Policy Mechanisms for Increasing Transparency in Electronic Voting

by

Joseph Lorenzo Hall
B.S. (Astrophysics, Northern Arizona University) 2000
M.A. (Astrophysics, University of California, Berkeley) 2003
M.I.M.S. (Information, University of California, Berkeley) 2005

A dissertation submitted to the Graduate Division
of the University of California at Berkeley
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in
Information Management and Systems

Committee in charge:
Professor Pamela Samuelson, Chair
Professor Coye Cheshire
Professor Deirdre Mulligan
Professor David Wagner

Fall 2008

The dissertation of Joseph Lorenzo Hall is approved.

Professor Pamela Samuelson (Chair)	Date
Professor Coye Cheshire	Date
Professor Deirdre Mulligan	Date
Professor David Wagner	Date

University of California, Berkeley
Spring 2008

Policy Mechanisms for Increasing Transparency in Electronic Voting

Joseph Lorenzo Hall

Abstract

Policy Mechanisms for Increasing Transparency in Electronic Voting
by
Joseph Lorenzo Hall

Doctor of Philosophy in Information Management and Systems
University of California, Berkeley
Professor Pamela Samuelson, Chair

In the early years of the American republic, only white male landowners could vote, and then typically by expressing their preferences in a public setting, for all to witness. Our electoral system has changed drastically since that time; now almost all Americans cast votes with the assistance of computerized equipment. While much good stems from the use of computerized equipment in elections—notably increased efficiency, enfranchisement and flexibility—unintended consequences of this mechanization have left us with complicated, insecure and opaque voting systems.

My PhD thesis focuses on the issue of transparency in e-voting; that is, what public policy mechanisms can serve to make our voting systems less opaque? After exploring what we mean by "electoral transparency", I examine the question of e-voting transparency on three fronts. I analyze the role of disclosed and open source software in election systems and conclude that, while fully disclosed source code is a valid goal, limited disclosure to experts serves many of the same goals in the short-term while preserving vendor trade secrecy. I investigate how contractual provisions between local election jurisdictions and voting system vendors serve to frustrate transparency and find that election officials need to be more careful in these negotiations. Finally, I turn to the question of auditing black box elections systems; that is, since we cannot know how these systems work in the full-disclosure ("white box") case, possibly because of contractual provisions that limit investigation, what methods and procedures can we use for "checking the math" behind our elections?

Professor Pamela Samuelson

This dissertation is dedicated to those who have supported my work:

Michelle, my family and each of my mentors.

CONTENTS

Preface

When I began research into voting technology and election administration, I was surprised at the complexity of the subject. Something we rely on as the primary mechanism for directing our government is, unfortunately, still poorly understood and an active area of research. As someone who has always been interested in issues of secrecy, security, control and access to information, I was concerned that neither average voters nor seasoned experts could explain exactly how the machinery of our democracy functions.

In this dissertation, I have attacked the opacity of voting system technology along three axes: access, oversight and accountability. Over the five years of work on my dissertation, I worked to make solid contributions towards increasing transparency through research that aims to make our elections system more tractable, understandable and accountable.

Acknowledgments

The members of my qualifying and thesis committees are due a special thanks for their mentoring during the development of my thesis. My family and my partner, Michelle, were bastions of unwaivering support, the likes of which every young scholar should enjoy.

This material is based upon work supported by the National Science Foundation under A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), Grant Number CNS-0524745. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

The following sections acknowledge the work of individuals specific to each published chapter in this thesis.

Acknowledgments for Chapter 2

A very special thanks to my legal supervisor and mentor, Deirdre K. Mulligan; without her advice and direction, this work would only have been a shadow of itself. Discussions with the following people were important in the development of this work: Pam Samuelson, Eddan Katz, David Molnar, Ka-Ping Yee, Pam Smith, Naveen Sastry, Dan Wallach, Michael Shamos and Mitch Kapor.

Acknowledgments for Chapter 3

I would like to acknowledge the assistance of Aaron Burstein, Kim Alexander, Larry Norden, Ray Martinez, Deirdre Mulligan, Dan Wallach, Dan Sandler, Bev Harris, and the computing staff of the UC Berkeley School of Information, without which scanning and OCRing thousands of pages of contracts would have been unthinkable.

Acknowledgments for Chapter 4

The Brennan Center and the Samuelson Clinic thank Alex Yacoub, a student at New York University School of Law, for his substantial legal analysis, as well as his extensive review and edits of this work. We also thank Policy Analyst Kahlil Williams and Research Associate

Vijay Das of the Brennan Center, and Common Cause legal interns David Fialkov and Lindsay Frischer for their comments and research assistance. This work benefited greatly from the insightful and thorough editorial assistance of Deborah Goldberg, Director of the Brennan Center's Democracy Program.

We are grateful to John McCarthy of the Verified Voting Foundation for his many helpful suggestions and ideas for improving this study. We thank David Jefferson, Chair of the California Post-Election Audit Standards Working Group and computer scientist at the Lawrence Livermore National Laboratory's Center for Applied Scientific Computing, and Robert Kibrick, Legislative Analyst at the Verified Voting Foundation for their careful review of drafts of this work and substantive feedback. Pamela Smith, President of the Verified Voting Foundation was an indispensable resource with an extensive knowledge of state audit laws. We also thank Lee Mosher, Professor of Mathematics and Chair of the Department of Mathematics and Computer Science at Rutgers, the State University of New Jersey for his participation in conversations about post-election audits and this work.

The participation of Aaron Burstein and Joseph Lorenzo Hall is made possible by the support of the National Science Foundation under A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), Grant Number CNS-0524745.

Generous grants to the Brennan Center from an anonymous donor, the Carnegie Corporation of New York, the Ford Foundation, the HKH Foundation, the JEHT Foundation, the Knight Foundation, the Open Society Institute, the Rockefeller Family Fund, and the Tides Foundation supported the development and publication of this work. Opinions, findings, and conclusions or recommendations expressed in this work are the responsibility solely of the authors and the Brennan Center.

Acknowledgments for Chapter 5

Considering the almost 2-year time period over which this research was conducted, there are many contributors to acknowledge. Close collaborators in this work included Kim Alexander, Aaron Burstein, Arel Cordero, David Dill, Deirdre Mulligan, Philip Stark and David Wagner. This work would have not been possible without the cooperation and patience of local

and state election officials and their staff, such as Warren Slocum, David Tom, Theresa Rabe, Freddie Oakley, Tom Stanionis, Elaine Ginnold, Dave MacDonald, Jennie Bretschneider, Lowell Finley and California Secretary of State Debra Bowen. In the process of completing this work, the author found discussions with the following people helpful: Judy Bertelsen, Tim Erickson, Michelle Gabriel, Candice Hoke, Meg Holmberg, David Jefferson, Bob Kibrick, Mark Lindeman, John McCarthy, Lawrence Norden, Dennis Paull and Pam Smith.

CHAPTER 1

INTRODUCTION & BACKGROUND

1.1 How Elections Have Changed

Elections have changed considerably over the course of American history. In the beginning, only certain Americans were permitted to vote and the method they used to vote was quite simple.[1] Voters initially consisted entirely of white male landowners and they would often vote *viva voce*, meaning they would speak their preferences aloud in a public venue. This method offered a number of advantages, notably observers could convince themselves that a given person was permitted to vote. Also, since observers could keep their own tally of how each individual voted, there was little need for complicated methods of privacy-preserving tallying; observers would be able to tell immediately if the announced result differed from what they observed. Finally, the contents of ballots were much more simple, often consisting of only a few contests.[2]

Elections today are remarkably different. We have removed restrictions on the franchise tied to property ownership, gender and race while also specifically seeking to enfranchise voters who would normally not be able to vote, or at least voters who could not before vote privately and independently.

Over the mid- to late-nineteenth century, concerns with voter fraud motivated most jurisdictions to move to a secret ballot. Harris notes extensively that election fraud has been a recurring problem throughout our history.[3] As Albright discusses, ballots were for many

[1] Joseph P. Harris. *Election Administration in the United States*. The Brookings Institution, 1934. URL: http://vote.nist.gov/harris_electadmin/harris_6.pdf.

[2] Spencer D. Albright. *The American Ballot*. American Council on Public Affairs, 1942. URL: http://josephhall.org/albright_american_ballot.pdf.

[3] Chapter IX of Harris, see n. 1.

years produced by political parties for fixed slates of candidates on colorful paper, often serving to identify voters' choices from a distance.[4] This would end with the introduction of the secret ballot—where the voter's identity and choices were no longer connected—and then the Australian ballot—where the government produces uniform ballots cast in secret.

Our elections are also now more complex. Population growth coupled with movement from rural agricultural communities to a concentrations in and around urban centers has meant that many more people vote, in much larger densities. To accommodate these changes, our representative form of government has come to operate on at least four levels: Federal, State, Local and Sub-local. That is, in addition to casting votes to elect representatives at the Federal level, we also vote on State-level offices and ballot initiatives, local level offices and initiatives and the sub-local types of offices and initiatives such as, for example, water districts and school bond issues. This can mean very long ballots, in some cases up to four pages long, front and back.[5] The areas on the map corresponding to all these elected offices and questions are not necessarily aligned, so even within a given precinct, there may be voters eligible to vote in different races that must be provided different ballot styles.

Election technology and technologists have endeavored to deal with these difficulties since the mid-19th century. Patents for voting machines used in legislative chambers appeared as early as 1840 and their polling place cousins a few decades later.[6] Voting machinery was, at that time, seen as a cure for election frauds such as ballot box stuffing. While the new election machinery did make those types of activities much more difficult to perpetrate, they also tended to centralize key pieces of election administration, facilitating new types of fraud involving colluding election officials. Mechanical lever machines evolved from simple types that could only display a few races to much more complex models that could handle essentially an arbitrary number of contests per ballot.[7]

---

[4] Albright, see n. 2, at 20-30.

[5] The City of Berkeley might have just such a ballot in the November 2008 General Election (Alameda County Registrar of Voters, Dave MacDonald, *personal communication*). This is due to a record number of 11 ballot initiatives, many individual state and local offices and the Berkeley Mayoral race which requires three times its normal space (in order to implement the "instant-runoff" method of voting on an optical scan paper ballot).

[6] Douglas W. Jones. "Technologists as Political Reformers: Lessons from the Early History of Voting Machines". In: *Society for the History of Technology Annual Meeting*. 2006. URL: `http://www.cs.uiowa.edu/~jones/voting/SHOTpaper.pdf`, at 2–3.

[7] Here is an example of a small lever voting machine, probably used for demonstration purposes, owned by

Lighter and cheaper solutions to lever machines, the punchcard and the optical scan system, became popular between 1950-1965.[8] Punchcard voting involves using a stylus or hole-punch to pierce holes in a ballot corresponding to named or numbered choices. Optical scan voting has the voter fill in a bubble on what appears to be a normal ballot. In both cases, the marked or pierced ballots are deposited into a conventional ballot box and "scanned" later, in bulk, by scanning equipment which can detect the presence of a mark and associate that mark with a contest choice.

However, even the high-capacity lever, punchcard and optical scan voting systems lacked features that have become increasingly important in recent years. The requirements discussed above in terms of permitting the disabled to vote privately and independently as well as support for alternative voting languages put pressure on voting system vendors to produce new voting systems. Computerized voting systems could display many languages, many ballot styles and also support various disabilities, with a particular emphasis on blindness and manual dexterity disabilities.

The background provided here has been necessarily brief. A more thorough accounting of the background upon which current voting systems have been built can be obtained through the works cited so far in this section. Roy Saltman, who has been involved with electromechanical and computerized voting systems since the 1960s, has recently published what is perhaps the definitive work on the recent history of voting systems.[9]

San Mateo County, CA, made by the Shoup Voting Machine Corporation: http://www.flickr.com/photos/joebeone/2293493872/. Here is an example of the last generation of lever voting technology: http://www.cs.rice.edu/~dwallach/photo/avm-lever/.

[8] See: Ed Arnold. *History of Voting Systems in California (unpublished)*. California Secretary of State (Bill Jones), 1999. URL: http://josephhall.org/arnold_ca_vs_hist.pdf, at 28–33. In fact, in the late 1950s the county of Los Angeles commissioned the Norden Division of United Aircraft, at a development price of one million dollars ($8 million in 2008 dollars), to invent a faster and less cumbersome method of counting ballots, which became the optical scan or "mark-sense" voting method. While Los Angeles did not use this system due to their recurring problems with ballot complexity, optical scan voting systems have enjoyed abundant use. (Arnold, see n. 8, at 25)

[9] Roy G. Saltman. *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. Palgrave Macmillan, 2006. ISBN: 1403963924. URL: http://www.palgrave-usa.com/catalog/product.aspx?isbn=1403963924.

1.2 A Brief Aside: How I Got Involved

To understand why I chose the projects for this thesis, the reader might be interested in hearing how I originally became involved with voting technology.

My interest in voting systems started about 5 years ago, in the Fall of 2003. That Fall, I had watched with some interest how a particular voting system vendor, Diebold Election Systems, Inc. (DESI)—now Premier Election Solutions, Inc. (PESI)—had used copyright law to quash discussion about a leak from their company.[10] In particular, students had posted a set of email archives containing technical support and bugtracking mailing lists internal to DESI. DESI's legal team sent what are called "notice and takedown" letters under Section 512 of the Digital Millennium Copyright Act (DMCA) to compel removal of the material from each student's website. This provision of the DMCA allows copyright holders to send a notice to internet service providers (ISPs) when they find material they believe to be infringing their copyrights.

The students involved with posting these documents began to retaliate against these legal threats by organizing what they called a "whack-a-mole" protest.[11] This is to say that when one student would get a notice from DESI legal and be forced to take down the email archive, other students would put the archive up on their own page, creating an almost perpetual availability of the leaked documents.

At one point, in late December of 2003, DESI legal had actually been quite successful at keeping up with whacking the student moles. When an undergraduate friend of mine from Harvard, Derek Slater, received a takedown notice and had to remove his copy of the memos archive, a few of us at Berkeley also felt that it was a critical time to continue the online protest. A number of students, notably Sean Savage (SIMS),[12] Parker Thompson (SIMS), Ping Yee (CS) and myself, decided to host the memos and risk also being "whacked". Curiously, I was the only one of the three to receive a 512 notice from DESI legal (for a copy,

[10] Declan McCullagh. "Students buck DMCA threat". In: *CNET News.com* (Nov. 2003). URL: `http://www.news.com/2100-1028_3-5101623.html`.

[11] Whack-a-mole is named after a popular arcade game where the object is to *whack* each *mole* as they poke their heads out of their holes. See: Wikipedia. *Whac-A-Mole — Wikipedia, The Free Encyclopedia*. 2008. URL: `http://en.wikipedia.org/w/index.php?title=Whac-A-Mole&oldid=227078062`.

[12] The current UC Berkeley School of Information was formerly known as the School of Information Management and Systems (SIMS).

see Appendix A), despite Ping going so far as creating a step-by-step guide for hosting the memos and processing the memos to make them easier to read.[13]

Having spent the Fall 2003 semester enrolled in the Samuelson Law, Technology and Public Policy Clinic at Berkeley Law, I was intimately familiar with the DMCA Section 512 notice and takedown process. After receiving some informal legal advice from Matt Zimmerman (then of the Free Speech Project), I chose not to contest the notice I received as it wasn't clear to me, at the time, that we were making fair use of the memos. However, the Electronic Frontier Foundation (EFF) and the Center for Internet and Society Cyberlaw Clinic at Stanford Law School filed a lawsuit to challenge DESI's copyright claim. After various legal maneuvers, a California district court found that the email archive was likely not protected by copyright and that, in sending the takedown notices, Diebold had violated part of the DMCA which forbids sending takedown notice when the copyright holder knows there has been no infringement.[14]

The underlying lessons from this experience were: 1) DESI seemed willing to use questionable legal threats to prohibit the further distribution of the email archive; and, 2) the contents of the email archive were sensitive from DESI's perspective. Later on the same year, the true implications of the contents of the email archive became known when DESI was implicated and then found to have used software that was uncertified by the State of California.[15]

The entire purpose of this section is to emphasize what interested me in electronic-voting: as we've seen in many other areas unrelated to e-voting, intellectual property law

[13] Ka-Ping Yee. *Diebold, Hear This: We Won't Rest (a step-by-step guide to participating in the DESI memo protest).* 2003. URL: http://web.archive.org/web/20071105012922/http://people.ischool.berkeley.edu/~ping/diebold/.

[14] *OPG, Pavlosky & Smith v. Diebold.* 337 F.Supp.2d 1195 (N.D. Cal. Sept. 30, 2004). URL: http://www.eff.org/files/filenode/OPG_v_Diebold/OPG%20v.%20Diebold%20ruling.pdf; *Case Archive for Online Policy Group v. Diebold.* The Electronic Frontier Foundation. 2004. URL: http://www.eff.org/cases/online-policy-group-v-diebold.

[15] See: Kim Zetter. "Did E-Vote Firm Patch Election?". In: *Wired News* (Oct. 2003). URL: http://www.wired.com/politics/law/news/2003/10/60563. In fact, it appears that all vendors in California had been deploying voting systems running uncertified software. See: Joseph Lorenzo Hall. *More Uncertified Voting Systems in California? (unpublished).* Aug. 2007. URL: http://www.josephhall.org/nqb2/index.php/2007/08/22/certmess2003; Jocelyn B. Whitney. *Subject: State Certification and Federal Qualification of County Voting System Components.* R&G Associates LLC. Apr. 2004. URL: http://web.archive.org/web/20041108232732/http://www.ss.ca.gov/elections/ks_dre_papers/randgsummary.pdf; Jocelyn B. Whitney. *Revised Phase II - County Voting System Review.* R&G Associates LLC. Apr. 2004. URL: http://web.archive.org/web/20041108230726/http://www.ss.ca.gov/elections/ks_dre_papers/rg_phase_II_revised_report.pdf.

was being used to remove discussion, criticism and analysis of technical systems from the public sphere. This was particularly paradoxical: In an area that entirely depends on transparency for democratic legitimacy, elections, vendors and election officials had been overly protective of the machinery on which our democracy is run. Shortly afterwards, I began research related to e-voting policy with Deirdre Mulligan. In 2005, we were part of a team that applied for and received a Center-Level CyberTrust Grant from the National Science Foundation to found A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE).[16]

1.3 What is Governmental Transparency?

> "Like many other notions of a quasi-religious nature, transparency is more often invoked than defined, and indeed might ironically be said to be mystic in essence, at least to some extent." —Christopher Hood[17]

Transparency is a concept that people use often but rarely define. As a word applied to notions of open governance, it has only been in active use for a few decades, specifically after the passage of freedom of information acts such as our Freedom of Information Act and Sunshine Act of 1976. Hood notes that Jonathan Bentham was the first to use transparency in its modern governance-related sense when he talked about "transparent-management or publicity" in the 1790s with his *Panopticon* work, but that the word did not enjoy more widespread use until the 1980s.[18]

What do people mean when they use the word transparency? As Heald points out, even though people often call for "more" transparency, they are really concerned with directions of transparency—vertical or horizontal and external or internal to an entity—and varieties of transparency—event vs. process transparency, real-time vs. *post hoc* transparency and symbolic vs. effective transparency.[19] In addition to directions and varieties of transparency,

[16] See: `http://accurate-voting.org/`

[17] Christopher Hood. "Transparency in Historical Perspective". In: *Transparency: The Key to Better Governance?* Ed. by Christopher Hood and David Heald. The British Academy, 2006. Chap. 1, 3–23, at 3.

