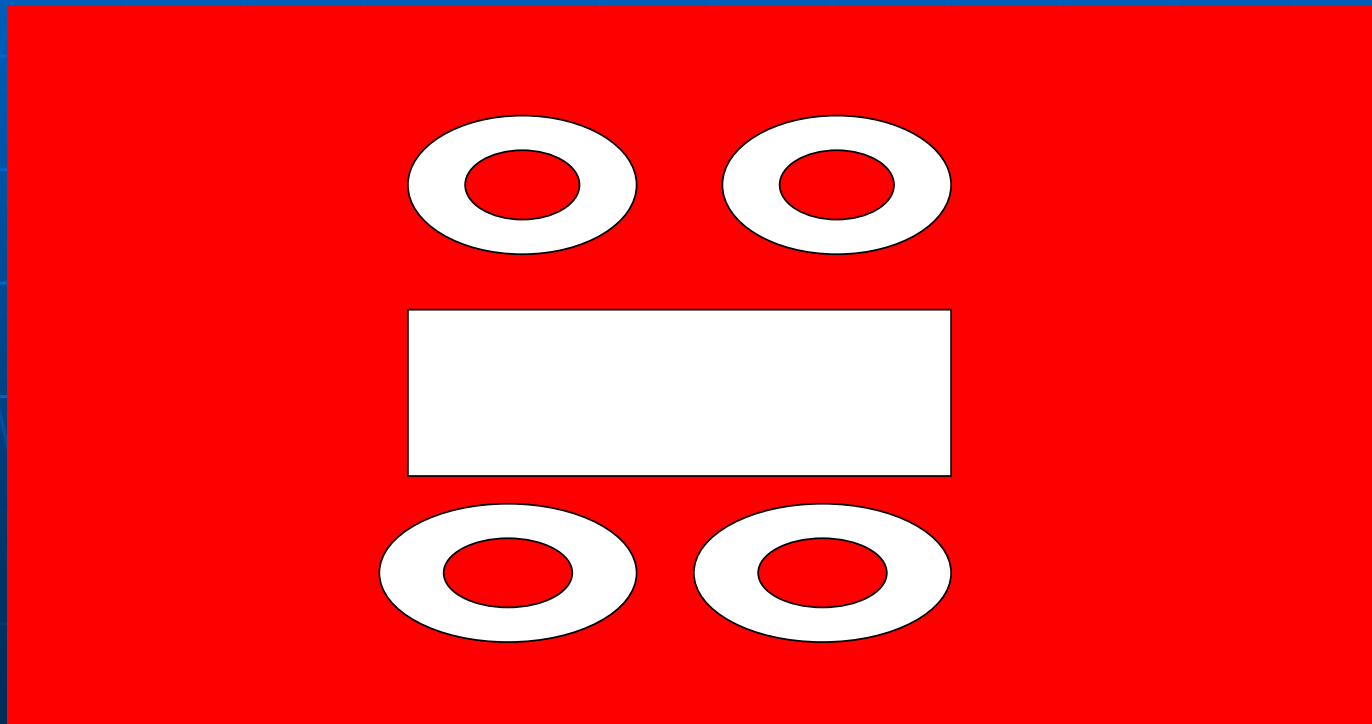
- The more sets of eyes on a single ballot, the greater certainty in the results.
- Generally, this means the more observers, the greater degree of certainty in the results.
- (Still, using the sort and stack method, 2 counters (no observers) can apply 3-4 sets of eyes to each ballot, and still achieve accuracy.)
- An extra set of observers for 7 teams would cost \$210 (7 observers X 3 hours X \$10/hour) in an average US polling place counting a 20-contest ballot without volunteer help.
- New Hampshire recounts rely on observers selected by the candidates, often resulting in tables with 4 or 5 persons – 2 counters and 2-3 observers.

2 counters

**1 observer
2 counters**



2 counters & 2 observers



Preliminary Organizational Work

- Have the checklist (pollbook) supervisors count the number of voters who are checked off as having voted.
- Identify those who will be counting.
- Identify those counters who have not yet taken the oath of office.