[18] Hood, see n. 17, at 9, 15–16. Of course, the various elements making up more modern notions of transparency are much older; e.g., the idea that governing entities should act in a noncapricious manner can be traced back to historical China and Greece.

[19] David Heald. "Varieties of Transparency". In: *Transparency: The Key to Better Governance?* Ed. by Christo-

Hood notes three dimensions of transparency: interactions operating under open discourse, fairness based on process consistency and accountability in the distribution of resources.[20]

From this literature on transparent government, I have boiled down these various ideas into a more streamlined definition of electoral transparency from the perspective of a voter, including four elements.

> "A fully transparent election system is one that supports *accountability* as well as *public oversight*, *comprehension* and *access* to the entire process."[21]

I explain these four elements, three somewhat objective and one entirely subjective, in turn.

Access: The most basic element of transparency is access. Voters should be able to get access to basic information about their electoral system, voting system and procedures used to conduct elections.

Oversight: Closely related to Heald's "effective transparency", the element of oversight means that a voter has the information they need to participate effectively and convince themselves that processes, people and machinery are working as intended. This can also be thought of as *meaningful* access; that is, someone may have threshold access to pieces of the system but not all the pieces they need to effectively monitor government action.

Accountability: Moving into the policy realm, in order for access and oversight to be truly meaningful, there need be appropriate mechanisms for acting upon both positive and negative issues that access and oversight expose. Specifically, the people, process and technology involved in elections should be rewarded and recognized when things go well and they should be reprimanded and revised when things do not go well.

Comprehensibility: The final element of transparency, comprehensibility, is highly subjective depending on the voter in question. Voters need to be able to understand how the elections system works, or trust someone that does. Considering the complexity of the U.S. elections system and the extent to which we aim to achieve maximal enfranchisement, this

---

pher Hood and David Heald. The British Academy, 2006. Chap. 2, 25–43.

[20] Hood, see n. 17.

[21] Joseph Lorenzo Hall. "Transparency and Access to Source Code in Electronic Voting". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2006* (June 2006). URL: `https://www.usenix.org/events/evt06/tech/full_papers/hall/hall.pdf`, at 2.

can be a very difficult property to achieve. It becomes especially difficult for certain types of voters; for example, voters with mental disabilities often have difficulty understanding even the most basic concepts, but should be allowed to vote if they can perform the action of casting a vote and understand, at a high level, what "voting" means.[22]

1.4 How Might We Begin to Increase Transparency?

Through the lens of the above definition, I have structured a set of projects that tackles discrete issues with each of the three objective elements of transparency. In terms of access, I examine the role that disclosed and open source software can play in electronic voting (see Chapter 2). I conclude from this analysis that governmental entities should not simply mandate disclosure or unilaterally disclose source code, but consider offering incentives for vendors to move in this direction. I also note that many of the benefits of source code disclosure can be achieved through limited (non-public) disclosure to experts. As the results of the original project were published in 2006, I've updated this work with comments on how exactly the mode of disclosure I recommend has borne fruit with a slew of expert reviews of voting system source code.

For the oversight element, I study how procurement agreements between voting system vendors and state and local jurisdictions limit the nature of information that a jurisdiction can make available to voters (see Chapter 3). Although limited by a convenience sample, I am able to make a number of observations about how procurement contracts can limit as well as enable more effective oversight of voting systems: from the most basic suggestion such as making explicit that the contract itself is public to the more complicated notion that the contract should permit certain types of analyses of the voting system. Since the publication of this work in 2007, I have begun a more extensive contracts analysis project, with my ACCURATE colleague Aaron Burstein, to systematically sample a large set ($N \sim 600$) of jurisdictions stratified by population. In addition, we have since assisted a number of jurisdictions—including San Francisco County, Californa; the State of Hawaii; and Cuyahoga

[22] Jason H. Karlawish, Richard J. Bonnie, Paul S. Appelbaum, et al. "Addressing the Ethical, Legal, and Social Issues Raised by Voting by Persons With Dementia". In: *Journal of the American Medical Association* 292 (2004). 1345–1350. URL: http://jama.ama-assn.org/cgi/reprint/292/11/1345.pdf.

County, Ohio—in negotiating better voting system contracts.

Finally, to further the accountability element of transparency, I have engaged in two separate projects involving post-election audits.[23] The first project was to review, at a high level, the increasingly expansive literature on models of conducting post-election audits of voting systems (see Chapter 4). Audits of voting systems that produce paper records are becoming important as the majority of states have passed laws mandating that their voting systems produce paper records that voters can verify before casting their ballots. In our review, we examine fixed-percentage audits, tiered-percentage audits, variable-percentage audits and what we call "polling" audits. We conclude that variable-percentage audit models with a fixed-percentage floor best serve to meet the various goals involved in audits of paper records.

In the second auditing project, I examined, at a considerably lower level, the actual procedures used in conducting post-election audits (see Chapter 5). My aim in this project was to examine actual procedures used in elections in order to develop a more tight coupling between what observers can observe, the written procedures governing the process and what actually occurs during the process. This project involved collaborators with expertise in information security and systems verification and expanded to encompass security aspects of manual tally procedures. In addition, it became important to "give something back" to the election officials that cooperated with us in this research, and their interests are reflected through increased efficiency of their procedures. The result from this project is a set of procedures for the manual tally that any California jurisdiction can use in whole or in part to improve their existing procedures.

[23] As I note later, the term "post-election audit" has unfortunately come to mean something much more narrow than might be expected. Here we use it to mean post-election manual tallies of paper records where the manual tally is compared against tallies produced by election management software. (Election management software is the software that aggregates and tabulates votes in modern computerized voting systems.)

CHAPTER 2

TRANSPARENCY AND ACCESS TO SOURCE CODE IN ELECTRONIC VOTING

> "Moving decisions from the smoke-filled rooms of power brokers to the caffeine-fueled rooms of programmers is not progress in terms of transparency."
> —L. Jean Camp[1]

In this Chapter, we examine the potential role of source code disclosure and open source code requirements in promoting technical improvements and increasing transparency of voting systems.[2]

2.1 Introduction

Elections, like many aspects of society in the United States, have changed dramatically over the course of history. With the growth of urban areas during the last century, and passage of various federal and state laws that specify increased electoral enfranchisement of citizens, we are placing greater and greater demands upon voting technology and election administration. In the past few decades we have started to use computers and networking to further increase efficiency. The most fundamental act of our democracy—the mechanics of casting and counting ballots on election day—that initially took place in plain sight and was

[1] L. Jean Camp. "Varieties of Software and their Implications for Effective Democratic Government". In: *Transparency: The Key to Better Governance?* Ed. by Christopher Hood and David Heald. The British Academy, 2006. Chap. 11, 183–195, at 194.

[2] The material in this chapter is based on work originally published in 2006. See: Joseph Lorenzo Hall. "Transparency and Access to Source Code in Electronic Voting". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2006* (June 2006). URL: https://www.usenix.org/events/evt06/tech/full_papers/hall/hall.pdf.

fully comprehensible to the franchise now takes place within machines that foreclose observation and obscure this formerly fully comprehensible act. An electoral system that was once highly transparent—supporting public scrutiny and ease of understanding its functions and policies—has undergone an "enclosure of transparency". That is, much like the enclosure movement in English history where public land was increasingly privatized, the requirements to which we hold our voting technologies have resulted in a gradual "fencing in" of transparency.[3] Voting system software is one of the most opaque aspects of electronic voting as it is often large, complex and generally unavailable for inspection. Unsurprisingly, academics, activists, election officials and commentators have called for increased access to, and heightened examination of the source code that powers election systems. Efforts to increase access and scrutiny range from source code escrow requirements,[4] independent code reviews,[5] system performance testing,[6] required disclosure of source code to requirements that systems use open source code.[7]

Efforts to broaden the number of individuals with access to the source code of election technology are part of a larger project of increasing the trustworthiness and transparency of electronic election systems. This larger project focuses on both technical improvements that increase security, accuracy, privacy, reliability, usability and reforms—at some level independent of technical improvements—that instill confidence in the voting public by facilitating public oversight, comprehension, access and accountability. As such, calls for source code disclosure to the public or to a set of independent experts should be measured

[3] See Sec. 2.2.

[4] Source code escrow involves depositing the source code for a voting system with a third party and/or an election official and stipulating under what conditions the source code can be released. See the discussion of source code escrow in note 45.

[5] A state election official may reserve the right to ask an independent party to do source code review on top of what is done at the federal certification level.

[6] Performance testing involves testing a system in conditions similar to those used on election day.

[7] A note on terminology: There are three important distinctions to make in this discussion. The difference between *open source development* and *releasing commercially developed code under an open source license* is important as these are two modes that we see clearly in voting systems (see discussion of eVACs in Sec. 2.7.1). Open source software is software that is usually developed by a team of volunteers and released under generous licensing terms that allow users to exercise a number of rights, such as copying, modification and distribution, which traditional software licenses withhold. (The Open Source Initiative (OSI) issues and Open Source certification mark to software licenses that follow their Open Source Definition: `http://www.opensource.org/docs/definition.php`.) In contrast to both open source development and releasing software under an open source license, *disclosed source* code allows a much more limited use of source code, usually for evaluation purposes only and without permissions to make further copies, modify works or distribute. For example, see VoteHere's license agreement: `http://www.votehere.net/VoteHere_Source_Code_License_2.htm`.

along a number of related but independent axes:

- What role could access to voting system source code play in increasing the transparency of voting systems?
- What are the risks and benefits of open source and disclosed source regimes for security and the market?
- If open source code offers measurable benefits, what regulatory and marketplace barriers exist to the development of open source software in the voting systems environment?
- What business methods from the landscape of open source software may translate to voting systems?
- Are there alternatives to public disclosure of code or open source code requirements that might yield similar benefits in technology performance and increased transparency, but minimize potential risks posed by source code disclosure?

This chapter examines the potential role of source code disclosure and open source code requirements in promoting technical improvements and increasing transparency of voting systems. Section 2.2 reiterates what we mean by transparency and then elaborates on the concept of the "enclosure of transparency" of voting technology. Section 2.3 explores what implications source code disclosure might have for values associated with transparency. Section 2.4 details the negative effects that the enclosure of transparency has had at various levels. Section 2.5 reviews recent efforts to increase the capacity for public scrutiny of voting systems through disclosed and open source code regulation and legislation. Section 2.6 examines the benefits and risks of open and disclosed source code regimes in the voting systems context and considers additional issues posed where access rules are driven by regulation rather than the market. Section 2.7 reviews past and current efforts to provide open source voting systems and contemplates which existing open source business models might translate to the voting systems context. Section 2.8 then considers regulatory and market barriers to disclosed or open source code voting systems. Section 2.9 reviews what trans-

parency and trustworthy-promoting alternatives might exist outside of public disclosure of source code.

We conclude that disclosure of full system source code to qualified individuals will promote technical improvements in voting systems while limiting some of the potential risks associated with full public disclosure. Acknowledging that this form of limited source code disclosure does not support general public scrutiny of source code, and therefore does not fully promote the transparency goals that we have articulated, we note that in a public source code disclosure or open source code model most members of the public will be unable to engage in independent analysis of the source code and will need to rely on independent, hopefully trusted and trustworthy, experts. Given the potential risks posed by broad public disclosure of election system source code, we conclude that moving incrementally in this area is both a more realistic goal and the prudent course given that it will yield many benefits, greatly minimizes potential risks and provides an opportunity to fully evaluate the benefits and risks in this setting.

2.2 The "Enclosure of Transparency" of Voting Technology in the U.S.

Early vote casting in the United States was essentially a show of hands or voice vote in front of an official body. In small or even moderately sized towns, it was possible to keep one's own records and do an independent tally of the vote. Of course, this ultimate level of elections transparency in early America had serious implications for voter privacy, coercion and vote selling.[8]

The extreme example of elections in early America allows us to better define what we mean by "transparency": a fully transparent election system is one that supports *accountability* as well as *public oversight*, *comprehension* and *access* to the entire process. This notion of transparency is the core principle of democratic governance; when voters can easily

[8] Arthur M. Keller, David Mertz, Joseph Lorenzo Hall, and Arnold Urken. "Privacy Issues in an Electronic Voting Machine". In: *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Ed. by Katherine J. Strandburg and Daniela Stan Raicu. Springer Science+Business Media, 2006. 313–334. URL: http://josephhall.org/papers/privacy-electronic-voting-chapter.pdf.

access and comprehend election processes and have the opportunity to observe election-related actions, they are directly exercising their democratic right to hold the system and its pieces accountable.

The private ballot, aimed at eliminating coercion, was one of the first major changes to the U.S. voting process and eventually the Australian ballot[9] took hold throughout the vast majority of U.S. states.[10] This helped lessen problems such as biased ballot design, denying ballots to certain groups of people and simple as well as sophisticated forms of vote-selling and voter coercion. Today, all states save West Virginia[11] provide for "secret" or "private" ballots. The requirements to support public scrutiny in a system with secret ballots include ensuring that each voter casts one ballot, that the container in which ballots are cast is initially empty at the beginning of voting, and that no ballots are modified or introduced into the container after the voting is closed. In a paper ballot system, these are largely chain-of-custody concerns and can be ensured by scrutinizing the process and ensuring that there are two people from different parties with the ballot materials at all times.

Due to increasing complexity in counting and casting votes during the last century, voting technology has become mechanized. A number of factors have contributed to this move towards mechanization. Citizens have moved from rural to dense urban areas, causing the number of ballots in cities to increase remarkably. Ballots have become more complex; they often have federal, state and local contests on a single ballot, they often vary from precinct to precinct and they can vary by political party for primary elections.[12] This makes designing and hand-tallying paper ballots difficult and inefficient. Finally, statutory accessibility requirements under state and federal law stipulate accommodations that must be made for voters who don't read or understand English and for voters with physical and mental

[9]The Australian ballot provides for a uniform ballot, free from bias in design and presentation, printed by the government and cast in secret.

[10]Keller, Mertz, Hall, and Urken, see n. 8, at 2.

[11]West Virginia allows "open voting" whereby a citizen may choose to show their marked ballot to whomever they choose (W.V. CONST. ART. IV, Sec. 4, cl. 2.). Interestingly, West Virginia also makes it a crime to sell or buy votes. (W.V. CODE 3-9-13(a) & (b))

[12]For example, in Cuyahoga County, Ohio—which is not required under the Voting Rights Act to provide ballots in non-English languages—there were over 6,000 ballot styles provided to voters in the 2006 primary election. See: Candice Hoke, post to the *Election Law listserv*, available at: http://majordomo.lls.edu/cgi-bin/lwgate/ELECTION-LAW_GL/archives/election-law_gl.archive.0605/date/article-63.html

disabilities.[13]

This mechanization and computerization has had profound consequences. On the positive side, election administration has become more efficient as large quantities of paper no longer need to be produced, counted and stored securely. The counting process itself is quicker and many non-English language speakers and persons with disabilities can be accommodated with a single piece of equipment.

Increased mechanization has disadvantages. Flaws with current voting technologies spur concerns that we were too quick to embrace the productivity-enhancing features of computerized technology while not recognizing the vulnerabilities to which this new technology exposes our electoral system.[14] A more general concern is that the transparency that was at one time a necessary feature of casting and counting votes has been all but lost. Similar to how common property in England during the fifteenth through nineteenth centuries underwent a series of enclosure movements where a public good—common land—was gradually removed from the public sphere, the notion of transparency in the voting franchise has been progressively removed from the electoral franchise.[15] This "enclosure of transparency" has made the mechanisms of the electoral process opaque to the individual voter or, more importantly, even their trusted representative. When "counting votes" consists of running proprietary software to process proprietary vote data, voters can no longer "observe" the canvass process. Nor can regulators or experts, with whom the public places its trust, easily gain access to and evaluate whether votes are being counted as they were intended to be cast.

[13]Relevant authorities include the Voting Rights Act of 1965, Public Law 89-10 (VRA), The Americans with Disabilities Act of 1990, Public Law 101-336 (ADA), Voting Accessibility for the Elderly and Handicapped Act, Public Law 98-435 and The Help America Vote Act of 2002 Public Law 107-252 (HAVA).

[14]T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. "Analysis of an electronic voting system". In: *Proceedings of the IEEE Symposium on Security and Privacy* (2004). 27–40. URL: `http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1301313` at 27.

[15]The "enclosure" metaphor has also been extended by legal scholars to apply to recent efforts to reduce the amount of material in the public domain. James Boyle. "The Second Enclosure Movement and the Construction of the Public Domain". In: *Law and Contemporary Problems* 66 (2003). 33–74. URL: `http://ssrn.com/abstract=470983`

2.3 The Implications of Source Code Availability for Transparency

In Sec. 2.2 we defined electoral transparency to have four primary aspects: access, oversight, accountability and comprehension. Disclosed and open source software support access to the system by allowing a greater sphere of individuals the ability to scrutinize the detailed workings of a voting system. In the case of publicly available source, this access is to all members of the public. With limited disclosure, access is simply increased to a strategically chosen subset of the public to facilitate effective evaluation.

Access to source code supports independent technical evaluation of voting systems that, in turn, facilitates oversight and accountability of software. With access to source code and design documentation, system evaluators can see and analyze each element that goes into building the binary executable which runs on a voting system during the election process.[16] They can recompile the code in different manners to facilitate ease of testing and tracing where data goes during processing.

In addition to manual source code review, there are many bug-finding software applications.[17] These tools are developed to automatically find bugs in software by examining source code files or dynamically while the software is running. Evaluators point these tools at large bodies of source code, such as the Linux codebase, and are making much progress at finding common programming errors and vulnerabilities.[18] If voting system software were available to bug-finding researchers, they could examine and perfect their tools further while increasing the integrity of the software. Of course, bug finding is just one example of security-increasing research applications that source code availability could catalyze.

There are also evaluation techniques outside of source code review. It is not impossible to evaluate binary versions of voting system software using techniques from reverse engi-

[16] Note that one essential component in this process is the "build environment". The build environment consists of all compilers, linkers, libraries and other tools necessary to build the executable code from the source code software. Unfortunately, these elements have not been provided in recent state-level reviews conducted by California and Ohio, significantly limiting these analyses.

[17] For a partial list of bug-finding tools, see: List of tools for static code analysis, `http://en.wikipedia.org/w/index.php?title=List_of_tools_for_static_code_analysis&oldid=58643351` (last visited June 14, 2006).

[18] For an example of what can be done with automated source code analysis, see: K. Ashcraft and D. Engler. "Using programmer-written compiler extensions to catch security holes". In: *Proceedings of the IEEE Symposium on Security and Privacy* (2002). 143–159. URL: `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1004368` at 143.

neering; however, it makes the task more complex and prone to error.[19] There is a rich literature surrounding testing of computerized systems that incorporate unknown, "black box" components[20] and emerging work that seeks to greatly reduce the trusted base in voting systems.[21]

From a systems perspective, evaluation of code is not enough. Even in analyses outside of the national Independent Testing Authority (ITA) process (see section 2.4), critical flaws have been found that only become evident when testing the integrated system.[22] We must also include other techniques such as adversarial penetration testing,[23] parallel monitoring,[24] reliability testing and forms of feedback that we have in other areas of computing such as incident reporting and feedback.[25]

[19]For an example of work that has used binary analysis techniques to uncover vulnerabilities in executable applications, see: Fabrice Desclaux. *Skype uncovered: Security study of Skype*. EADS CCR/STI/C. Nov. 2005. URL: http://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf; Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. "Security Analysis of the Diebold AccuVote-TS Voting Machine". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2007* (2007). URL: http://www.usenix.org/event/evt07/tech/full_papers/feldman/feldman.pdf; Aggelos Kiayias, Laurent Michel, Alexander Russell, et al. *Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting*. Mar. 2008. URL: http://voter.engr.uconn.edu/voter/Reports_files/seeA-tamperEVoting.pdf

[20]For early work in this area, see: B. Beizer and J. Wiley. "Black Box Testing: Techniques for Functional Testing of Software and Systems". In: *IEEE Software* 13.5 (1996). 98. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=536464

[21]See text in Sec. 2.9.2 and notes 90-92.

[22]See the discussion of the *Hursti II* findings in Joseph Lorenzo Hall. *Background on Recent Diebold Election Systems, Inc. (DESI) Vulnerabilities*. National Committee for Voting Integrity Briefing for Congressmembers and Staff. 2006. URL: http://josephhall.org/papers/DESI_vulns_background_briefing-20060607.pdf. Also, see: *Top-To-Bottom Review of California's Voting Systems*. California Secretary of State. Aug. 2007. URL: http://www.sos.ca.gov/elections/elections_vsr.htm; Patrick McDaniel, Matt Blaze, Giovanni Vigna, et al. *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing (Academic Final Report)*. Dec. 2007. URL: http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf; *Software Reviews and Security Analyses of Florida Voting Systems*. Florida State University's Security and Assurance in Information Technology Laboratory. Feb. 2008. URL: http://www.sait.fsu.edu/research/evoting/index.shtml

[23]Penetration testing (sometimes called "Red team" or "tiger team" attacks) involve a simulated attack on a system where the attack team may know everything ("white box" testing) or very little ("black box" testing) about a system and attempt to compromise it in the same manner and environment as would a malicious actor. These types of exercises are common in the testing and implementation of high-integrity systems. For more on penetration testing rationales and methodologies, see: Open Source Security Testing Methodology Manual, available at: http://www.isecom.org/osstmm/.

[24]Parallel monitoring, employed during elections in the State of California, Washington and soon Maryland, involves randomly quarantining a subset of voting machines on election day and voting on them with fake voters and scripted votes to detect bugs, procedural flaws and evidence of possible malicious activity. For more, see: Douglas W. Jones. *Voting Systems: Parallel testing during an election*. The University of Iowa, Department of Computer Science. 2004. URL: http://www.cs.uiowa.edu/~jones/voting/testing.shtml

[25]For example, Carnegie Mellon University's Computer Emergency Response Team (CERT) is a computer security incident tracking and response service, see: http://www.cert.org/. In response to a question asked by the author at the NIST Voting Systems Threats workshop in 2005, EAC commissioners Davisdson and DeGregorio expressed interest in setting up a similar service and process for computerized voting systems. The EAC has since provided a forum for publishing reports commissioned by state-level election officials. See:

Of course, source code availability does not address comprehension; most voters will not gain any more insight into the operation of a voting system when source code has been made available to them. However, the mere fact that it is available and that they or a trusted representative could examine it will increase the level to which they trust these systems.

2.4 Enclosing Transparency Has Had Negative Effects

This increasing enclosure of transparency has negative effects on a number of levels. First, the voting public cannot see with their eyes or generally comprehend what is happening during the voting process. They have to trust that the voting system works without flaws and that the election official has implemented the voting system correctly.

In a similar vein, election administrators cannot observe what is happening in the depths of their election machinery. Even in cases where the official has access to the technical details of the system, they do not necessarily have the appropriate expertise and resources required to review the system. To provide the level of scrutiny required for their trust, election officials have historically relied on the national voting system standards and the associated ITA certification process, coupled with any additional state-level evaluation.

However, the national-level process has also suffered from lack of transparency. The process by which a voting system is state and federally approved to be fit for use in a local jurisdiction is widely believed to be inadequate and dysfunctional and is highly opaque. Existing Federal voting system guidelines are weak and out-of-date.[26] Federally certified voting systems have lost votes when used on election day[27] and critical parts of voting systems have made it through federal certification without being examined.[28] The federal certification process has relied on Independent Testing Authority (ITA) laboratories to test voting systems for compliance with the federal voting system standards and guidelines.[29]

http://www.eac.gov/program-areas/research-resources-and-reports.

[26] *Public Comment on the 2005 Voluntary Voting System Guidelines*. A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE). Sept. 2005. URL: http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf

[27] Associated Press. "More than 4,500 North Carolina Votes Lost Because of Mistake in Voting Machine Capacity". In: *USA Today* (Nov. 2004). URL: http://www.usatoday.com/news/politicselections/vote2004/2004-11-04-votes-lost_x.htm

[28] *Voting System Memory Card Issues*. National Association of State Election Directors. Mar. 2006. URL: http://www.nased.org/ITA%20Information/NASED%20Memory%20Card%20Report.pdf

[29] The set of federal standards that were in effect at the original time of writing were the FEC's 2002 Vot-

The ITAs are paid by the vendors and all communications and subsequent output from the ITA testing is considered confidential and protected under non-disclosure agreements (NDAs) by the vendors.[30] Vendors have claimed that the disclosure of information by the ITAs would implicate their intellectual property rights and compromise the security of their systems.[31] In part, the vendors object to sharing information from the ITA review process based on their desire to maintain "security through obscurity," a principle from computer science that has long been discredited.[32] Source code review by independent, dedicated evaluation teams improves system security; however, the circumstances of the evaluation and relationship between the parties involved should be carefully considered to maximize the utility of evaluation and minimize any undue influence.[33]

Over the past year, there have been a number of cases where the ITA laboratories failed to catch violations of the federal standards.[34] In the face of these failures at the federal level, State and local election officials have had to increase the scrutiny of their systems. Election officials are reluctant to rely on the vendor or ITA to effectively evaluate these systems. They have started to commission their own investigations of particular voting systems using their own independent experts.[35] These officials want to conduct evaluations that are either out

---

ing System Standards (2002 VSS). The EAC's 2005 Voluntary Voting System Guidelines (2005 VVSG) were approved by the EAC but did not go into effect until January 2008. See: *2005 Voluntary Voting System Guidelines*. U.S. Election Assistance Commission. Dec. 2005. URL: http://www.eac.gov/voting%20systems/voluntary-voting-guidelines/2005-vvsg. The EAC is currently reviewing recommendations on a new VVSG.

[30]Kim Zetter. "E-Voting Tests Get Failing Grade". In: *Wired News* (Dec. 2004). URL: http://www.wired.com/politics/security/news/2004/11/65535, (notes that ITAs cannot discuss specific systems due to NDAs with vendors).

[31]ITAA letter to Assemblymember Tom Umberg, "OPPOSE: AB 2097", March 22, 2006, on file with author. Similar sentiments were expressed in written testimony to a California State Senate Committee on Elections hearing in February of 2006; see: *Comments submitted on behalf of the Information Technology Association of America Election Technology Council to the members of the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments*. Election Technology Council. Feb. 2006. URL: http://web.archive.org/web/20070411003519/http://www.electiontech.org/downloads/ITAA+ETC+CA+OSS+TESTIMONY+-+FINAL.pdf

[32]Rebecca T. Mercuri and Peter G. Neumann. "Security by obscurity". In: *Communications of the ACM* 46 (2003). 160. URL: http://doi.acm.org/10.1145/948383.948413; One of the best discussions of the notion of "security through obscurity" is available on the Wikipedia page for the term. See: Security through obscurity: http://en.wikipedia.org/w/index.php?title=Security_through_obscurity&oldid=58172204 (last visited June 14, 2006). Full disclosure: the author is one of the many editors of this Wikipedia page.

[33]Steven B. Lipner. "Security and source code access: issues and realities". In: *Proceedings of the IEEE Symposium on Security and Privacy* (2000). 124–125. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=848476

[34]Hall, *Background on Recent Diebold Election Systems, Inc. (DESI) Vulnerabilities*, see n. 22.

[35]McDaniel, Blaze, Vigna, et al., see n. 22; *California Secretary of State's Top-to-Bottom Review* see n. 22; David Wagner, David Jefferson, Matt Bishop, Chris Karlof, and Naveen Sastry. *Security Analysis of the Diebold AccuBasic Interpreter*. Voting Systems Technology Assessment Advisory

of scope or performed poorly in the ITA process. In many cases, especially with additional security testing, access to the source code for voting systems is essential to perform effective evaluation.

2.5 Regulation and Legislation Relevant to Source Availability

2.5.1 State-level Disclosed Source Regulation and Legislation

To increase the level of access that they have to voting system source code for evaluation purposes, election officials and state legislatures have started to require that voting system source be disclosed in some form.[36]

In California, the office of the Secretary of State has taken a series of steps to increase the transparency and robustness of voting systems used in the State. The Secretary of State keeps a copy of the source code and binary executables for voting systems and retains the right to perform a full independent source code review.[37] The Secretary exercised this right in Spring of 2006.[38]

In the California legislature, there has been one resolution passed and a bill introduced that concerns disclosed and open source software in voting systems. A legislative resolution, ACR 242, was passed in August of 2004 that tasked the California Secretary of State with producing a report on open source code in voting systems.[39] In 2006, California As-

Board. Feb. 2006. URL: http://www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf; Linda Lamone. *Letter to Diebold, Inc. CEO Swidarski Concerning Memory Card Issues*. Dec. 2005. URL: http://truevotemd.org/images/stories/ll-diebold.pdf, (discussing official's concern and reserving the right to hire an independent expert of their choice to review source code).

[36] There have also been movements to obviate some of the need for increased transparency, such as the move to require voter-verified paper records (VVPRs). At the time of writing, there are currently 31 states that have enacted legislation requiring Direct-Recording Electronic voting machines to produce a Voter Verified Paper Record to provide an independent check on the voting system's recording functions. See VerifiedVoting.org's Legislation Tracking page: http://verifiedvoting.org/article.php?list=type&type=13.

[37] Other provisions relevant to public scrutiny and expert evaluation include: Vendors must establish a California County User Group and hold one annual meeting where the system's users are invited to review the system and give feedback and volume reliability testing of 100 individual voting machines under election-day conditions. See: *10 Voting System Certification Requirements*. California Secretary of State. Dec. 2005. URL: http://www.sos.ca.gov/elections/voting_systems/vs_factsheet.pdf

[38] Wagner, Jefferson, Bishop, Karlof, and Sastry, see n. 35

[39] "[T]he Legislature hereby requests the Secretary of State to investigate and evaluate the use of open-source software in all voting machines in California and report his or her findings and recommendations to the Legislature." See: *Assembly Concurrent Resolution No. 242—Relative to ballot tally software.* California State Assembly. June 2004. URL: http://www.leginfo.ca.gov/pub/03-04/bill/asm/ab_0201-0250/acr_242_bill_20040831_chaptered.html; *Open Source Software in Voting Systems*. California Secretary of State.

semblymember Goldberg introduced AB 2097 and Assemblymember Krekorian introduced AB 852 in 2007; both bills would have mandated public disclosure of voting system technology.[40] This bill would have forbade the Secretary of State from approving any voting system for use in California unless "all details of its operating system and specifications are publicly disclosed." It further prevents voting system vendors from exercising any rights against any voter who evaluates the voting system. The Election Technology Council of the Information Technology Association of America, came out against the bill, as introduced, for a variety of reasons from competitive concerns to intellectual property issues.[41]

In August of 2005, the North Carolina legislature passed SB223/H238 into law which stipulated that all source code used in voting systems certified in North Carolina would have to undergo a variety of evaluations. The provision stated that "all source code" would be made available for review, even that of third party vendors such as the operating system.[42] It is clear this statute would not be enforced.[43]

Wisconsin passed Assembly Bill 627 in 2005 which, in its original form, required municipalities to provide to any person "the coding for the software that the municipality uses to operate the system and to tally the votes cast."[44] The bill was subsequently amended to stipulate the escrow of voting system software "necessary to enable review and verification of the accuracy of the automatic tabulating equipment" but removing public access to code.[45]

2006. URL: http://www.sos.ca.gov/elections/open_source_report.pdf

[40] *AB 2097—An act to add Section 19213.5 to the Elections Code, relating to voting systems, and declaring the urgency thereof, to take effect immediately.* California State Assembly. 2006. URL: http://leginfo.ca.gov/pub/05-06/bill/asm/ab_2051-2100/ab_2097_bill_20060217_introduced.html; *AB 852—An act to add Section 19213.5 to the Elections Code, relating to voting systems.* California State Assembly. 2007. URL: http://leginfo.ca.gov/pub/07-08/bill/asm/ab_0851-0900/ab_852_bill_20070222_introduced.html.

[41] See n. 31, Comments submitted on behalf of the Information Technology Association of America Election Technology Council.

[42] See Sec. 163-165.7(c), available as passed by both houses of the NC Legislature here: http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/HTML/S223v7.html.

[43] Diebold Election Systems, Inc. was concerned that, among other things, it didn't have the rights to provide access to the source code of third-party software components of its system. It sued the North Carolina Board of Elections to prevent this regulation from taking effect. The case was dismissed as the Court found that there was no dispute as to the language or interpretation of the statute. See: *Diebold v. North Carolina Board of Elections.* unpublished (NC. Super. November 30, 2005). Nov. 2005. URL: http://www.eff.org/files/filenode/diebold_v_nc/diebold_order_dismissal.pdf

[44] *Assembly Bill 627, as introduced.* Wisconsin State Assembly. 2005. URL: http://www.legis.state.wi.us/2005/data/AB-627.pdf

[45] *Wisconsin Act 92.* 2005. URL: http://www.legis.state.wi.us/2005/data/acts/05Act92.pdf. The author knows of at least eight states with escrow requirements in regulation or statute (CA, CO, IL, MN, NC, UT, WI and WA). Unfortunately, it is unclear how many states actually escrow software; some states use

The intent of legislators and election officials involved in these efforts is to make information about the operation of voting systems publicly available because they think the public has a right to see it, or they see disclosure of source code as a necessary precursor to adequate testing to meet their election responsibilities; or both.

2.5.2 Federal Legislation

There have been a number of Federal bills relevant to source code access introduced. In 2006, there were three bills in Congress address the use of open source or disclosed source software:[46] H.R. 550 (known as "The First Holt Bill"), H.R. 939/S. 450 and H.R. 533 would each mandate the use of either open source or disclosed source software in election systems used for federal contests. These were narrow efforts to increase public scrutiny in that they only include source code for systems used in federal elections and it appears that there has been little appetite in Congress for electoral reform on top of HAVA.[47]

---

the National Institute of Standards and Technology's (NIST) National Software Reference Library (NSRL) as a form of "escrow". However, the NSRL stores *binary* versions of software products, not *source code*. See: http://www.nsrl.nist.gov/. The conditions for when escrowed software can be accessed and by whom vary but generally protect proprietary information from public disclosure. See discussion of contractual escrow terms in Chapter 3.

[46] There has been no federal electoral legislation since the passage of HAVA in 2002. At the original time of writing (in 2006), there were at least six bills—excluding companion bills—in the U.S. Congress that would have substantially reformed the conduct of elections on top of the reforms of HAVA. These six bills were: H.R. 550 (text is available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00550:), H.R. 704/S. 330 (text is available at: http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.704: and http://thomas.loc.gov/cgi-bin/query/z?c109:S.330: respectively), H.R. 939/S. 450 (text is available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00939: and http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.00450: respectively; note the two versions of these bills contain significant differences), H.R. 533/S. 17 (text is available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00533: and http://thomas.loc.gov/cgi-bin/query/z?c109:S.17: respectively; note the two versions of these bills contain significant differences), H.R. 278 (text is available at: http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.278:) and H.R. 3910 (text is available at: http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.3910:). VerifiedVoting.org maintains a comprehensive list of these bills and their differences here: http://www.verifiedvoting.org/article.php?list=type&type=13. Since publishing this chapter, Congressman Holt introduced a new version of his bill, H.R. 811, and Senators Feinstein and Bennett have introduced a bipartisan bill, S. 3212. Both bills depart from the more simple software disclosure language of previous bills in favor of highly restrictive and complicated language that would significantly limit the scope of such disclosure. See: 110th Congress. *H.R. 811—Voter Confidence and Increased Accessibility Act of 2007*. GovTrack.us (database of federal legislation). 2007. URL: http://www.govtrack.us/congress/bill.xpd?bill=h110-811; 110th Congress. *S. 3212—Bipartisan Electronic Voting Reform Act of 2008*. GovTrack.us (database of federal legislation). 2008. URL: http://www.govtrack.us/congress/bill.xpd?bill=s110-3212

[47] Congressman Bob Ney, former chair of the Committee on House Administration—which has federal election law jurisdiction—has expressed the sentiment that possible election reform should wait for past legislative action to run its course. See: *Speech by Rep. Bob Ney at Cleveland State University, Center for Election Integrity*. United States Congress Committe on House Administration. Nov. 2005. URL: http://web.archive.org/web/20070203050001/http://cha.house.gov/MediaPages/PRArticle.aspx?NewsID=1146. This sentiment appears to be the main cause behind why no legislation

Both H.R. 550 and H.R. 939/S. 450 would have mandated disclosed source for voting system software used in federal elections.[48] The emphasis in these bills was that the source code used to create software used in voting systems be made available to the public. It is unclear from the language of these bills what "disclosed source" would mean exactly; the term is not defined in either bill. H.R. 533 mandates open source, which includes public disclosure, and specifics that the EAC will set standards for such software.[49]

While these bills are motivated by similar concerns, the choice of disclosed or open code is significant. The disclosed source bills provide that software should be available for inspection. The later bill, which uses the term "open source software", leaves the specifics to the EAC to work out. The lack of definitions for these terms is unfortunate given the wide range of possible meanings and possible interpretations for such technical terms.[50] Specifically, disclosed source allows a very narrow subset of rights when compared with open source software licenses.[51]

2.5.3 California's "Open Source" Mandate

There is one interesting case where a regulator required voting system source code be open source. This appears to be the first case of an "open source" mandate by a State in the

gained much traction. While wise in some respects, this mindset neglects the fact that the time cycles involved in development of computerized voting equipment are much quicker than the timeframes included as deadlines in the statutes.

[48] The relevant language in both bills is: "No voting system shall at any time contain or use any undisclosed software." See: H.R. 550 Sec. 247(c)(1) and H.R. 939/S. 450 Sec. 101(c). The one-word difference is that H.R. 550 would have allowed the disclosure to any "person" while H.R. 939/S. 450 only allowed disclosure to "citizens".

[49] H.R. 533 Sec. 329(a) and Sec. 299G.

[50] For an appreciation of the variety in open source licensing regimes, browse the Open Source Initiative's (OSI) "Approved License" list (`http://www.opensource.org/licenses`) and the Free Software Foundation's web page "Various Licenses and Comments about Them" (`http://www.gnu.org/philosophy/license-list.html`). Open source licensing covers many licenses, some of which are incompatible with each other. Licenses span a spectrum of very simple—like the modified BSD license (`http://www.opensource.org/licenses/bsd-license.php`)—to the very intricate and complex—like the GNU General Public License (`http://www.gnu.org/copyleft/gpl.html`).