Oath of Office

Swear in non-election officials as election officials

"I, (state your complete name), do solemnly swear (*affirm*), that I will bear faith and true allegiance to the United States of America and the State of New Hampshire, and will support the constitution thereof. So help me God. *This I do under the pains and penalties of perjury.*

Alternate language for those scrupulous of swearing, or mentioning God in this matter, is set forth in italics.

Training

- Read the instructions for counting to all the election officials who will be counting.
- Provide clear directions regarding method to achieve consistency.
- The moderator (senior local election official) has control and should exercise it.
- If people insist on using another counting method, consider asking them to act as an observer.
 - Observing the counters count is a key role and helps achieve accuracy.
- Oath of office and training take 20 minutes.

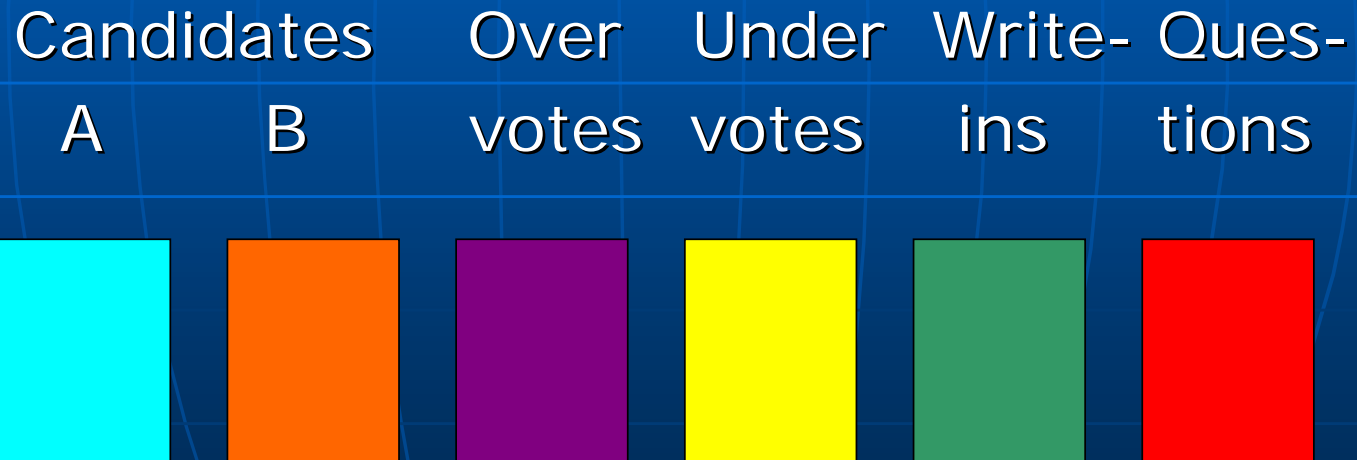
Distributing ballots to teams

- Open the ballot box in view of the public.
- Place an established quantity of ballots on the table to be used by each counting team.
- Both members count the ballots in groups of 50.
- If it becomes necessary to redo a particular part of the process because the results do not equal the number of ballots, counters can afford to recount 50.

Sort and Stack Ballots

One contest

Separate piles



Start counting ballots

- Team members should look at each ballot to ensure it is sorted into the correct pile.
- Once each table has the ballots assigned to it sorted into the six piles, start the counting process with the pile of ballots for the first candidate on the ballot.
- All other ballots should be set aside, but remain in public view on that table.

Counting ballots

- The team should count the ballots in the first candidate's pile into groups of ten.
- Stack each group of ten ballots and the remainder at right angles to each other on the same pile.
- Both counters count the piles of ten, plus remainders, agree on the number and enter it in the tally sheet.

Tally Sheet – single contest

| | Candidate A | Candidate B | Candidate C | Under-vote | Over-vote | Write-ins | TOTAL |
|--------------------------------|--------------------|--------------------|--------------------|-------------------|------------------|------------------|--------------|
| 1st group of 50 ballots | 19 | 17 | 9 | 4 | 1 | 0 | 50 |
| 2nd group of 50 ballots | 17 | 22 | 8 | 3 | 0 | 0 | 50 |
| 3rd group of 50 ballots | 16 | 18 | 11 | 3 | 1 | 1 | 50 |
| 4th group of 50 ballots | 18 | 20 | 9 | 2 | 0 | 1 | 50 |
| TOTALS | 70 | 77 | 37 | 12 | 2 | 2 | 200 |

Next candidate, same contest

- Then begin counting the next candidate in the same contest.
- When all the piles have been counted and checked, that counting team is done with that set of ballots for that candidate in that contest.
- Counters agree on the number to enter on the tally sheet.
- If there is another candidate in that contest, counters count the pile for that candidate and agree on the number to enter on the tally sheet.

Same contest, counting the piles of undervotes and overvotes

- Counters count separately the piles for undervotes and overvotes and agree on the numbers to enter on the tally sheet.
- The team should add the votes for each candidate (including write-ins) and the number of undervotes (skipped/abstentions) and overvotes (defective) in that contest.
- Enter the total in the far right column of each row. It should equal 50.

Next contest

- Begin the sorting and counting process for the first candidate in the next contest.
- When all piles for that contest have been counted, checked and entered on the tally sheet, that counting team is done with that set of ballots for that contest.
- The team should add the votes for each candidate (including write-ins) and the number of undervotes (skipped/abstentions), and overvotes (defective) in that contest. That number should equal 50.

Tallying

- Tally sheets should be turned in - after the numbers equal 50 on the far right, and the aggregate of votes = 200 on the bottom right.
- Tally sheets should be signed by the counters before being turned in.
- Moderator should designate someone who routinely works with numbers to tally and check the team tally sheets.

Moderator (local election manager) Review

- The moderator (manager) should stop before announcing the results and check the final tallies.
- If a count was done of the total number of persons checked off as having voted on the checklist, the aggregate tallies for each contest (office or question) should be verified against that count.
- The total votes for all candidates (including write-ins) in a single contest, plus the undervotes (skipped/abstentions) in that contest, plus the overvotes (defective) in that contest, should equal the total number of ballots used.

Dealing with Discrepancies

- The moderator should be looking for any significant discrepancies between the totals. It may be difficult to get a perfect count from the checklist (pollbook).
- It is not essential that the total count for each office or question exactly match the total of those checked off on the checklist (pollbook).
- Provided the write-in, undervotes (skipped/abstentions) and overvotes (defective) were tallied, the totals from one contest to the next for the same set of ballots should be the same (50 per batch).

Dealing with Discrepancies

- Tally sheets from each team should be carefully checked as each contest is counted. Reconciliation should be kept current during the night.
- Any mismatch of votes per contest with number of ballots per batch should be addressed immediately.
- When the last tally sheet is handed in for the last race, reconciliation should be largely complete. Little tally work remains.
- If any discrepancies are found, the moderator should investigate and attempt to resolve the discrepancy before declaring the results.

Advantages of using tally sheets to track undervotes and overvotes

- Tally sheets permit ongoing reconciliation (number checking) as the count progresses.
- Surprises at the end are less likely.

**This is a start.
There is more to learn.**

The State of New Hampshire plans more study on this subject, with the help of towns and cities.