[51] Most open source licenses grant or withhold the exclusive rights, granted to creators under copyright law, of copying, modifying and distributing. For detailed inspection of the source code, inspectors would need at least the rights to copy and make modifications. That is, to properly test and debug a program, inspectors will need all source code necessary to build the binary application in a machine-readable format. They would then need to be able to transfer this code to their own build environment, verify that the source code behaves as it purports to, properly build the application and verify that the executable built behaves appropriately and matches the binaries on the target voting systems in the field. Transferring of code, compilation and modification necessary to test source routines implicates the right of reproduction and the right to prepare derivative works or modifications granted by copyright. The right to distribute the source code is not necessarily essential from this perspective as long as the inspecting parties get full access to the code.

U.S. In this case, the top election official in California determined that the only solution to a technical dilemma would be to require a critical piece of code be disclosed. Under recommendations from technical consultants, the Office of the Secretary of State in California issued regulations in November 2003 stating that all electronic voting system vendors would have to provide the functionality required to produce an Accessible Voter-Verified Paper Audit Trail (AVVPAT).[52] An order of March 2004 stated what requirements had to be met for a paper audit trail to qualify as an AVVPAT[53] where AVVPAT was defined as a contemporaneous paper record of a ballot that allowed disabled and non-English speaking voters to vote privately and independently. The biggest surprise in these regulations was the "open source mandate" it included. This part of the regulation provided:

> "All DREs must include electronic verification, as described in the Task Force's report, in order to assure that the information provided for verification to disabled voters through some form of non-visual method accurately reflects what is recorded by the machine and what is printed on the VVPAT paper record. **Any electronic verification method must have open source code in order to be certified for use in a voting system in California.**[54] (bold emphasis added.)

The regulation required an electronic verification mechanism that allows disabled voters to assess through a non-visual interface whether what is printed on the AVVPAT record is consistent with their intended vote. This requires either interpreting the signals sent to the printer or reading directly from the AVVPAT, not from the computer's memory or the electronic record of the vote. The code that interprets the printing signals or reads the AVVPAT must be "open source" per this regulation so that, in the words of David Jefferson, one of the experts that provided input, they would not have "merely transferred the need to trust software from the proprietary vote capture software to proprietary vote verification

[52] *Position Paper and Directives of Secretary of State Kevin Shelley Regarding the Deployment of DRE Voting Systems in California.* California Secretary of State (Kevin Shelley). Nov. 2003. URL: `http://josephhall.org/ks_casos/ks_ts_response_policy_paper-nov_2003_directive.pdf`

[53] *Standards For Accessible Voter Verified Paper Audit Trail Systems In Direct Recording Electronic (DRE) Voting Systems.* California Secretary of State (Kevin Shelley). June 2004. URL: `http://josephhall.org/ks_casos/avvpat_standards_6_15_04.pdf`

[54] See n. 52, CA SoS Shelley Position Paper, at 5.

software."[55]

The regulation left several core terms undefined and the intent unclear. If we take David Jefferson's statement as reflective of the Secretary's goal, this regulation should have been clarified to support the evaluation of the verification software. The regulatory intent here was to ensure that the disabled voter or an organization representing the disabled voters could obtain and inspect the source code of the verification subsystem. They would want to exhaustively inspect the code to make sure that it was accurately verifying the vote from reading the printout or interpreting the signals sent to the printer to produce the printout. The Secretary's decision to require that the source code of this subsystem be open source was logical; however, a clear definition of "open source" is necessary for vendors to build such a system. For example, they will need strict control of what pieces of their intellectual property are included in this piece of software. The Secretary should have aligned the regulatory intent of the AVVPAT order with licensing requirements to establish some minimal licensing criteria for this "open source" software.[56] Then, with a minimal set of licensing requirements, a few representative open source licenses could be chosen and offered as valid licenses under which to develop verification code. This level of detail was not included.

In January of 2005 this requirement was implicitly revoked by new regulations that omitted it.[57] This could have been an interesting experiment in regulatory push of open source; however it seems instead that it was destined to fail without sufficient attention to the issues raised above.

2.6 Benefits and Risks of Source Availability

Open and disclosed source software present options for improving the performance and public scrutiny of computerized voting systems as they become even more complex. In this section we try to ascertain potential benefits and risks involved in these two models and use

[55] David Jefferson. *Re: Open Source for "electronic verification method[s]"*. post to the Voting-Project mailing list. Feb. 2004. URL: `http://gnosis.python-hosting.com/voting-project/February.2004/0031.html`

[56] Minimal licensing criteria would be statements such as "The software source code is distributable to any member of the public."

[57] *Proposed Changes to Accessible Voter Verified Paper Audit Trail (AVVPAT) Standards*. California Secretary of State (Kevin Shelley). 2005. URL: `http://www.sos.ca.gov/elections/voting_systems/012005_1b_s.pdf`; *State of California Standards for Accessible Voter Verified Paper Audit Trail Systems in Direct Recording Electronic (DRE) Voting Systems*. California Secretary of State (Kevin Shelley). 2005

this information to evaluate various policy options. Here, we highlight the risks and benefits of both open source and disclosed source software as used in voting systems, by regulatory or legislative mandate or by vendor choice.

If a vendor chooses to use open source software as the basis for the functioning of their system, the most obvious benefit would be the direct access available to source code; anyone who accepts the terms of the open source license will, at least, have the freedom to examine the code. Many more individuals will be able to examine the code using manual or automated analysis. This is one piece necessary to catalyze comprehensive source code review, a key component of the increased security and reliability of source-available software systems.[58]

Disclosed code provides for enhanced access, but does not necessarily support the robust testing that open source code promotes, due to possible restraints on the making of derivative works—such as compiled or modified code—and other manipulations key to certain forms of testing. Disclosed source code regimes provide vendors more flexibility to protect the intellectual property interests than standard open source licenses, which require at a minimum the abilities to copy, modify, prepare derivative works and distribute source code.

Open source software has interesting implications for competition in the market, as the role of copyright and trade secrecy in limiting competition is removed. Therefore a vendor's competitors would be free to modify their code and compete against them with it. Naturally, intellectual property claims will, in general, cease to be a hurdle in commenting on, evaluating, using and procuring these open source voting systems. This is significant given recent efforts by vendors to use IP claims to frustrate oversight and testing of voting systems.[59] Few, if any, of these cases would have been an issue with an open source voting

[58]See Lipner, see n. 33; "Fuzz testing"—where software products are bombarded with random input to test reliability—has shown that source-available software utilizing open source development techniques is considerably more reliable than closed, proprietary products. See: Barton P. Miller, David Koski, Cjin Pheow Lee, et al. *Fuzz Revisited: A Re-examination of the Reliability of UNIX Utilities and Services*. University of Wisconsin-Madison, Computer Sciences Dept, 1995. URL: `http://reactos.ccp14.ac.uk/advocacy/fuzz-revisited.pdf`

[59]Here are a few examples: In the Fall of 2004, Diebold sent cease-and-desist letters to a number of students who had published an internal email archive that exposed the fact that Diebold had been using uncertified software on their machines. (*OPG, Pavlosky & Smith v. Diebold*. 337 F.Supp.2d 1195 (N.D. Cal. Sept. 30, 2004). URL: `http://www.eff.org/files/filenode/OPG_v_Diebold/OPG%20v.%20Diebold%20ruling.pdf`) Diebold has also sent letters and a "product use advisory" to Florida election officials warning them of intellectual property limitations on the testing of their voting systems in conjunction with other vendors systems. See see n. 26, at 21. In North Carolina, in response to the new legislation discussed in Sec. 4.3.2,

system as in each case the user of the system would be able to exercise their rights to copy, modify and distribute the software of the system. With disclosed source, we would not have the clear cut case where intellectual property claims become less of an issue, as such claims would now turn substantially on the substance of the disclosed source license the vendor chose to use; it is likely that a vendor would choose to restrict rights to improve its competitive position.

However, there are risks associated with fielding an open or disclosed source voting system. Since computer scientists have yet to find a method for writing bug-free software, public disclosure of the system source code will inevitably result in disclosing vulnerabilities. Voting systems are not the same as general-purpose computing technology. Voting technology is used highly infrequently, runs specialized software and is difficult to upgrade or change without extensive vendor involvement. In the case of voting systems, disclosing information on known vulnerabilities arguably helps would-be attackers more than system defenders.[60] Those tasked with defending voting systems—usually local election officials and their staff—are poorly positioned to shore-up these systems in the case of a serious source code-level vulnerability. Setting aside the fact that most jurisdictions don't have access to system source code, in most states any changes in the system's software will need to be recertified at the Federal and State level before being reinstalled on voting equipment.[61]

Open or disclosed source code voting systems will need to be accompanied by contingency planning in the face of system flaws. Simple flaws may be innocuous enough to allow for the usual running of the election. For serious flaws, such as if there were any suspicion that the flaw will affect the voter experience or the casting, storage and counting of vote data, there will need to be a mechanism to mitigate serious vulnerabilities close to an elec-

---

Diebold sued the State Board of Elections arguing that it could not provide source code to third-party software for the evaluation demanded by the new statute (see see n. 43).

[60] Swire develops a model of when disclosing security vulnerabilities will help or hinder system defenders: Peter Swire. "A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?". In: *Journal on Telecommunications and High Technology Law* 2 (2004). 163–. URL: `http://ssrn.com/abstract=531782`

[61] In the past, vendors have "updated" software on voting systems in the field without requesting recertification. After the California Attorney General settled a lawsuit against Diebold Election Systems, Inc. in the Winter of 2004, in part for fielding voting systems which were running uncertified software, this practice seems to have stopped. See: *Press Release: Attorney General Lockyer Announces $2.6 Million Settlement with Diebold in Electronic Voting Lawsuit*. California Attorney General (Bill Lockyer). Nov. 2004. URL: `http://ag.ca.gov/newsalerts/release.php?id=843`

tion. Among the options here would be a "postpone, then patch" strategy where the election in question would be postponed, a fix for the vulnerability developed, the system quickly recertified at the Federal and State level and then the new system used in the postponed election.[62] Another option, more simple than the last, would be for each jurisdiction to be prepared to run the entire election using paper ballots and hand counting. Naturally, jurisdictions using closed source products likely face these problems—known or unknown—now and will want to consider and plan for contingencies; open and disclosed source code raise the stakes of identified flaws.

2.6.1 The Case of Mandated Source Disclosure

There are risks and some benefits associated with government-mandated public disclosure using either a disclosed source regime or open source licenses. One such risk is that trade secrecy would be de facto eliminated from the highly competitive, small-margin voting systems market. A trade secret is defined as any secret information used in business that gives one a competitive advantage; trade secrecy protection only applies to information that is kept secret.[63] Vendors have asserted that their software contains trade secrets that would no longer be protectable if their software source were disclosed.[64]

The end of trade secrecy in software source code could mean the end for larger companies, which are more sensitive to the smallness of margins, as it will cause a slip of their market position and competitive edge against other larger vendors. If open source software is required, a body of open source software for election management and tabulation will be created that will lower the barriers to entry into the market and necessarily increase competition. The available software will be one piece that new firms will not need to develop in creating a viable voting system (see Sec. 2.8 for a discussion of other barriers to entry).

[62] There are unanswered questions about whether or not Presidential elections can be postponed without amending the Constitution. See: *Postponement and Rescheduling of Elections to Federal Office*. Congressional Research Service. Oct. 2004. URL: `http://www.fas.org/sgp/crs/RL32623.pdf`

[63] "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." Restatement of Torts Sec. 757, comment b (1939). Also, see the discussion of the Uniform Trade Secrets Act on page 51 of the next chapter.

[64] "Similarly, software source code, like many other written works (e.g., customer lists, secret formulas for products, strategic plans for future competition and an almost infinite variety of similar materials) can be protected against unauthorized disclosure under state trade secrets laws and with contractual non-disclosure agreements." See: see n. 31

Either of these possibilities will make it easier for small firms to enter the market, but also may make the market less appetizing for large vendors.

There could be narrower licensing options under a government mandate. That is, if a governmental entity deems it necessary to mandate disclosure, it would seem that they would also specify the terms of such disclosure. This would prohibit vendors from doing their own calculus of what to allow and disallow in the terms of their software license and would mean that they now had to fit their previous business models into the licensing arrangement mandated for the market in which they seek to operate. In addition, the issue of license compatibility would become problematic; only open source software licensed under comparable terms may be combined into a downstream product.

Finally, there is an evolving concept of eminent domain in the field of intellectual property, where the government must compensate an individual for taking intangible "property" subject to exclusive rights. The government "takings" here apply to situations where a vendor's intellectual property is disclosed or made available without their consent or approval. Should vendors be compensated for the release of intellectual property in the source code that runs their systems? The relevant forms of intellectual property implicated in the source code for voting systems are patents, copyright and trade secrets. Patents and copyrights are not much of an issue as both these forms of intellectual property will still be enforceable upon disclosure and there are statutory limits to damages.[65] Claims under the Freedom of Information Act (FOIA) or its state-level equivalents will usually protect proprietary and confidential information.[66]

That leaves the case of trade secrets released against the vendor's wishes. In *Ruckelshaus v. Monsanto Co.*,[67] the Supreme Court found that the disclosure of trade secrets claimed to

[65] For patents and copyright, 28 USC 1498 provides that a patent or copyright holder can sue the government for "recovery of his reasonable and entire compensation" but cannot enjoin the work being "used by or for" the government. Disclosure of patented, copyrighted software would not correspond to large financial exposure for voting systems vendors; depending on the terms of distribution (limited or public), the availability of the source code for voting system software would not undermine their ability to sell software products or enforce and license their patents.

[66] State equivalents to FOIA in the form of public records acts typically have broad exemptions for confidential information and trade secrets. Exemption 4 of FOIA allows the government to withhold trade secrets under certain circumstances involving FOIA requests. See: M. K. Erisman. "The never ending saga of unit prices: To disclose or not to disclose, that is the question". In: *Army Law* 2005 (2005). 138

[67] *Ruckelshaus, Administrator, United States Environmental Protection Agency v. Monsanto Co.* 467 U.S. 986 (1984).

be held in confidence by the Environmental Protection Agency (EPA) as part of a pesticide registration program was a 5th amendment "taking" of property.[68] The Court ruled that the "taking" existed when Monsanto had a "reasonable investment-backed expectation" of confidentiality and that this was formed when the EPA allowed vendors to mark certain information as trade secret through their registration program.[69] Further, without a reasonable investment-backed expectation, no taking existed. A key feature of the *Ruckelshaus* notion of "takings" is its retroactive nature; that is, the analysis turns on the expectation of confidentiality that the vendor had when submitting information to the government.

For voting systems, this means that any disclosure should be done carefully. That is, with rules or laws that mandate disclosure, any efforts to extend the effects of such policy to source code submissions made under a previous regime would likely run afoul of the *Ruckelshaus* notion of 5th Amendment "taking" of trade secrets. Voting systems vendors will likely not find it difficult to make a showing of "reasonable investment-backed expectation", as past indications show that vendors have been highly protective of their intellectual property.[70] From this analysis, the best course of action would be a non-retroactive policy in which the government clearly stated its intent to disclose system source code and also stipulated that any trade secrets would have to be removed by the vendor prior to submission after a certain date.

2.7 Open Source Voting Systems in the Voting Systems Market

If open source voting systems have real advantages compared to closed and disclosed source voting systems, then they should appear in the market much in the way that open source solutions have gained a substantial market presence in other areas of information technology. In this section, we review past and existing efforts to produce an open source voting system and then examine which types of existing open source business models might translate to the voting systems market.

[68] Id., at 1003-1004.
[69] Id., at 1010-1014.
[70] See discussion accompanying note 59.

2.7.1 Open Source E-Voting Projects

There have been a number of efforts to write open source voting code.[71] Most exist purely in software form, but three systems are used or aim to be used in actual elections: Australia's eVACS, The Open Voting Consortium (OVC) and Open Voting Solutions (OVS). These efforts are interesting as they are often driven by design criteria stemming from democratic ideals rather than values from the voting systems market itself.

Among international efforts,[72] The Australian Capital Territory Legislative Assembly commissioned an electronic voting system in 2000 to be used in the 2001 assembly election.[73] The winning bid, from an Australian firm called Software Improvements, was chosen on the grounds of superior project and quality management as well as increased transparency, as their solution would be freely licensed under the GNU GPL license. Software Improvements designed eVACS to be used on regular PCs that were used during the rest of the year for other purposes.

Aside from the fact that it was the first officially commissioned open source voting system, there are other interesting aspects of the eVACs system. First, while being a GPL'd product, it was not a product of an open source development model; software engineers employed by Software Improvements conducted all development in a highly controlled contribution environment. In fact, when a bug was discovered in the code by outside researchers and brought to the attention of the vendor firm, they developed their own internal fix in-

[71] The first quasi-open source software product to be used in U.S. elections was ChoicePlus by Voting Solutions. This software has been used to administer local-level ranked-ballot elections in Cambridge, MA since 1998 and Burlington, VT. It was planned to be released under the GNU GPL in November of 2003 but one small, proprietary piece of code has prohibited the full release of the software under the GNU GPL. Interview with Steve Willet of Voting Solutions, April 7, 2006, on file with author; Jay Lyman, Successful public election joins Diebold, free software, *NewsForge*, April 4, 2006, available at: `http://trends.newsforge.com/article.pl?sid=06/03/23/2040258&tid=136&tid=132`.

[72] The following nations have either posted or claim to have posted voting system software in publicly-accessible forums or to select organizations: Argentina, Venezuela, Estonia and Kazakhstan. See: "Publicación de Software y Documentación", available (in Spanish) here: `http://www.buenosaires.gov.ar/dgelec/index.php?module=pruebaPiloto&file=publicacion`, See: "Auditorías en Venezuela garantizan la integridad del voto", available (in Spanish) at: `http://www.smartmatic.com/noticias_077_2005-18.htm`, See (in Estonian): `http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf` and documentation/software at: `http://www.vvk.ee/elektr/dokumendid.htm`, Kazakhstan claims to allow review of the source code used to power their voting systems; it is hard to find. The Kazakh elections website (in Cyrillic): `http://election.kz/`.

[73] Clive Boughton and Carol Boughton, "Credible Election Software—eVACS™", white paper on file with author (2005).

stead of accepting the outside researchers' fix.[74] Second, the GPL was abandoned for the latest version of the system due to concerns of inadequate Australian legal footing[75] as well as a desire of the firm to protect their intellectual property.[76] However, ACT Electoral Commissioner Philip Greene has said that any future work will have to support the same level of access as what Software Improvements provided with eVACS.[77] Software Improvements is currently in the process of designing a licensing model that would simultaneously solve their concerns while allowing third-party examination and evaluation of the code.[78]

Two groups, The Open Voting Consortium (OVC) and Open Voting Solutions (OVS) have emerged in the U.S. that aim to design or build voting systems with software source code distributed under an open source license. OVS is very new and seems still in the coordination phase of their work but has as its mission to "develop open public specification based voting systems." The OVC, a loose-knit group of activists, information technology professionals and academics, produced a prototype system in 2003 that consisted of demonstration software that ran on commodity computers running the Linux operating system. The OVC's mission now appears to have shifted toward advocacy for the use of open source code in electronic voting systems and away from the production of an electronic voting system.[79]

Given the interest in electronic voting systems powered by open source software it is notable that no working models have fully matured in the current market. I discuss some of the potential reasons for this in Section 2.8 below. While the verdict is certainly not in on whether the market will independently yield open source powered voting systems, it might now be appropriate to think about other ways of incentivizing open source development so

[74] Email interview with Carol Boughton of Software Improvements Pty Ltd. (on file with author).