The End

EXHIBIT 8

IEEE VSSC/P1622 Joint Meeting

February 5-6, 2014

Georgia Tech Research Institute

Atlanta, GA

VSSC/P1622 Meeting Feb 5

- Call to Order
- Roll Call

Opening Remarks

- Welcome
- IEEE Call for Patents
- Agenda overview
- Goals

Georgia Voting

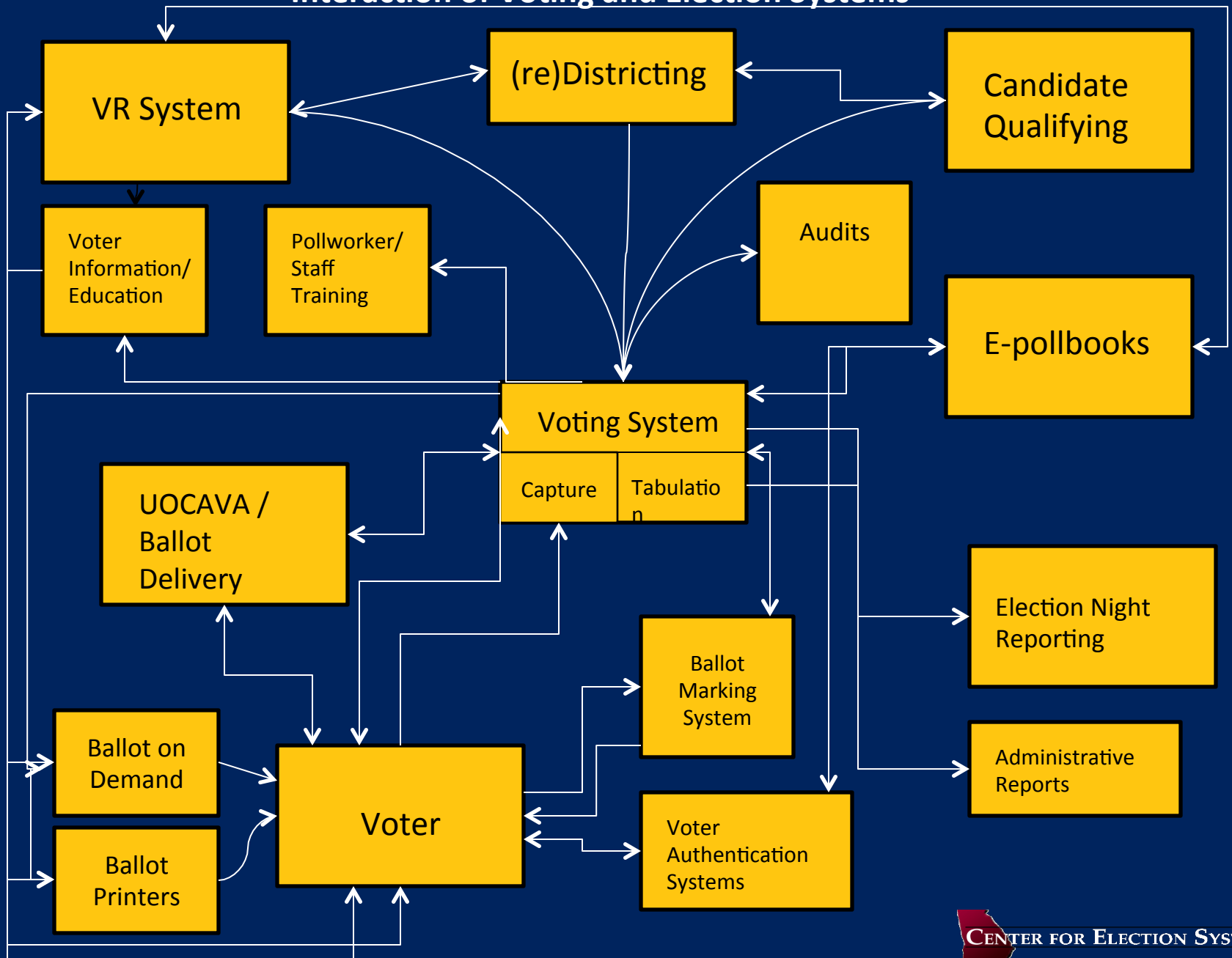
- Merle King



The Georgia Voting System

February, 2014

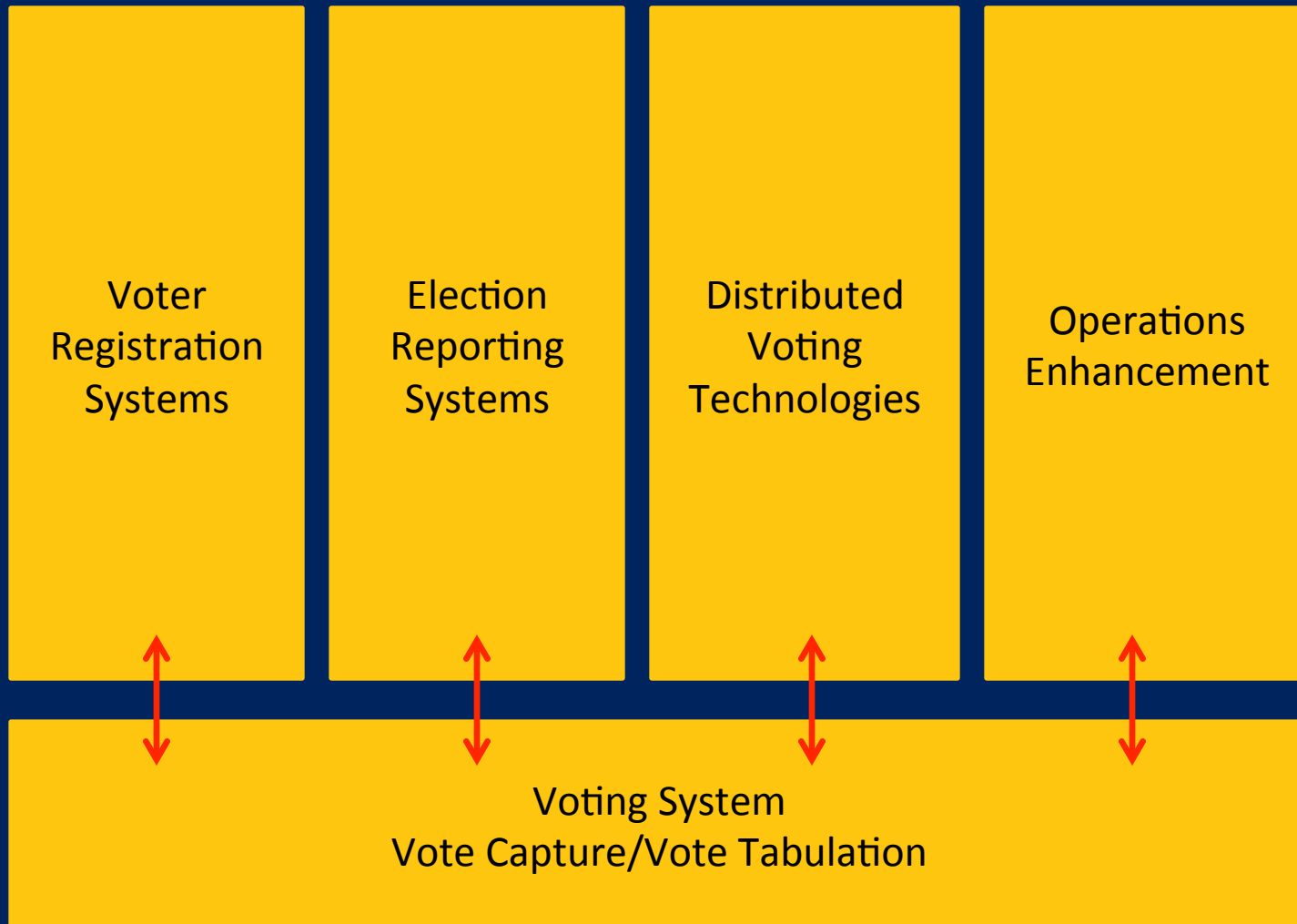
Interaction of Voting and Election Systems



Uniform Voting System

- Since 2002, Georgia has supported a **uniform voting system**
 - Every county uses the same equipment in the same way
 - Centralized services, including
 - Ballot Building
 - Training
 - E-pollbook preparation
 - VR system
 - ENR

System Convergence



Core Competencies of Election Officials and Election Workers

Voter
Registration
Systems

Election
Reporting
Systems

Distributed
Voting
Technologies

Operations
Enhancement

Voting System
Vote Capture/Vote Tabulation

Uniform Voting System

- ~26,500 DREs
- ~621 O/S units
- ~6,825 e-pollbooks
- ~6,075 bar code scanners
- Media for devices
- 159 tabulation servers
- Deployed in 159 counties with VR list of 6.1M (2014)

Uniform Voting System

- In constant use since 2002
 - Over 5,000 elections
 - Over 50,000,000 votes cast
- Repairs / replacements of DREs approximately .5% per year
 - 2011: ~160
 - 2012: ~150
 - 2013: ~135