[75] For example, under Sec. 68(1) of Australia's Trade Practices Act of 1974, a disclaimer of warranty is void if it does not follow the particular conventions and wording of the Act. See: Fitzgerald, B., And Bassett, G. Legal issues relating to free and open source software. *Essays in Technology Policy and Law (Queensland University of Technology School of Law) 1* (2003).

[76] Software Improvements stated two concerns with releasing code that they've written under the GPL: first, that they would loose any trade secrecy embodied in the code and second, that another firm could use software that they've developed to compete against them.

[77] Email interview with Philip Greene of the ACT electoral commission. (on file with author).

[78] We should note that it appears to be more secure than other voting system software, see: Ananya Das, Yuan Niu, and Till Stegers. *Security Analysis of the eVACS Open-Source Voting System*. University of California at Davis, Department of Computer Science. Dec. 2005. URL: `http://midgard.cs.ucdavis.edu/~niu/projects/final-report.pdf` (pointing out that eVACS, in 2005, did not suffer from many of the problems plaguing other voting system software).

[79] The OVC has since demonstrated their voting system in an election at the LinuxWorld conference, see: DJWM. "LinuxWorld gets an open source voting tryout". In: *Heise Open Source UK* (Aug. 2008). URL: `http://www.heise-online.co.uk/open/LinuxWorld-gets-an-open-source-voting-tryout--/news/111243`.

that groups like the OVC can attract the resources needed to produce marketable products. We discuss some possible ideas for this in Section 2.9.

2.7.2 Open Source Business Models and the Voting Systems Market

The larger information technology and services sector has seen a substantial growth in business activity directly or indirectly tied to open source software. Is disclosed and open source software something that would naturally arise in the voting systems market? The voting technology market and regulatory environment are sufficiently distinct that a direct translation of current open source business models is questionable. Here, we cover what business models from other open source business endeavors might be applicable in the voting systems market. In Section 2.8, we highlight some barriers to entry and ongoing business that such an enterprise might face.

A few ways to make money off of open source software used in the IT sector might apply to the business environment surrounding voting systems. Firms such as 10X Software make money off of integrating IT systems into operating environments. A similar idea could be extended to voting, where a system integrator would incorporate open source voting system software and voting hardware to produce a voting solution for a state or local jurisdiction. Some firms, such as Wild Open Source, structure their business around targeted development of open source software. A software firm could be hired by a jurisdiction to add, fix or modify certain features of an open source voting system to their own specifications. This could ensure that specific functionality, such as supporting Instant Runoff Voting, was available in the technology that the customer was going to purchase. This also has the benefit that a feature could be added to the software before the open source voting system as a whole was certified and minimize the costs of having to re-certify a base system with the contracted modifications. Dual licensing is where a company offers the same software under two different software licenses, usually one being free software or open source and the other being a commercial license.[80] This can allow their product to benefit from some aspects of open source development while also allowing their customers, commercial

[80] Of course, under U.S. copyright law, a copyright holder can license their works under as many licenses as they like.

and non-commercial, flexibility in their licensing options. For example, MySQL AB offers its MySQL database software freely under the terms of the GNU GPL, but also allows companies to purchase commercial licenses that permit them to deviate from the terms of the GPL. In the voting systems context, a vendor could offer its software for free under a disclosed or open source license, but then charge commercial users to build variants. Companies could use the open source software simply to sell their hardware. That is, with open source software running their voting hardware, they can devote more resources to ensuring that their voting hardware is innovative and as cutting-edge and economical as their customers demand. For example, to concentrate their efforts at selling their high-quality hardware, Apple computer has embraced open source software as the core of their Mac OS X operating system.[81]

Some ways that companies use to make money off of open source do not translate well to the voting systems market. For example, Google's business strategy involves running optimized web search services on server clusters running the Linux operating system. Given the concerns and problems with networking in election systems, it would be difficult for a company to make money off of running open source voting software remotely. IBM sells proprietary software that works on top of or in concert with open source software. A company that tried to do this in the voting market would have to marshal each version of its software package through certification, and then it would only be partially open as a whole.

2.8 Barriers to Open Source Voting Systems

In addition to the restricted environment for open source business models discussed in the last section, there are also significant regulatory, economic, organizational and perceptional barriers to the use and development of open source software in the voting systems market. In terms of voting system regulation, any changes in system source code trigger system recertification at all levels. Unlike traditional open source software where the ability to change the software frequently is important, open source voting system software devel-

[81] However, as this article went to press, there were indications that Apple closed pieces of its software in a strategy to prevent people from running their software on non-Apple hardware. See: Tom Yager, Apple closes down OS X, *InfoWorld*, May 17, 2006, available at: `http://www.infoworld.com/article/06/05/17/78300_21OPcurve_1.html`.

opment would have to operate differently and take into account that once a product is out on the market, it will be very difficult to change or "patch" the software. In addition, federal and most state certification processes are evaluations of an end-to-end system; it will be insufficient to simply develop the software, as any successful certification will have to include hardware, documentation, and procedures in addition to the software.

Even with sufficient attention to planning and development, it will still be difficult for small firms or non-profits to get a foothold in the elections systems market. It takes quite a bit of infrastructure and financial backing to be able to develop, certify, market, implement and service voting systems. Federal certification alone can take from two months to a year and cost between $150,000 and $400,000 for a single voting system.[82] Contractual performance bonds—where a vendor puts a certain percentage of the cost of a contract in escrow until the system has performed according to a set of criteria in the contract—can be hundreds of thousands to millions of dollars. Due to the nature of state and federal voting systems standards and guidelines, voting systems must be certified as end-to-end voting systems—including precinct-tabulation, data storage and central tabulation—or a vendor of a subsystem has to team up with a larger firm that has the missing pieces and is willing to sponsor a full system certification.[83]

Of course, other pieces of a voting system business outside of code development need to be in place to field a product. To support the requirements of certifying and marketing an end-to-end system, an open source voting systems vendor will need to have a support organization the likes of which no other open source software applications have had to develop. Some open source businesses such as MySQL AB and SugarCRM do have extensive marketing and support infrastructures for their paying customers, but no open source business produces a product like an end-to-end voting system with on-site support where software, hardware, documentation and procedures are developed, evaluated, marketed, sold and maintained throughout the lifetime of the product.

[82] Carolyn Coggins. "Independent Testing of Voting Systems". In: *Communications of the ACM* 47 (2004). 34–38. URL: http://doi.acm.org/10.1145/1022594.1022619. There are indications that these expenses are increasing under the new EAC federal certification program: David Beirne. *Broken: The Regulatory Process for the Voting Industry*. Election Technology Council. June 2008. URL: http://www.electiontech.org/documents/ETC-BROKEN.pdf.

[83] Vogue Election Products & Services, LLC. did just this recently when it teamed up with Election Systems and Software (ES&S) to certify and market the AutoMARK ballot marking device.

Finally, in addition to these regulatory, economic and organizational barriers, there are a number of perceptional barriers related to voting system customers that an open source voting system vendor would have to overcome. First, voting system customers—typically local election officials—might not understand the debate around disclosure and system security. The intuitive view is that disclosing system source code will result in a less-secure system. Vendors will have to take care to explain the arguments against "security through obscurity" and how openly published algorithms, for example in cryptography, have proven more robust to attack. Also, to make a sale, open source vendors will need to be able to demonstrate that the organizational structure they choose will be able to support the system over its lifetime or provide alternatives to such support if the vendor goes out of business.

2.9 Alternatives to Blanket Disclosure that Increase Transparency

Given what we have described as the "enclosure of transparency", that source code access is a key aspect of voting system evaluation and that there are clear risks to public source code disclosure, we now turn to examining alternatives to blanket disclosure of source code. Such alternatives include limited disclosure, increased public access at the Federal level, incentivized or coordinated disclosure and technological mechanisms that support or obviate access.

2.9.1 Limited Disclosure

It is clear that source code access is key part of effective evaluation. As in the California case mentioned before,[84] where a critical interface between the paper record and a non-sighted voter was mandated to be open, there are critical pieces of a computerized voting system where public oversight and comprehensibility of the technology is of great importance. The interfaces between ballot presentation and the storage of vote data as well as the myriad of input and output methods are such critical points where maintaining secrecy results in pushing trust from one part of a voting system to another. In the end, openness is a natural and highly efficient way to break this cycle of pushing trust from one system

[84] See, *supra*, Sec. 2.5.3.

to another. Other areas of critical importance include vote storage, reading and writing. Limited disclosure of this code could achieve many of the benefits of source disclosure while minimizing risks.

Limited disclosure can be achieved by restricting the scope of code disclosed and the audience to which it is disclosed. That is, what in the code should be disclosed, critical systems (as argued for above) or all the code? Disclosing all the code has the benefit of ensuring that there is no place for malicious or erroneous code to hide. Allowing the public to view all the source code would have the benefits and risks discussed in Sec. 2.6. Along these lines, the CalTech/MIT Voting Technology Project, in a 2001 report, proposed a policy-based solution that required certain critical portions of the code be disclosed:

> "...the source code for all *vote recording and vote counting processes* must be open source. The source code for the user interface can and should be proprietary, so that vendors can develop their products" (emphasis added).[85]

This version of limited disclosure would specifically disclose software source code of voting system functionality that is critical while allowing vendors to compete in other, less critical, areas.

Once the decision as to what code is disclosed has been made, we need to decide who gets to see it. As in the federal open source and disclosed source bills discussed previously, do we allow all the public to acquire the voting systems code that will run our election or do we limit the pool to a select few or a subset of the public? On the contrary, if source code dissemination was controlled by application and contract,[86] the goal of having third-party code review could be achieved without the exposure and intellectual property concerns associated with public dissemination. However, a critical piece of restricted dissemination would be a requirement that all output from such reviews would be publicly available and unredacted to balance the exclusivity of code availability.

[85] *Voting—What Is, What Could Be.* CalTech/MIT Voting Technology Project. 2001. URL: `http://www.votingtechnologyproject.org/media/documents/july01/July01_VTP_Voting_Report_Entire.pdf`

[86] For example, an individual or organization could have to submit an application attesting to certain competences and sign a legally binding agreement that forbid certain activities. Such pre-requisite competencies could be to have a PhD-level degree in an area such as computer science and experience in system evaluation. Examples of activities to forbid would be to distribute the code further, to compile code flaws that aren't made available to the regulatory agency, to publish non-public reports and to transmit source-level information to a vendor's competitors.

2.9.2 Other Alternatives

A natural approach to increasing voting system transparency would be first to tackle the most obscure aspect of the current system. The Federal testing process (discussed in Sec. 2.4) has been the most mysterious and critically obscure step in ensuring voting systems perform according to federal standards. We can infer from increased state-level certification requirements and the fact that numerous vulnerabilities have slipped through federal certification over recent years that the federal evaluation process and the voting system standards do not ensure that a voting system can be used in elections free from serious flaws. A first step in increasing the quality of the federal certification process would be to make the testing plans and full evaluation reports public, perhaps in redacted form.[87]

Incentivized disclosure is another option. State governments or a consortium of state governments could decide to hold a contest or post a prize for the first development team to produce a voting system, like the ACT's eVACS, that would be released under a specified open source license. Another interesting model is that of "community source" where a consortium of government entities would agree to donate annual dues and full-time coders to a foundation that would develop, certify, market and support the consortium's voting systems.[88] This would also have the beneficial effect of bringing more detailed technical expertise inside the bounds of election officials' offices.

Finally, there are technological mechanisms for increasing transparency of voting systems. For example, the move in many states to mandate that DRE voting systems produce a VVPAT is essentially public verification of a record independent of the larger system. This allows the customer to treat the larger voting system as a black box as there will always be a verified indelible record of each vote as cast. In this vein, there is a body of work being developed by researchers that narrows the scope and minimizes the amount of what has to

[87] The EAC has moved to do exactly this with their new oversight of the federal certification process. See: *Voting System Testing and Certification Manual*. U.S. Election Assistance Commission. Dec. 2007. URL: http://www.eac.gov/program-areas/voting-systems/docs/certification-docs-certification-program-manual-omb-3265-0004-exp-6-30-2010.pdf/attachment_download/file.

[88] The SAKAI project uses this "community source" model, where a consortium of higher educational institutions have started to develop their own course management software instead of paying vendors . See: http://sakaiproject.org/.

be evaluated. Examples of this work include software independence,[89] isolated vote storage systems[90], voting systems with dramatically less trusted code[91], and hardware isolation techniques for security verification[92].

2.10 Conclusion

There has been an enclosure of transparency surrounding voting technology in the United States with recent efforts to halt the enclosure by increasing access to source code. It is clear that some source code access is needed to support transparency of voting systems. There are risks associated with public disclosure of source code and more substantial risks associated with mandated disclosure. The regulatory, financial, organizational and perceptional barriers to the entry of open source voting system software combine such that the open source business models that are now thriving in other sectors don't easily translate to the voting systems market.

We conclude that disclosure of full system source code to qualified individuals will promote technical improvements in voting systems, while limiting some of the potential risks associated with full public disclosure. Considering the alternatives to blanket disclosure mentioned in Sec. 2.9.2, such as increased access to the Federal process, incentives, collaborative models and technological solutions, we still have not explored all our options. We acknowledge that limited source code disclosure to experts does not support general public scrutiny of source code, and therefore does not fully promote the transparency goals of public oversight, comprehension, accuracy and accountability. However, in a public source code disclosure or open source code model most members of the public will be unable to engage in independent analysis of the source code and will need to rely on independent, hopefully

[89] Ronald L. Rivest and John Wack. *On the Notion of "Software Independence" in Voting Systems*. July 2006. URL: http://vote.nist.gov/SI-in-voting.pdf.

[90] David Molnar, Tadayoshi Kohno, Naveen Sastry, and David Wagner. "Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract)". In: *Proceedings of the IEEE Symposium on Security and Privacy* (May 2006). URL: http://http.cs.berkeley.edu/~daw/papers/vds-oak06.pdf

[91] Ka-Ping Yee, David Wagner, Marti Hearst, and Steven M. Bellovin. "Prerendered user interfaces for higher-assurance electronic voting". In: *USENIX/ACCURATE Electronic Voting Technology Workshop* (2006). URL: http://www.usenix.org/events/evt06/tech/full_papers/yee/yee.pdf.

[92] Naveen Sastry, Tadayoshi Kohno, and David Wagner. "Designing voting machines for verification". In: *USENIX Security Symposium* (2006). URL: http://www.usenix.org/events/sec06/tech/full_papers/sastry/sastry.pdf

trusted and trustworthy, experts. Given the potential risks posed by broad public disclosure of election system source code, we conclude that moving incrementally in this area is both a more realistic goal and the prudent course given that it will yield many benefits, greatly minimizes potential risks and provides an opportunity to fully evaluate the benefits and risks in this setting

CHAPTER 3

CONTRACTUAL BARRIERS TO TRANSPARENCY IN ELECTRONIC VOTING

In this Chapter, we explain a project completed in 2007 where we analyzed a data set of 55 contracts between state and local election jurisdictions and voting system vendors for transparency-inhibiting terms and provisions. We discuss the advantages and disadvantages of certain provisions and make recommendations that jurisdictions can follow to better support transparency in the elections process.[1]

3.1 Introduction

Electronic voting has faced increasing scrutiny since the disputed presidential race in Florida 2000. There has been a considerable amount of attention, to varying degrees, on issues such as election security, auditing, usability and accessibility. One area virtually devoid of attention to date is that of market and economic issues in voting systems. Information about market relationships between voting system vendors and their customers remains relatively unexamined.

The formal and informal relationships between election administrations and voting system vendors play a large role in shaping elections. The core of such formal relationships is voting systems contracts in which both vendors and election officials negotiate and agree to the terms of an initial purchase agreement and subsequent licensing, support, maintenance, training, etc. These contracts govern many of the activities in an election cycle dealing with

[1] The material in this chapter is based on work originally published in 2007. See: Joseph Lorenzo Hall. "Contractual Barriers to Transparency in Electronic Voting". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2007* (June 2007). URL: `http://www.josephhall.org/papers/jhall_evt07.pdf`.

voting technologies. For example, contract terms tightly control pre-election evaluation and certification, typically spelling out the environment and parameters around acceptance testing and logic and accuracy testing. In addition, these agreements and proprietary claims are often central to post-election disputes and audits.[2]

Voting systems contracts often restrict, in complex ways, activities and disclosure relating to voting technology. This can directly impact what a jurisdiction can and cannot do and what kinds of public communications it may make. Certain activities related to oversight, such as security testing, public disclosure, auditing and assembling mixed systems, can pose complex legal questions relating to contractual agreements and intellectual property.[3] Unfortunately, this can often affect the degree of transparency and the public's perception of transparency surrounding controversial voting technology.

In previous work, we outlined dimensions of transparency in terms of *access*, *oversight*, *accountability* and *comprehensibility*.[4] That work focused primarily on the access dimension of transparency by examining the role for disclosed and open source software in electronic voting systems. This work examines contractual relationships between voting system vendors and election jurisdictions to catalog terms and conditions that might limit oversight of voting technologies.

In section 3.2, we talk briefly about related work. Section 3.3 describes the data set and how we conducted the initial analysis. In section 3.4, we discuss the results of the analysis and in section 3.5 we offer recommendations for transparency-facilitating terms and provisions. Finally, we offer our thoughts on how to extend this work in section 3.6.

---

[2]For example, in Alaska the State Democratic Party sued to get access to raw vote data that was claimed as proprietary by both the State and Vendor. Alaska subsequently agreed to release the data. Lisa Demer. "State Rebuffs Raw Vote Demand". In: *Anchorage Daily News* (Jan. 2006); *Alaska: Public Records From 2004 Election Will Be Released (Press Release)*. Alaska Democratic Party. Sept. 2006. URL: `http://votetrustusa.org/index2.php?option=com_content&do_pdf=1&id=1801`. Also see: *Collaborative Public Audit of the November 2006 General Election*. The Cuyahoga County Collaborative Audit Committee and Cleveland State University Center for Election Integrity. Apr. 2007. URL: `http://urban.csuohio.edu/cei/public_monitor/cuyahoga_2006_audit_rpt.pdf`, at 5.

[3]Aaron Burstein, Stephen Dang, Galen Hancock, and Jack Lerner. *Legal Issues Facing Election Officials in an Electronic-Voting World*. Samuelson Law, Technology and Public Policy Clinic at the UC Berkeley School of Law (Boalt Hall). Mar. 2007. URL: `http://www.law.berkeley.edu/clinics/samuelson/projects_papers/Legal_Issues_Elections_Officials_FINAL.pdf`.

[4]See: Joseph Lorenzo Hall. "Transparency and Access to Source Code in Electronic Voting". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2006* (June 2006). URL: `https://www.usenix.org/events/evt06/tech/full_papers/hall/hall.pdf`. Note that I do not delve deeply or specifically into comprehensibility as it is a entirely subjective notion of transparency.

3.2 Related Work

There are other U.S. governmental contexts in which both protection of intellectual property—usually in the form of trade secrets—and transparency directly conflict.[5] However, typically one or the other prevails. Levine has highlighted, in addition to the environment surrounding computerized election systems, two other examples where trade secrecy has thwarted access, oversight and accountability: security vulnerability disclosure and municipal wireless procurement agreements.[6]

Using examples from the domain of electronic voting, Jones has demonstrated how blanket prohibitions on the disclosure of security-related information, either in law or vendor-jurisdiction agreements, directly inhibit public oversight.[7] The electronic voting context is one in which we expect the optimal solution to involve both protecting manufacturers' interests in trade secret protection as well as achieving a high level of public disclosure.

To date, there has been no in-depth substantive analysis of contractual agreements between voting system vendors and state and local election jurisdictions. There has been only one research project that we know of that made use of contracts as input into their analysis. In 2006, The Brennan Center for Justice at the New York University School of Law published an analysis that used cost and pricing data from a set of voting system contracts to model the upfront and ongoing costs of electronic voting systems.[8]

We hope that our analysis of contractual transparency barriers will further the use of voting systems contracts as data for future analyses. In this spirit, we are creating a "voting systems contract portal" hosted by the NSF ACCURATE center that will facilitate download-

[5] As discussed in the last chapter, trade secrets are unique in the realm of intellectual property; they are no longer protectable once publicly disclosed (See "trade secret" definition in note 32). Copyrights and patents still retain their protectability once disclosed. Thus, there is little or no conflict if a governmental entity has to disclose information covered by patent or copyright. (Software products in source or executable form are one exception to this in that they simultaneously tools and protectable works under trade secret, copyright and patent doctrines.)

[6] David S. Levine. "Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure". In: *Florida Law Review* 59 (2006). 135–. URL: http://ssrn.com/abstract=900929.

[7] Douglas W. Jones. *Computer Security Versus the Public's Right to Know: Notes for a panel discussion on Electronic Voting Integrity*. Computers, Freedom and Privacy 2007. May 2007. URL: http://www.cs.uiowa.edu/~jones/voting/cfp2007.pdf.

[8] See the chapter on Cost of: Lawrence Norden. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*. Brennan Center for Justice at NYU School of Law. Oct. 2006. URL: http://www.brennancenter.org/content/resource/the_machinery_of_democracy_voting_system_security_accessibility_usability_a

ing and submission of voting system contracts.[9]

3.3 Data and Methodology

3.3.1 Data Description

The data set for our analysis consists of 55 separate contracts between state and local election jurisdictions and voting system vendors.

We stress that this is not a representative sample from which one can draw generalizable quantitative conclusions.[10] We employed a convenience sample to acquire contracts from some of the major markets for electronic voting systems (i.e., California, Ohio, Florida) as well as a number of contracts from smaller jurisdictions. When setting about to do this work, we were interested in a qualitative sample that, as a threshold matter, helped us determine the nature of barriers to oversight in voting system contracts. We quickly determined in our research design that a sampling strategy that aimed to make generalizable conclusions from a representative sample was not within the scope of a first analysis.

With these comments about generalizability aside, some statistics of our sample include:

- The contracts cover jurisdictions from 18 states; with 14 (25%) from California and no more than 5 from any other individual state.[11]

- The contracts are between jurisdictions and 5 voting system vendors: Diebold Election Systems, Inc (DESI), Election Systems & Software, Inc. (ES&S), Hart InterCivic, Inc. (Hart), Microvote General Corp. (Microvote), and Sequoia Voting Systems, Inc. (Sequoia).[12]

- The three major vendors, DESI, ES&S and Sequoia, are parties to the lion's share of the contracts in our data set (45 (82%)); these vendors are parties to 16, 17, and 12

[9] The Voting Systems Contract Portal resides here: `http://www.accurate-voting.org/contracts/`.

[10] With our sample, we cannot report general statistical properties of the larger population of voting system contracts. For example, a representative sample would allow us to examine the prevalence of certain clauses and to control for certain properties of the jurisdiction.

[11] States include: AK, CA, FL, GA, IA, IL, IN, MA, MI, MS, MT, ND, NJ, OH, TX, UT, WA, WY.

[12] Note: Contracts between jurisdictions and Global Election Systems, Inc.—a predecessor of DESI—and LHS Associates, Inc.—a New England-based DESI reseller—are counted for DESI. DESI has since changed its name to Premier Election Solutions, Inc. (PESI).

contracts, respectively.

- These contracts cover a time period from March 2000 to July 2006. Over half (29) are from 2003 and 2004 with the remainder spread approximately equally over 2001-2002 and 2005-2006.[13]

- 9 contracts are missing exhibits and appendices or otherwise incomplete.

It was a challenge to assemble this data set. Voting system contracts aren't necessarily public documents and often pieces of contracts are considered proprietary and confidential. For example, in communication with the California Voting Modernization Board (VMB), which administers state and federal funds for improving elections, we requested certain missing pieces of some California contracts. The Board could not give us exhibits A-B of Solano County's old contract with DESI, explaining:

> "The VMB is in possession of Solano County's February 2003 Diebold contract exhibits A and B. However, these exhibits are identified as 'Confidential Trade Secret Information,' and are therefore privileged and not for public disclosure."[14]

Depending on a State's public records or open records laws, pieces of a contract that are considered proprietary and/or confidential may be exempt from disclosure.[15] However, even when sections of a contract are missing, we can use tables of contents (when present) to give us clues about the content being claimed as proprietary and/or confidential. Typically, withheld portions of contracts are pricing related information.[16]

[13] Only one contract is from 2000 (*Contract between Riverside County, California and Sequoia.* 2000. URL: `http://accurate-voting.org/contracts/CA/Riverside/CA_riverside_2000.pdf`). One of our original working hypotheses was that there would be a significant difference between contracts before and after the presidential election of November 2000. We anticipated that provisions protecting proprietary and confidential information as well as other competition-protective provisions would have substantially increased given the scrutiny that the 2000 election brought and the injection of money into the market that vendors undoubtedly expected (via HAVA). Unfortunately, we found it difficult to easily acquire contracts before November 2000. However, the one contract we did examine before this period, between Riverside County, CA and Sequoia Pacific Voting Equipment, Inc., is notable in that it displays some of the same transparency-prohibitive provisions seen in the remaining contracts, contrary to this hypothesis.

[14] Email from Jana Lean, Staff Consultant to the California Voting Modernization Board to the author, dated 31 January 2007, *on file with author.*

[15] There are a variety of ways that State entities handle public or open records requests. In some cases, as in the California example above, the State entity does not undertake any analysis or findings of fact to corroborate a vendor's claims. In other cases, a FOIA or public records officer is tasked with making a determination as to vendors claims and may or may not find that certain information is exempt from disclosure.

[16] But see discussion of pricing information protection in n. 33.

We obtained most of the contracts in our data set from the California Voter Foundation, the Brennan Center for Justice at New York University School of Law, the California Voting Modernization Board and the Black Box Voting Document Archive. Other contracts were obtained individually through email solicitations we sent to various election-related email listservs requesting procurement-related materials.

3.3.2 Methodology

After obtaining the contracts on paper, we scanned each contract into a PDF document at high-resolution (600dpi) and used Adobe Acrobat Pro's Optical Character Recognition (OCR) engine to translate the page images into text.[17] We read the PDF text of each contract to become qualitatively familiar with typical terms and conditions relevant to oversight transparency and developed a key of "terms of interest" for search-based extraction of blocks of text. The key was developed iteratively by marking up a few contracts from different vendors and locales and then finding common words of interest between them. The resulting key includes the following terms: "confidential", "confid", "proprietary", "propr", "escrow", "trade secret", "trade", "secret", "source code", "source", "code", "benchmark" and "bench".[18] Finally, we printed out the blocks of text extracted from each contract and sorted them by vendor and then by date. The final analysis involved looking at these documents in order and manually comparing how they evolved over time in the context of basic information about the procuring jurisdiction.

[17] Unfortunately, we received some contracts in a poor or difficult state. For example, the contracts we obtained from Black Box Voting were protected from copying and content extraction and contained a large, diagonal watermark that said, "from Black Box Voting Document Archive". When these contracts were rescanned and OCR'd, text could only be extracted when not near the watermark and often only on one side of the watermark. Where we use text from these documents in our analysis, missing portions of the text were transcribed from the document manually.

[18] Note that partial words were helpful in documents that had particularly low quality images or complications in page structure. Perhaps the worst case is the 2005 Mississippi contract with DESI which suffers from both low image quality *and* the watermark complications mentioned in note 17 (*Contract between the State of Mississippi and Diebold*. 2005. URL: `http://accurate-voting.org/contracts/MS/MS_diebold_2005.pdf`).

3.4 Analysis

In our analysis, we found evidence of contractual terms relevant to confidential information and trade secrets, prohibitions on use of voting systems, stipulations about public records acts, escrow release conditions, authorized testing and analysis of voting systems, voting system benchmarking and mandatory software upgrades.

3.4.1 Confidentiality and Trade Secret Protection

Voting system contracts restrict copying, duplication, decompilation, reverse engineering, and preparing derivative works as well as other actions like translation,[19] analysis,[20] and even extend to training materials and ballots.[21] Contracts consider it a breach of confidentiality if anyone else than the customer's "employees, agents or contractors" engage in these kinds of activities. And, complicating matters, confidentiality obligations can extend to information recorded in tangible forms (hardware, software, manuals, etc.) as well as oral communications and "know-how" obtained while interacting with the system.[22]

Certain types of information are explicitly excluded from being "confidential" in some contracts. Non-confidential information usually includes information in the public domain, information that the vendor discloses itself, information that becomes known without being misappropriated and information independently developed by the customer.[23]

While some of these provisions are typical of mass-market software licenses, other types of restrictions—such as limitations on the analysis of the voting system—are much more broad. Certainly, trade secrecy and other types of information protection are not usually troubling to a typical mass-market computer software customer. However, scholars have begun to question whether or not trade secrecy should be honored in applications involving governmental infrastructure such as electronic voting.[24]

[19] Riverside County 2000 contract, see n. 13, at 8.

[20] *Contract between Bergen County, New Jersey and Sequoia*. 2001. URL: `http://accurate-voting.org/contracts/NJ/Bergen/NJ_bergen_2001.pdf`, at 5.

[21] *Contract between Sarasota County, Florida and ES&S*. 2001. URL: `http://accurate-voting.org/contracts/FL/Sarasota/FL_sarasota_2001.pdf`, at 8–9.

[22] *Contract between Orange County, California and Hart*. 2003. URL: `http://accurate-voting.org/contracts/CA/Orange/CA_orange_2003.pdf`, at 34.

[23] Orange County 2003 contract, see n. 22, at 34.

[24] Levine, see n. 6.

Some contracts explicitly restrict output from voting systems. For example, ES&S has a standard term in the majority of its contracts that restricts copying or printing of output from any ES&S software:

> Customer shall not [...] Cause or permit any copying, reproduction or printing of any output generated by the ES&S Software in which ES&S owns or claims any proprietary intellectual property rights (e.g., copyright, trademark or patent), including, but not limited to, any ballot shells or code stock.[25]

This language was added to ES&S contracts in 2002 to cover "any output" and to specifically control "ballot shells or code stock", referring to blank ballots printed with timing marks for use with optical scanning systems.[26]

Meaningful oversight of electronic voting systems requires access to detailed data produced by the voting system. Outputs such as ballot images, raw vote data, audit and event logs, etc. are becoming increasingly important in litigating election disputes involving election technology as well as certification and evaluation of voting systems.[27] The bulk of contracts in our data set do have explicit carve outs for permitted activities that have become necessary as part of election administration. Most of these contracts permit election-related and internal uses of proprietary and confidential information, archiving and backup of software products, copying to enable "emergency restarting" and even replacement of worn copies of software.[28] While election administration offices may use this kind of detailed information internally, many of these offices do not have staff with the expertise needed to analyze these data to facilitate oversight. Thus, restrictions on disclosure of such output will complicate such activities if not stop them altogether.

In 2003, some ES&S contracts began to explicitly permit public demonstrations of voting machines and allow jurisdictions to print their own ballots[29] or procuring the printing of

[25] *Contract between Bloomington County, Illinois and ES&S*. 2003. URL: http://accurate-voting.org/contracts/IL/Bloomington/IL_bloomington_2003.pdf, at 3–4.

[26] *Contract between Chambers County, Texas and ES&S*. 2002. URL: http://accurate-voting.org/contracts/TX/Chambers/TX_chambers_2002.pdf, at 3.

[27] Kim Zetter. "2004 CA Election Results Nullified; Election Officials Sanctioned by Court". In: *Wired.com* (July 2007). URL: http://blog.wired.com/27bstroke6/2007/07/2004-election-r.html.

[28] *Contract between Palm Beach County, Florida and Sequoia*. 2001. URL: http://accurate-voting.org/contracts/FL/Palm_Beach/FL_palmbeach_2001.pdf, at 12.

[29] Bloomington County 2003 contract, see n. 25, at 3–4.

their ballots from a firm other than ES&S.[30]

In a particularly interesting display of controlling the flow of information, San Bernardino's 2003 contract with Sequoia has a blanket, bilateral prohibition on public communications without both parties' written approval:

> RELEASE OF INFORMATION. No news releases, advertisements, public announcements or photographs arising out of this agreement or SEQUOIA's relationship with COUNTY may be made or used without prior written approval of the COUNTY and SEQUOIA.[31]

This provision would be more troubling if unilateral on behalf of the vendor, but in this context it appears that both parties to the contract felt it was in their best interests to require such a cumbersome chokepoint on information dissemination.

In some cases, contracts purport to grant trade secret protection to information that is not typically considered protectable in this way.[32] For example, the unit prices that a vendor charges are typically claimed as proprietary in our data set. This is puzzling because, in most if not all cases, these numbers would be subject to budgetary disclosure provisions of the customer after the contract has been awarded.[33] For example, in DESI's 2001 contract with Alaska:

> It is expressly understood between the parties that [...] unit pricing constitute

[30] *Contract between Sacramento County, California and ES&S*. 2004. URL: `http://accurate-voting.org/contracts/CA/Sacramento/CA_sacramento_2004.pdf`, at 4, 8–9.

[31] *Contract between San Bernardino County, California and Sequoia*. 2003. URL: `http://accurate-voting.org/contracts/CA/San_Bernardino/CA_sanbernardino_2003-2.pdf`, at 16.

[32] Trade secret protection is governed by state law and may vary from state to state. However, the definition of what constitutes a trade secret has increasingly become more uniform. Forty-four of fifty states have adopted (some with slight differences) the Uniform Trade Secrets Act (UTSA), which defines "trade secret" as "[I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *See:* UTSA Sec. I(4), *available at:* `http://www.law.upenn.edu/bll/ulc/fnact99/1980s/utsa85.htm`.

[33] A notable Freedom of Information Act case, *McDonnell Douglas v. USAF*, concerned whether or not unit prices submitted in a bid were discloseable under the (federal) Freedom of Information Act. The D.C. Circuit allowed some of the pricing information to be disclosed—historical pricing information that couldn't harm McDonnell Douglas' future competitive position—but prohibited disclosure of other information—unit pricing information for future years in which the USAF was free to rebid the contract. *McDonnell Douglas Corp. v. United States Department of the Air Force*, 375 F.3d 1182 (D.C. Cir. 2004), *reh'g en banc denied*, No. 02-5342 (D.C. Cir. Dec. 16, 2004).

> proprietary information the nature of which is a trade secret, and that disclosure of this information may place [DESI] at a competitive disadvantage.[34]

While many contracts limit claims for damages, in some cases, these limitations don't apply in the event of a breach of confidentiality:

> Except for claims of personal injury and breaches of confidentiality obligations contained in this Agreement, CONTRACTOR and COUNTY liability for all damages shall not exceed the total value of this Agreement.[35]

From an oversight perspective, this kind of a provision serves as a chilling effect on the customer. The jurisdiction may overly-protect election information, even that which might not run afoul of confidentiality requirements, out of fear of unknown and potentially massive damages.

3.4.2 Prohibitions on Use

In many cases, the physical location of the hardware or software and the specific computers on which the software runs are contractually restricted. One motivation for these kinds of restrictions is to contractually control the security environment in which the hardware and software operate. However, another equally compelling rationale for these geographic and platform-related controls is to prevent secondary markets from emerging where jurisdictions might rent or lease equipment and thus effectively compete against the vendor.

For example, vendors restrict the hardware on which their software may run:

> Customer shall not, without DESI's prior written consent: [...] Use the DESI Application Software on any hardware other than the hardware identified in Exhibit A, Project Configuration Summary, the DESI Hardware on which it was pre-loaded by DESI, or other hardware for which DESI has granted its written approval.[36]

[34] *Contract between the State of Alaska and Global Election Systems, Inc. (DESI).* 2001. URL: http://accurate-voting.org/contracts/AK/AK_anchorage_2001.pdf, at 3.

[35] *Contract between Snohomish County, Washington and Sequoia.* 2002. URL: http://accurate-voting.org/contracts/WA/Snohomish/WA_snohomish_2002.pdf, at 13.

[36] *Contract between Solano County, California and DESI.* 2003. URL: http://accurate-voting.org/contracts/CA/Solano/CA_solano_2003.pdf, at 8.

In addition, DESI, Hart and Microvote have also restricted the physical locations or sites where their licensed software and/or hardware may be operated:

> "Customer shall not [...] Use the DESI Application Software outside of Customer's jurisdiction [...]."[37]

These types of restrictions can prohibit types of analyses that require the voting system to be examined in a specific environment such as a laboratory or problematic polling place. If the vendor objects and does not give its written authorization, provisions like these can effectively hold up location- or platform-specific activities.

As described above, third-parties are often excluded from being able to use or otherwise examine voting systems. Some jurisdictions have negotiated provisions that allow them to hire third-party programmers and operators to interact with their voting system, as long as those individuals are not employed by the vendor's competitors:

> Diebold will allow the licensee to contract with outside individuals or firms to program using the GEMS software. The outside individual contractors will exclude individuals currently employed by the other election system vendors.[38]

This type of provision balances the competitive concerns of the vendor and the desires of election administrators to hire the right expertise for a given job.

Contracts typically prohibit modification of their voting system hardware and software, without the written approval of the vendor, explicitly and through warranty limitations. However, in some cases any modifications have to be provided in source code form back to the vendor:

> In the event Customers obtains approval to modify and/or enhance the Software

[37] Solano County 2003 contract, see n. 36, at 7. Also: Bergen County 2001 contract, see n. 20, at 5; *Contract between Pulaski County, Indiana and Microvote*. 2003. URL: http://accurate-voting.org/contracts/IN/Pulaski/IN_pulaski_2003.pdf, at 5; *Contract between Miami County, Indiana and Microvote*. 2003. URL: http://accurate-voting.org/contracts/IN/Miami/IN_miami_2003.pdf, at 5; *Contract between Dubois County, Indiana and Microvote*. 2003. URL: http://accurate-voting.org/contracts/IN/Dubois/IN_dubois_2003.pdf, at 5; Orange County 2003 contract, see n. 22, at 26; *Contract between Yolo County, California and Hart*. 2006. URL: http://accurate-voting.org/contracts/CA/Yolo/CA_yolo_la_2006.pdf, at 8.

[38] *Contract between the State of Michigan and Diebold*. 2004. URL: http://accurate-voting.org/contracts/MI/MI_diebold_2004.pdf, at 202.

> Product, Customer shall provide [DESI] with the source code for the modifications and/or enhancements.[39]

This kind of provision may discourage third-party commercial auditing of voting systems where the auditing firm writes custom code, database reports or source-code level analysis tools to analyze the system's operation.[40]

Finally, some contracts feel the need to clarify that voters or "individuals participating in an election"[41] are allowed to use and operate the voting system, but only in a manner according to the voter instructions for a system:

> "Voters are also authorized to interact with the Sublicensed Software, in a manner consistent with voter instructions."[42]

It is notable that vendors and jurisdictions recognize that these agreements might be construed, without such provisions, to be so strict as to not allow voter interaction with the voting system. However, there is a wider sphere of uses that needs to be recognized going forward, such as security evaluation, post-election auditing and election litigation.