System Components

- Beginning in 2002, Georgia required the use of a uniform voting system for all state and county elections.
 - DREs used for in-precinct voting and advanced / early voting
 - Direct Record Electronic – touchscreen
 - Votes are directly recorded onto electronic media
 - HAVA section 301 compliant
 - Flexible
 - Accuvote OS used for mail-in absentee
 - Other components
 - ExpressPoll – electronic pollbooks
 - GEMS servers

System Components

- Election Systems and Software (ES&S)
 - Supports State of Georgia Contract for voting system components:
 - New purchases
 - Repairs
 - Services
 - Ballot Printing
 - L&A Support
 - Election Day Support
 - In-state contract manager
 - Licenses software to state for voting system components
 - Purchased inventory and IP from Premier Election Solutions (Diebold)



System Components

GEMS Servers – One in every county at the tabulation location (usually county elections office)



System Components

GEMS Servers – One in every county at the tabulation location (usually county elections office)

Dell 1900



Vision I



System Components

DRE

– All DREs run Ballot Station 4.5.2!

Don't know what "!" means.



System Components

- Optical Scanner
 - Accuvote OS, running firmware 1.94



System Components

- ExpressPoll 4000 (with barcode scanner)



System Components

- ExpressPoll 5000



System Components

Encoder



Certification

- System is certified by FEC/NASED, to the 1990 VSS standard. note certification standard.
- Georgia requires federal certification.
- State Certified
- Acceptance Tested

Local Jurisdiction Acceptance. After a voting system is delivered to a local jurisdiction, acceptance tests shall be performed in the user's environment to demonstrate that the voting system as delivered and installed is identical to the system that was certified by the State and satisfies the requirements specified in the procurement documents.

- Rules of the Secretary of State, 590-8-1-.01 Certification of Voting Systems

Certification

- Acceptance Tested
 - DREs and OS units sent off for repair must be acceptance tested upon return to the county or municipality.

GEMS

- GEMS – Global Election Management System.
Version 1.18.22G!
- Used statewide since 2002
- Resides on a dedicated, non-networked computer (server) within the county election office
- Used to create election databases, program the voting equipment, and produce the ballots and reports for any given election within the county
- GEMS Verify

"!" --what does this mean?

Artifacts

- Object: Seals
- Function: Detective Control. Used to denote pre-election (red) and post election (blue) status of equipment. Other applications include secure shipping by the Center for Election Systems. All seals have multi-digit numeric values
- Location/Owner: County election offices. Equipment storage facilities. Center for Election Systems. Seals can be ordered directly from the vendor or from the SOS warehouse.

Artifacts

- Object: Seals

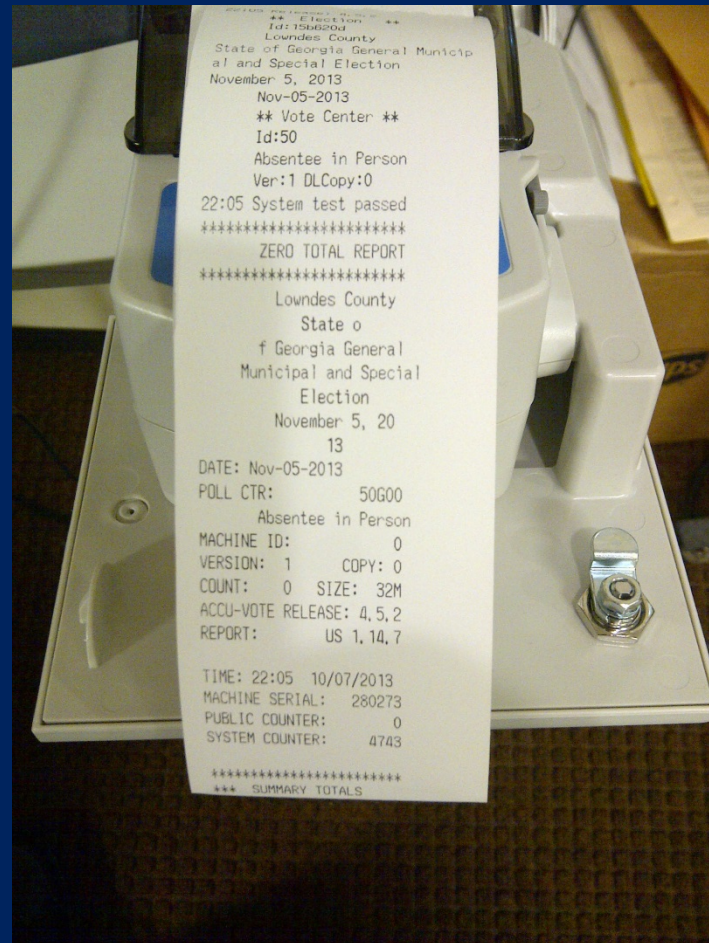


Artifacts

- Object: Zero Tapes
- Function: Demonstrate there were no votes on a TS or OS unit prior to vote capture. The zero tape provides the “before” snap shot of a unit’s status at poll opening. The poll manager and two poll workers have to sign the zero tape.
- Location/Owner: Counties will have the zero tapes for each unit as a part of the election materials brought in from the precincts.

Artifacts

- Object: Zero Tapes



Artifacts

- Object: Acceptance Test Labels
- Function: Each election device must have an Acceptance Test Label that affirms the device conforms to the certified model. A device without an Acceptance Test label is not permitted for use in an election (exceptions are municipalities using non-certified equipment).
- Location/Owner: AT labels are applied by the Center at the conclusion of successful acceptance testing. Only the Center has the labels. There are different labels for each type of device.

Artifacts

- Object: Acceptance Test Labels

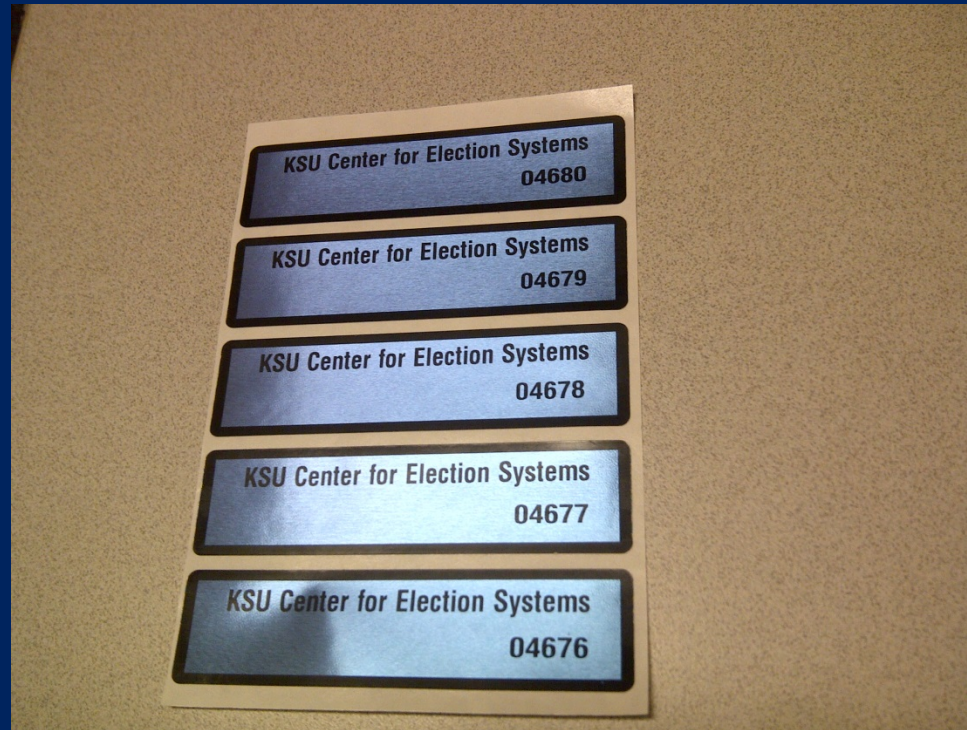


Artifacts

- Object: Security Seals from KSU
- Function: Detect whether a server's case has been opened.
- Location/Owner: Applied to server at Acceptance Testing.

Artifacts

- Object: Security Seals from KSU



Artifacts

- Object: Card Label
- Function: Used to identify the election to which a memory card belongs. These labels are produced by the TS or OS unit when the memory card is created during election preparation.
- Location/Owner: The county is responsible for generating and affixing these tape labels.