3.4.3 Accommodations for Public Records Laws

Most contracts include provisions that contemplate election officials' duties under Open Records or Public Records Laws. They also include a duty on behalf of the customer to notify the vendor of any such request within a certain amount of time. The period of time required between such notice and possible disclosure varies considerably from "immediate"[43] to "as soon as possible"[44] to "as soon as [a] public disclosure request is made"[45] to "promptly"[46] to "as much prior notice as reasonably practicable"[47] to no less than 10, 15 or 20 business

[39] Alaska 2001 DESI contract, see n. 34, at 22.
[40] Note: as mentioned in Section 3.4.5 local jurisdictions are not typically given access to source code.
[41] Solano County 2003 contract, see n. 36, at 7.
[42] Orange County 2003 contract, see n. 22, at 17.
[43] *Contract between the State of Utah and Diebold.* 2006. URL: http://accurate-voting.org/contracts/UT/UT_diebold_2006.pdf, at 24-25.
[44] Riverside County 2000 contract, see n. 13, at 8; Palm Beach County 2001 contract, see n. 28, at 12.
[45] Snohomish County 2002 contract, see n. 35, at 10–11.
[46] *Contract between the State of Georgia and Diebold.* 2002. URL: http://accurate-voting.org/contracts/GA/GA_diebold_2002.pdf, at 15.
[47] *Contract between the State of Ohio and Diebold.* 2004. URL: http://accurate-voting.org/contracts/OH/OH_diebold_2004.pdf, at 14; *Contract between Cuyahoga County, Ohio and Diebold.* 2005. URL: http://accurate-voting.org/contracts/OH/Cuyahoga/OH_cuyahoga_2005.pdf, at 7.

days.[48] It is unclear why there is so much variation in these time periods.[49] From an oversight perspective, it would be wise to tailor the time between notice and disclosure based on the information being requested and the time the request occurs in an elections cycle. For example, if it is a small, crucial request made before or immediately after an election, it should be disclosed as soon as possible and not subject to a delay in disclosure.

Contracts in our data set go so far as to declare the agreement itself as confidential. For example, the following provision appears in two ES&S contracts from different states:

> [Confidential] Information includes the terms of this Agreement.[50]

Considering how important contractual terms are in governing what a jurisdiction may or may not do with their voting system, other jurisdictions have explicitly negotiated language that allows full public disclosure of their agreement.[51] From the 2006 contract between Yolo County, California and Hart:

> Upon its execution, this Agreement (including all exhibits and attachments) shall be subject to disclosure pursuant to the California Public Records Act.[52]

Contracts in Florida explicitly limit the customer's liability due to open/public records disclosure:

> The Supervisor shall not be liable for any damages suffered by Sequoia as a result of any disclosure of Sequoia's materials pursuant to [the Florida Public Records Act,] Chapter 119[, Florida Statutes].[53]

[48] *Contract between Alameda County, California and Sequoia.* 2006. URL: http://accurate-voting.org/contracts/CA/Alameda/CA_alameda_2006.pdf, at 23; San Bernardino County 2003 contract, see n. 31, at 11; *Contract between Santa Clara County, California and Sequoia.* 2003. URL: http://accurate-voting.org/contracts/CA/Santa_Clara/CA_santaclara_2003.pdf, at 16.

[49] Note individual states' records laws may stipulate a period of notice and opportunity to respond to records requests.

[50] *Contract between Bexar County, Texas and ES&S.* 2002. URL: http://accurate-voting.org/contracts/TX/Bexar/TX_bexar_2002.pdf, at 19; *Contract between Will County, Illinois and ES&S.* 2003. URL: http://accurate-voting.org/contracts/IL/Will/IL_will_2003.pdf, at 9–10.

[51] "Contractor agrees that the contract will be a public document [...]" Utah 2006 DESI contract, see n. 43, at 8. "In the event that there are requests for copies of Agreements between the County and Contractor(s), the County is under obligation to comply with such requests for information [...]." Alameda County 2006 contract, see n. 48, at 23.

[52] Yolo County 2006 contract, see n. 37, at 25.

[53] Palm Beach County 2001 contract, see n. 28, at 12. Similar language exists in other Florida contracts. (Sarasota County 2001 contract, see n. 21, at 9; *Contract between Pasco County, Florida and ES&S.* 2001. URL: http://accurate-voting.org/contracts/FL/Pasco/FL_pasco_2001.pdf, at 9–10)

This type of provision is similar, but in the opposite sense, to the lack of a limit on damages for confidentiality breach discussed in Section 3.4.1. This will tend to facilitate oversight through public records requests by ensuring that the jurisdiction will be shielded from any harm related to disseminating information about their voting system.

3.4.4 Escrow Release Conditions

Many jurisdictions contractually or through regulations require vendors to deposit copies of source and object code with an escrow agent. The escrow agent is required to provide access to the escrowed code under certain conditions called "release conditions". Escrow agreements typically specify that source code shall be released to a jurisdiction if a vendor goes bankrupt, otherwise goes out of business or ceases to support or maintain a given product. In addition to these types of release conditions, the State of Ohio has negotiated a few more in its master contract:

> (iv) Vendor makes the source code generally available to other users of the Licensed Materials (in which case Vendor shall make it available to the Secretary under similar terms and conditions); (v) Vendor is unable to correct a logic error or other bug in the software and such failure to correct constitutes an uncured breach of its obligations under Schedule E [the Software License Agreement]; or (vi) For purposes of temporarily auditing and/or testing the software source code held in escrow in accordance with the Escrow Agreement.[54]

These additional provisions provide for access to source code if the vendor makes it available to other jurisdictions, if a vendor fails to correct "bugs" in the software or for temporary audit and testing purposes. If jurisdictions had the ability to patch bugs and fix vulnerabilities in the software that runs their voting systems, they could potentially have a powerful self-preservational recourse. There have been numerous cases of flaws in voting systems going "uncured" for many, many years; this type of provision would allow jurisdictions to claim access to voting system source code and contract for a solution.[55] Of course, this

[54] Ohio 2004 DESI contract, see n. 47, at 9–10.

[55] Douglas W. Jones. *Connecting Work on Threat Analysis to the Real World*. Threat Analyses for Voting System Categories; A Workshop on Rating Voting Methods (VSRW 2006). June 2006. URL: `http://www.cs.uiowa.edu/~jones/voting/VSRW06.pdf`.

would have to be done carefully but the idea is a promising one.[56]

3.4.5 Authorized Testing and Analysis

Voting system source code is not usually provided to local jurisdictions. In the language of a recent contract between DESI and Alameda County, California, "DESI does not provide its source code to Customers in the ordinary course of business."[57] and ES&S's standard contract includes specific language prohibiting use of source code:

> The licenses granted in Section 2.2 do not permit Customer to use the source code for the ES&S Software Products. [...] The source code will remain the property of ES&S and may not otherwise be used by Customer.[58]

However, in contracts negotiated at the state-level we see evidence that access to source code is increasingly included in contract negotiations. For example, from the 2006 contract between Utah and DESI:

> In addition, if requested, DESI will cooperate in order to enable a third party that is acceptable to the State to conduct an independent security review of its source code.[59]

And from the 2004 master contract between DESI and the state of Michigan:

> The Department of State or an authorized agent of the Department of State shall be able to obtain the software for purposes of analyzing and testing the software.[60]

Considering the increasing importance of source code analysis in conducting pre- and post-election oversight and auditing of voting systems,[61] having these provisions explicitly stip-

[56] Note that, in a majority of states, any voting system modifications have to be certified to national voting system guidelines. If the vendor refuses to submit changes that a jurisdiction has made under escrow release/seize circumstances, the scenario could become substantially more complex.

[57] Alameda County 2006 contract, see n. 48, at 11.

[58] Sarasota County 2001 contract, see n. 21, at 4.

[59] Utah 2006 DESI contract, see n. 43, at 11.

[60] Michigan 2004 DESI contract, see n. 38, at 34.

[61] Hall discusses the importance of source code availability in voting system evaluation, (Hall, "Transparency and Access...", see n. 4, at 3–4). There have been numerous studies over the past few years using source code review as a significant or central part of voting system vulnerability analysis. A few

ulated in the contract can ensure that such access is provided in a timely manner and in the form preferred by the jurisdiction.

In terms of access to source code for smaller jurisdictions we know of only one such agreement that provides for such access. Alameda County, California was recently able to negotiate a "failsafe operation" provision that provides for either a court or the California Secretary of State to call for a source code review if an unexplained discrepancy in vote data occurs during an election:

> If there is an unexplained issue with votes being lost/added/changed during any election during the contract term and the California Secretary of State makes a determination that such unexplained issue requires investigation or if such a determination is so ordered by a State of California court, the County will have the election source code reviewed for malicious code by an independent third party mutually agreed upon by both parties with a Sequoia confidentiality agreement. The review will be commissioned by the County and, if so ordered by a court or the California Secretary of State, the cost borne by Sequoia.[62]

This provision is notable in how much more narrow it is compared to the similar provisions in state-level contracts mentioned previously. In other smaller jurisdictions we see either complete absence of these kinds of provisions or explicit prohibition of access during an audit.[63] It is unfortunate that smaller jurisdictions don't seem able to negotiate access to source code as needed.[64]

---

recent studies include: David Wagner, David Jefferson, Matt Bishop, Chris Karlof, and Naveen Sastry. *Security Analysis of the Diebold AccuBasic Interpreter*. Voting Systems Technology Assessment Advisory Board. Feb. 2006. URL: http://www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf; Ryan Gardner, Alec Yasinsac, Matt Bishop, et al. *Software Review and Security Analysis of the Diebold Voting Machine Software*. July 2007. URL: http://election.dos.state.fl.us/pdf/SAITreport.pdf; *Top-To-Bottom Review of California's Voting Systems*. California Secretary of State. Aug. 2007. URL: http://www.sos.ca.gov/elections/elections_vsr.htm; Patrick McDaniel, Matt Blaze, Giovanni Vigna, et al. *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing (Academic Final Report)*. Dec. 2007. URL: http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf; *Software Reviews and Security Analyses of Florida Voting Systems*. Florida State University's Security and Assurance in Information Technology Laboratory. Feb. 2008. URL: http://www.sait.fsu.edu/research/evoting/index.shtml.

[62] Alameda County 2006 contract, see n. 48, at 28.

[63] "COUNTY's right to audit shall not extend to SEQUOIA's confidential and proprietary Information [...] or information pertaining to overhead, general administrative and/or profit percentages." (San Bernardino County 2003 contract, see n. 31, at 4–5)

[64] Smaller jurisdictions may not see a need for such access or may feel that requesting such access might cause them other contracting difficulties.

Finally, also in the recent Alameda contract, we see the first contractual agreement to cooperate with future disclosed and open source software legislation:

> In the event that "open source code" becomes a requirement of California law, Sequoia will work with the CA Secretary of State under the rules/regulations in effect at that time to comply with the law.[65]

This kind of forward-thinking provision is undoubtedly a good idea considering the interest of California and Federal officials and legislators in increasing disclosure of voting system source code.

3.4.6 Benchmarking

Some contracts explicitly prohibit publishing benchmark testing results of the voting software or sublicensed software products. For example, some ES&S contracts forbid publishing benchmarking tests of Oracle database software included in their product.[66] Hart contracts directly restrict publication of benchmark test results of any software that they provide:

> Client shall not publish any results of benchmark tests run on any Software.[67]

Unfortunately, the term "benchmark test" is not defined in these contracts and could be construed to cover any kind of stress- or performance-testing, comparative or not.[68]

3.4.7 Mandatory Software Upgrades

Earlier contracts in our data set contain mandatory software upgrade provisions. This is especially interesting given the scandal in 2003 surrounding uncertified software being installed in California.[69] For example, from the DESI contract with Alaska in 2001:

---

[65] Alameda County 2006 contract, see n. 48, at 42.

[66] "CUSTOMER is prohibited from publishing the results of benchmark test runs on the Oracle Software." Bexar County 2002 contract, see n. 50, at 7.

[67] Orange County 2003 contract, see n. 22, at 28.

[68] This would seem to include "volume testing" as conducted by the California Office of Secretary of State, where a large quantity of voting machines are voted on for many hours to simulate the loads and conditions of a real election.

[69] Kim Zetter. "Did E-Vote Firm Patch Election?". In: *Wired News* (Oct. 2003). URL: `http://www.wired.com/politics/law/news/2003/10/60563`.

> [DESI] may provide the Customer with unsolicited error corrections or changes to the Firmware which [DESI], at its sole direction, determines are necessary for the proper operation of its APPLICATION SOFTWARE and/or tabulating equipment, and the Customer shall incorporate these corrections or changes into the System within ten (10) days of receipt from [DESI].[70]

It is encouraging to see that these provisions ceased appearing in DESI contracts after 2003. Forced software upgrades, especially on a short time-scale and without any provisions for being close to an election, are extremely dangerous from a security perspective. From the perspective of oversight, forced upgrade provisions practically ensure that software a jurisdiction tested and evaluated months before would be suddenly essentially unknown to them.

3.5 Recommendations

Through the thicket of contractual issues in the last section, we distill a number of contracting principles that jurisdictions can use to better facilitate oversight.

1. **Contracts themselves should be fully disclosed.** Jurisdictions should negotiate for full disclosure of their agreements with vendors so that they can freely communicate with others about the terms of their relationships with voting system vendors. To the extent that such terms are confidential, jurisdictions might face inaccurate or conspiratorial charges from voters and advocates.

2. **Contracts should allow source code review in pre-election, post-election and litigation stages of the election cycle.** Source code review and analysis is increasingly becoming an important tool in oversight activities. Jurisdictions will need to explicitly reserve the ability to allow for source code review in all stages of the election cycle. Terms should also include that non-proprietary versions of final reports be published without restriction.

[70] Alaska 2001 contract, see n. 34, at 7. Similar provisions exist in: *Contract between Kern County, California and Diebold.* 2002. URL: `http://accurate-voting.org/contracts/CA/Kern/CA_kern_2002.pdf`, at 23 ("90 days" to install); Solano County 2003 contract, see n. 36, at 8 ("20 days" to install).

3. **Contracts should include options for other kinds of evaluation and auditing.** If the jurisdiction determines that it may be desirable or necessary to engage in other kinds of evaluations such as red team exercises, usability evaluation, accessibility testing and parallel testing, it should specify the terms relevant to the vendor for those activities in its contract. This may require, as discussed in Section 3.4.2, more relaxed provisions on who can operate the voting system, where they can operate it and for what purpose. Jurisdictions should be free to choose an independent auditor that can have in-depth access to their elections system and voting technology.[71]

4. **Contracts should contain explicit indications that all vote data including ballot definition material, raw data, ballot images, and audit logs are public records.** These categories of information are useful for oversight activities as well as forensic investigation of voting system anomalies. For example, the 2003 contract between Mendocino County, California and DESI includes such a provision, although it does not qualify that these data should be "public":

   > All data processed by the Election System and any derivative works of such data produced by the Election System are instruments of service which shall be deemed the property of the COUNTY.[72]

5. **Contracts should limit damages due to public and open records responses and breaches of confidentiality.** Jurisdictions must comply with public and open records requests in a timely manner. While they have a duty to protect confidentiality to the best of their ability, they should not be so preoccupied with potential damage claims so as to prohibit all but the most trivial types of disclosure.

[71] Restrictions such as these played a large role in recently preventing an audit team in Cuyahoga County from diagnosing a possible database corruption event. (Cuyahoga Collaborative Public Audit Report, *Cuyahoga Collaborative Public Audit Report*, see n. 2, at 35)

[72] *Contract between Mendocino County, California and Diebold*. 2003. URL: `http://accurate-voting.org/contracts/CA/Mendocino/CA_mendocino_2003.pdf`, at 6.

3.6 Future Work

There are a number of dimensions along which this work could be extended. In coming years, we aim to extend the immediate findings of this work to produce exemplar contract provisions and best practices in vendor contract language that jurisdictions and voting systems vendors can work with to promote transparency. In addition, while this analysis was focused on oversight-inhibiting terms and provisions, there are other data elements, such as pricing information, that could provide a basis for other types of inquiry.

Research that uses a stratified sampling strategy would allow more generalizable quantitative conclusions. Stratifying along either a per-state dimension or by grouping jurisdictions according to important properties, such as population, would make possible determinations about how prevalent certain provisions are and how jurisdictional properties effect the result of negotiations.

A promising line of analysis would be in the longitudinal dimension. We fully expect there to be a substantial difference in the nature of contractual provisions in agreements executed before and after 2000 due to the increased scrutiny and competitive pressure in the post-2000 environment. Research based on a substantial sample of contracts before November 2000 would test such longitudinal hypotheses.

CHAPTER 4

POST-ELECTION AUDITS: RESTORING TRUST AND TRANSPARENCY IN BLACK-BOX VOTING SYSTEMS

4.1 Introduction

In the last several years, most of the public debate on electronic voting has concerned whether voting machines should include a voter-verifiable paper record.[1] In much of the country, that debate is now over: thirty one states require voter-verifiable paper records.[2] Another eight states use voter-verifiable paper records in every county without requiring them, and of the remaining eleven states that do not use voter-verifiable paper records statewide, several are currently considering legislation that would mandate such records in the future.[3]

The widespread adoption of voter-verifiable paper records does not resolve the security, reliability, and verifiability issues with electronic voting that many groups have identified. To the contrary, as the Brennan Center for Justice at the New York University School of Law (the Brennan Center) noted in its June 2006 study of electronic voting system security *The Machinery of Democracy: Protecting Elections in an Electronic World*,[4] paper records, by

[1] This chapter is an updated version of a paper originally co-authored in 2007 with three other individuals. See: Lawrence Norden, Aaron Burstein, Joseph Lorenzo Hall, and Margaret Chen. *Post-Election Audits: Restoring Trust in Elections*. Brennan Center for Justice at The New York University School of Law and The Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley School of Law (Boalt Hall). 2007. URL: `http://www.brennancenter.org/dynamic/subpages/download_file_50227.pdf`

[2] Robert Kibrick. *Voter-Verified Paper Record Legislation*. VerifiedVoting.org. May 2008. URL: `http://www.verifiedvoting.org/article.php?list=type&type=13`.

[3] These states include Florida, Georgia, Iowa, Maryland, Missouri, Pennsylvania, Texas, and Virginia.

[4] Lawrence Norden and Eric Lazarus. *The Machinery of Democracy: Protecting Elections in an Electronic*

themselves, are "of questionable security value." Paper records will not prevent programming error, software bugs or the introduction of malicious software into voting systems. If paper is to have any real security value, it must be used to check, or "audit," the voting system's electronic records.

Unfortunately, the value of voter-verifiable paper records has received little attention and study until recently. In the last few years, statisticians and election integrity experts have authored and released dozens of separate papers about post-election audits of voter-verifiable paper records.[5] Meanwhile, the prospect of a federal requirement for post-election

---

World: Brennan Center Task Force on Voting System Security. Brennan Center for Justice at NYU School of Law. 2006. URL: http://www.brennancenter.org/dynamic/subpages/download_file_39288.pdf, at 121.