Artifacts

- **Object: Memory Cards**
- **Function: Devices that use Memory Cards:**
 - **TS Units: PCMCIA cards or CF cards in PCMCIA adaptors**
 - **OS Units: OS Memory Cards**
 - **ExpressPoll units: Compact Flash Cards**

There is a one-to-one relationship between units prepared for an election and memory cards. EVERY memory card must be accounted for at tabulation. Counties MUST upload official election results directly from memory cards. Even un-voted memory cards must be uploaded.

Memory cards must be maintained for at least 30 days after an election.

Separate memory cards are used for run-offs.

- **Location/Owner: Counties.**

Artifacts

- Object: Memory Cards

ExpressPoll Memory Card



OS Memory Card



TS Memory Card



Artifacts

- **Object: GEMS Reports: Election Summary Report and Statement of Votes Cast (SOVC) Report**
- **Function: These are standard printed reports that present the vote totals by race and displayed by precinct, and a report that details the totals votes (ballots) cast in that election. Used to reconcile that all memory cards from all precincts have been loaded and that the number of votes cast match the number of voter access cards generated and the number of oaths signed in the precinct. The Election Summary Report is also generated before beginning the upload of memory cards to confirm the database contains zero results prior to the first results being uploaded.**
- **Location/Owner: County Election Office**

Artifacts

- **Object: Numbered List**
- **Function: A list of voters who cast ballots in a precinct and ballot they selected if a primary election. This list is used to reconcile with the number of votes cast in that precinct. This list is electronic on election night and is produced by the ExpressPoll unit. It can be extracted and printed to a file or to paper.**
- **Location/Owner: County has the initial list, but once the ExpressPoll CF cards are returned to the Center, that list is extracted and posted to the county via our password-protected web site. The list is public information and is requested by candidates and parties.**

Artifacts

- Object: Logic and Accuracy Test Forms
- Function: Each device used in the election is subject to L&A testing. Each device as well as the date and status of the test is recorded on an L&A document. This includes touchscreens, optical scanners, and ExpressPolls. The form will include seal numbers as well as who conducted the test.
- Location/Owner: County Election Office.

Artifacts

- Object: Access Logs
- Function: Manual logs are maintained for each voting equipment storage facility and the office/location where the GEMS server is located. This log will record who accessed the devices, when, why, and who signed-off at the county level.
- Location/Owner: County Election Office

Artifacts

- Object: Audit Logs
- Function: The GEMS server will maintain two audit logs. One is the Windows Server log. This will indicate when and by whom the server was accessed. This audit log is mapped to the access log.

GEMS maintains a separate log that records which databases were opened and what operations were performed on that database, including memory card activities.

- Location/Owner: These audit logs resides on the GEMS server and should only be pulled by Center personnel.

Artifacts

- Object: Audit Logs (continued) - Touchscreen
- Function: The TS audit log records all high level activities (not individual vote selections) on the TS unit, including opening and closing of polls. Can be used to determine at what time an election was ended on a TS unit and the total number of cast ballots on the unit at the ending time.
- Location/Owner: The TS audit log resides on the TS unit and should only be pulled by Center personnel.

Should be public record.

Artifacts

- Object: Voter Access Cards - Yellow with State Seal.
- Function: Are programmed with the code that brings up the appropriate ballot for a voter and with a counter that is set at 1 when the card is created and 0 once the ballot is cast. Cards can be viewed to determine the status of the vote cast field. No voter information is on the card. The current issue of the card has one 1/64" hole in the center column of the State Seal.
- Location/Owner: County Election Offices. Center personnel can use a card reader and software to review the card's contents.

Artifacts

- Object: Voter Access Cards - Yellow with State Seal.



Artifacts

- Object: Supervisor Card – Green with State Seal
- Function: Used to permit poll managers to access certain functions on the TS units. Each county's PIN is unique and changed every two years.
- Location/Owner: County Election Office. Center programs cards every two years. Currently, cards are being programmed by KSU. When complete all updated cards will have a total of four 1/64" holes; two of which will be in the bottom corners of each card.

Artifacts

- Object: Supervisor Card – Green with State Seal



Merle S. King
mking@kennesaw.edu