[5] See: Andrew W. Appel. *Effective Audit Policy for Voter-Verified Paper Ballots*. Center for Information Technology Policy / Department of Computer Science, Princeton University. Sept. 2007. URL: http://www.cs.princeton.edu/~appel/papers/appel-audits.pdf; Arel Cordero, David Wagner, and David Dill. "The Role of Dice in Election Audits—Extended Abstract". In: *IAVoSS Workshop on Trustworthy Elections 2006 (WOTE 2006)* (June 2006). URL: http://www.cs.berkeley.edu/~daw/papers/dice-wote06.pdf; Kathy Dopp and Ron Baiman. *How Can Independent Paper Audits Detect and Correct Vote Miscounts?* 2005. URL: http://electionarchive.org/ucvAnalysis/US/paper-audits/Paper_Audits.pdf; Kathy Dopp and Frank Stenger. *The Election Integrity Audit*. National Election Data Archive. 2006. URL: http://electionarchive.org/ucvAnalysis/US/paper-audits/ElectionIntegrityAudit.pdf (a computer program developed by Frank Stenger and Kathy Dopp for calculating audit details is available at http://electionarchive.org/auditcalculator/eic.cgi); Jerry Lobdill. *Considering Vote Count Distribution in Designing Election Audits*. Nov. 2006. URL: http://vote.nist.gov/Considering-Vote-Count-Distribution-in-Designing-Election-Audits-Rev-2-11-26-06.pdf; Jerry Lobdill. *Election Audit Sampling Plan—It's Not Just About Sampling Without Replacement*. Oct. 2006. URL: http://tinyurl.com/3e389n; Norden and Lazarus, see n. 4; Ron Rivest. *On Auditing Elections When Precincts Have Different Sizes*. 2007. URL: http://theory.lcs.mit.edu/~rivest/Rivest-OnAuditingElectionsWhenPrecinctsHaveDifferentSizes.pdf; Ron Rivest. *On Estimating the Size of a Statistical Audit*. Available at: http://theory.csail.mit.edu/~rivest/Rivest-OnEstimatingTheSizeOfAStatisticalAudit.pdf. 2006 (Howard Stanislevic has developed a computer program for calculating Rivest's equation at: http://mysite.verizon.net/evoter/AuditCalc.htm); Jonathan D. Simon and Bruce O'Dell. *An End to "Faith-Based" Voting: Universal Precinct-Based Handcount Sampling to Check Computerized Vote Counts in Federal and Statewide Elections*. Election Defense Alliance. Sept. 2006. URL: http://electiondefensealliance.org/files/UPSEndFaithBasedVoting.pdf; Howard Stanislevic. *Random Auditing of E-Voting Systems: How Much Is Enough?* 2006. URL: http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf; Ellen Theisen. *Auditing Election Equipment—The Real Scoop!* Aug. 2005. URL: http://www.votersunite.org/info/auditingissues.pdf; *The Titanium Standard for Election Verification and Security*. Oct. 2006. URL: http://www.velvetrevolution.us/titanium.pdf; Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. "Machine-Assisted Election Auditing". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2007* (Aug. 2007). URL: http://www.usenix.org/events/evt07/tech/full_papers/calandrino/calandrino.pdf; Stephen N. Goggin and Michael D. Byrne. "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2007* (Aug. 2007). URL: http://www.usenix.org/events/evt07/tech/full_papers/goggin/goggin.pdf; John McCarthy, Howard Stanislevic, Mark Lindeman, et al. "Percentage-Based versus Statistical-Power-Based Vote Tabulation Audits". In: *American Statistician* 62 (Feb. 2008). 11–16. URL: http://verifiedvoting.org/downloads/TAS_paper.pdf; David Jefferson, Elaine Ginnold, Kathleen Midstokke, et al. *Evaluation of Audit Sampling Models and Options for Strengthening California's Manual Count*. California Secretary of State. July 2007. URL: http://www.sos.ca.gov/elections/peas/final_peaswg_report.pdf; Joseph Lorenzo Hall. "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008). URL: http://josephhall.org/papers/jhall_evt08.pdf; Philip B. Stark. "Conservative Statistical Post-Election

audits has galvanized many election officials and election integrity activists to publicly debate various audit methods and procedures.[6]

Much of the recent literature on post-election audits has been sharply critical of existing audit laws, regulations and practices.[7] However, many of these papers seem to contradict each other by promoting very different audit models, and very few provide practical advice about how to implement their recommendations to improve audit practices.

Sorting through this flood of often seemingly contradictory information and using it to improve post-election audits is no easy task. It is, however, critically important. Congress and several state legislatures are likely to consider and pass into law new post-election audit requirements, and the several states that already conduct post-election audits are considering amendments to existing audit laws and procedures.[8]

With the intention of assisting legislators, election officials and the public make sense of this new information and convert it into realistic audit practices, the Brennan Center and the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall School of Law (University of California Berkeley) convened a blue ribbon panel (the "Audit Panel", see Appendix B) of statisticians, voting experts, computer scientists and several of the nation's leading election officials. Together with the Audit Panel, the Brennan Center and the Samuelson Clinic spent several months reviewing and evaluating both existing post-election audit laws and procedures, and the papers of academics and election integrity activists that have frequently criticized such laws and procedures as inadequate. Following this review and extensive consultation with the Audit Panel, the Brennan Center and the Samuelson Clinic make several practical recommendations for improving post-election audits, regardless of the audit method that a jurisdiction ultimately decides to adopt.

Audits". In: *The Annals of Applied Statistics* 2 (2008). 550–581. URL: http://arxiv.org/abs/0807.4005; Philip B. Stark. "A Sharper Discrepancy Measure for Post-Election Audits (in press)". In: *The Annals of Applied Statistics* (Apr. 2008). URL: http://statistics.berkeley.edu/~stark/Preprints/pairwise08.pdf; Stephen N. Goggin, Michael D. Byrne, Juan E. Gilbert, Gregory Rogers, and Jerome McClendon. "Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008)

[6] *Election Audits: Hearing Before the Subcommittee on Elections of the House Committee on House Administration.* 110th Congress. 2007.

[7] Simon and O'Dell, see n. 5; Stanislevic, see n. 5.

[8] Legislation introduced in 2007 to amend or introduce post-election audit requirements include: H.B. 537, 2007 LEG., REG. SESS. (Fla. 2007). H.B. 53, 2007 LEG., REG. SESS. (Pa. 2007), and H.B. 671, 185TH GEN. COURT, REG. SESS. (Mass. 2007).

4.1.1 Limitations of Study

We have limited our study to *post-election audits of voter-verifiable paper records*: how jurisdictions can use a randomly selected percentage of voter-verifiable paper records after the polls have closed to "check" the electronic vote tallies and the performance of electronic voting machines. There are many other types of examinations and audits of voting machines (and the entire voting system) that should be conducted before and after the polls close. For example, sound federal and state certification of voting systems, acceptance testing, and "logic and accuracy" testing are forms of "pre-election" audits and examinations that are critical to ensuring that voting systems accurately record and count votes. Similarly, after an election, comparisons of the number of ballots cast to the number of voters who signed in ("ballot reconciliation"), interviews with poll workers, and full recounts of a contested election are important ways of adding transparency to elections and improving voting technology and election administration.

Instead of attempting to survey all of these elements of examination and auditing, we have chosen to focus on voter-verifiable record-based audits of electronic vote tallies because these audits are at the center of many current legislative debates over election integrity, and because they hold immediate and long-term value for election integrity. The kinds of post-election audits that we discuss here may lend confidence in the results of a close election as well as shed light on voting system problems even when elections are not close. Although it would be ideal to detect voting system problems before an election takes place, recent elections have shown that some problems may be unavoidable, irrespective of the precautions that election officials take. This report sets forth ways in which post-election audits using voter-verifiable paper records may nevertheless provide a systematic means of understanding voting system performance (and failures).

4.1.2 Summary of Findings

Our study of the current academic literature and current state audit laws and procedures points to several important findings:

- Post-election audits of voter-verifiable paper records are a critical tool for detecting

ballot-counting errors, discouraging fraud, and improving the security and reliability of electronic voting machines in future elections. Unfortunately, of the thirty-nine states that require or use voter-verifiable paper records throughout the state, twenty-one do not require such audits after every election.[9]

- Of the few states that currently require and conduct post-election audits, none has adopted audit models that will maximize the likelihood of finding clever and targeted software-based attacks, non-systemic programming errors, and software bugs that could change the outcome of an election.

- We are aware of only two states, North Carolina and California, that have collected and made public the most significant data from post-election audits for the purpose of improving future elections. Based upon our review of state laws and interviews with state election officials, we have concluded that the vast majority of states conducting audits are not using them in a way that will maximize their ability to improve elections in the future.

- Regardless of the audit model a jurisdiction implements, there are several simple, practical, and inexpensive procedures that it can adopt to achieve the most important post-election auditing goals, without imposing unnecessary burdens on election officials.

4.1.3 Post-Election Audit Considerations

In our analysis of the post-election audit debate, we found that much of the disagreement about what constitutes a "sound" audit actually centers on disagreement over the *purpose* of an audit. In fact, there are a number of goals that a post-election audit may serve, and by emphasizing one, jurisdictions may make it more difficult to fulfill another. Among the goals an audit can fulfill are:

- creating an appropriate level of public confidence in the results of an election and allowing for public observation of each audit procedure;

[9] Kibrick, see n. 2.

- deterring fraud against the voting system;
- detecting and providing information about large-scale, systemic errors;
- providing feedback that will allow jurisdictions to improve voting technology and election administration in future years;
- providing additional incentives and benchmarks for elections staff to reach higher standards of accuracy;[10] and,
- confirming, to a high level of confidence, that a 100 percent manual recount would not change the outcome of the race.[11]

Our work is the first to articulate all of these goals and to comprehensively examine the trade-offs that may be entailed to satisfy all of them. We also look at additional considerations that jurisdictions will want to consider when developing audit methods and procedures, including to what extent the audits will be administratively burdensome (i.e., how much they will cost, how many hours they will take to complete, and how much certainty a jurisdiction will have about these issues prior to Election Day) and whether their effectiveness will depend heavily on the subjective judgments of election and other public officials in charge of the audit (something jurisdictions will generally want to avoid).

In most cases, lower administrative costs and greater certainty about the audit ahead of time means less certainty that evidence of an outcome-changing error or of fraud will be found once the election is over. Similarly, audits that are efficient at detecting widely distributed, systemic errors can provide feedback to improve elections, but are often poorer at pinpointing errors that might have affected the outcome of an election. They also generally provide election officials with little guidance as to what should be done when discrepancies between the paper and electronic records are found.

[10] *Collaborative Public Audit of the November 2006 General Election*. Apr. 2007. URL: `http://urban.csuohio.edu/cei/public_monitor/cuyahoga_2006_audit_rpt.pdf`.

[11] This is sometimes described as "confirm that the right candidate was declared the winner," though this is probably more than any statistical audit can guarantee.

4.1.4 Summary of Audit Recommendations

We do not endorse any particular audit model as the "best" one. Instead, we have identified certain basic principles that all jurisdictions should adopt, regardless of the audit model they choose. These recommendations are based on consultation with the Audit Panel and a thorough review of current practices in states and counties where audits are conducted, as well as recent academic literature on post-election audits. The recommendations can be broken into three categories: (1) best practices for selecting votes to be audited; (2) best practices for conducting the audit itself; and (3) best practices for ensuring audit effectiveness. They are discussed in much greater detail in Section 4.3, "Audit Best Practices" (additional recommendations for specific models are discussed in Section 4.2, "A Review of Current and Proposed Audit Models").

Selecting Votes To Be Audited

The method and manner employed by a jurisdiction for choosing votes to audit will have a tremendous impact on whether the audit itself is administratively burdensome, engenders public confidence in election results, detects errors, and provides feedback that will allow jurisdictions to improve elections in the future. Among the most important steps that jurisdictions can take in selecting votes to be audited are the following:

- **Use Transparent and Random Selection Processes for All Auditing Procedures.** Audits are more likely to prevent fraud and produce greater voter confidence in election results if the public can verify that the paper records, machines, or precincts to be audited are chosen in a truly random manner.

- **Audit a Minimum Percentage or Number of Precincts or Machines for Each Election, Including At Least One Machine Model and/or Precinct in Each County.** Much of the recent academic literature on post-election audits focuses on catching error or fraud that could change the outcome of an election. But finding an error that has changed the outcome of an election is in many ways a worst case scenario; most would prefer finding and correcting such errors in landslide elections where they would not affect

the outcome. An audit of a minimum number of precincts or machines supports election officials' efforts to monitor voting system performance and ensure that they operate optimally.

- **Account for Precinct Size Variability in Audit Selection and Sample Size Calculations.** Any analysis, legislation, or administrative procedures that do not take into account the varying number of votes in different precincts are likely to overestimate the audit's confidence level (or "statistical power") with respect to uncovering irregularities that could change the outcome of an election. Methods to deal with precinct size variability can be as simple as sorting precincts into bins of certain sizes (e.g., "small," "medium," and "large"), conducting random selection within each bin or listing precincts in order of size, and ensuring that auditors select a certain number of large precincts.

- **Allow Candidates To Select Precinct(s) or Machine(s) To Be Audited.** Making this option available to candidates would serve two purposes. First, it would give greater assurance to candidates and their supporters that that the election results are correct. Second, it would allow candidates to receive audits of results that seem anomalous that could suggest a programming error or miscount; in effect, allowing them to incorporate other types of data and knowledge that might not otherwise be available.

Conducting the Audit

There are specific steps that every jurisdiction can take to make it far more likely that the audit is accurate, useful to election officials, and likely to catch errors that could change the outcome of certain races. Most importantly, jurisdictions should:

- **Freeze and Publish Unofficial Election Results Before Selecting Precincts or Machines to be Audited.** Election officials should freeze and publish unofficial election results once all returns are received from jurisdictions. The random selection of precincts or machines to be audited should only occur afterwards. This practice allows the public to verify the accuracy and fairness of audit results and minimizes the chances that sources of error or fraud can be hidden from auditors.

- **Conduct "Blind" Manual Counts.** While unofficial totals should be made available to the public so that they can verify the accuracy and fairness of the audit, manual counters should be "blind" to the unofficial election results for the machines they are auditing to ensure that knowledge of the unofficial results does not influence their counting.[12]

- **Don't Just Match—Count! (Record and Publicly Release Meaningful Data on Votes Cast).** Audits that record and detail the overvotes, undervotes, blank votes, spoiled ballots, and, in the case of DREs with VVPATs, cancellations, could be extremely helpful in revealing software attacks and software bugs and in identifying problems with ballot design and/or ballot instructions. Rather than only matching paper and electronic tallies, election officials should record and publicly release this meaningful data, which should be useful for improving elections in the future.

- **Consider Auditing by Machine Rather Than Precinct.** In many states, it will be more efficient to audit by machine or ballot batches rather than by precinct. Particularly in states that use touch-screen voting machines, jurisdictions will be able to achieve the same or better level of confidence in their results by auditing a smaller percentage of machines.

- **Audit All Methods of Voting.** In conducting post-election audits, election officials should not exclude any category of votes (e.g., absentee ballots, provisional ballots, damaged ballots). In 2004, seven states reported that more than twenty percent of all votes were cast during early voting periods.[13] Excluding these ballots from an audit would leave a significant opportunity for errors to remain undetected.

Ensuring Audit Effectiveness

If the audit is to be effective, jurisdictions must have certain basic policies and practices in place. Most importantly, jurisdictions should:

[12] However, we discuss in the next chapter instances in which blind counting may be "too blind".

[13] *Final Report of the 2004 Election Day Survey*. Election Data Services. Sept. 2005. URL: http://www.eac.gov/clearinghouse/docs/eds2004/2004-election-day-survey-full-report/?searchterm=election%20survey%202004, at 4-7.

- **Ensure the Physical Security of Audit Materials.** Effective auditing of voter-verifiable paper records will serve to deter attacks on voting systems and identify problems only if states have implemented solid procedures to ensure the physical security of election materials used in a post-election audit, such as records of the vote, voting machines, and tally servers.

- **Implement Effective Procedures for Addressing Evidence of Fraud or Error.** If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for addressing discrepancies between the paper records and electronic tallies when they are found. Without protocols for responding to discrepancies, the detection of fraud or error will not prevent it from successfully altering the outcome of an election. Recommended responses include making corrections where warranted, disallowing results if an appropriate remedy cannot be determined, and ensuring accountability for discrepancies. Jurisdictions should document discrepancies and any actions in response to them in publicly available discrepancy logs.

  When there have been no losses or additions of paper records, a single unexplained discrepancy between the paper records and electronic tallies is a strong indication of a software problem of some kind. Any such discrepancy, even if it is just one vote and can have no effect on the outcome, is grounds for a review of voting machine software code. Such a review need not delay certification of the election, but it *should* be investigated. To be effective, election officials must have the ability to *audit the code,* not just the votes.

- **Audit the Entire Voting System, Not Just the Machines.** Although this study focuses only on post-election audits of voter-verifiable paper records, jurisdictions should conduct audits of the entire voting system to catch errors or fraud in other parts of the voting system. Historically, incorrect vote totals often result from aggregation mistakes at central vote tally locations. Accordingly, good audit protocols will mandate that the entire system—from early and absentee ballots to aggregation at the tally server—be audited for accuracy. This should also include, at the very least, the ability of election officials to *audit the code* where they deem necessary.

4.2 A Review of Current and Proposed Audit Models

There are three basic categories of post-election audits described in current law, proposed bills, and academic literature. They are as follows:

1. **Fixed-Percentage Audit Model.** Most states that currently conduct post-election audits use this model. Jurisdictions are required to randomly select a fixed percentage of precincts or machines to audit. All voter-verifiable paper records for the selected precincts or machines are hand-counted and compared to the electronic tallies.

2. **Adjustable-Percentage Audit Model**. This model requires jurisdictions to determine the percentage of precincts or machines to audit based on the size of the margin of victory between the two leading candidates in a race. The smaller the margin of victory, the larger the percentage of precincts or machines to audit. While we are unaware of any state that has explicitly adopted a form of this audit model, several states require full or partial recounts of voter-verifiable paper records when races are extremely close.[14] Moreover, most of the recent academic articles we have reviewed have endorsed flavors of this method, and it appears to be gaining support among legislators and election integrity activists around the country.[15]

3. **Polling Audit Model.** This model requires a randomly chosen, small sample of ballots be recounted in *every* precinct and that these tallies be compared to the unofficial electronic results. We are not aware of any jurisdiction that has adopted this approach, though several election integrity advocates have endorsed it.[16]

In the sections below, we describe and evaluate each audit model in detail and provide specific recommendations (in addition to those already discussed in Section 4.1.4) for improving each one.

[14] For instance, in statewide elections in Ohio, the Secretary of State shall order a recount when the vote total of the winning candidate is less than the vote total for the second-place candidate by less than one quarter of one percent. OHIO REV. CODE ANN. Sec. 3515.011 (West 2007).

[15] See *e.g.*, S. 507, 212TH LEG., REG. SESS. (NJ 2007); Dopp and Stenger, see n. 5; Lobdill, *Election Audit Sampling Plan—It's Not Just About Sampling Without Replacement*, see n. 5; Rivest, *On Auditing Elections When Precincts Have Different Sizes*, see n. 5; Rivest, *On Estimating the Size of a Statistical Audit*, see n. 5; McCarthy, Stanislevic, Lindeman, et al., see n. 5

[16] Simon and O'Dell, see n. 5.

4.2.1 The Fixed-Percentage Audit Model

This model, employed by most states that currently conduct audits, requires jurisdictions to randomly select a fixed percentage of precincts or machines to audit. All voter-verifiable paper records for the selected precincts or machines are manually counted and compared to the electronic vote tallies.

Model Implementation

Because some variant of this audit model is used in at least fourteen states, we have several examples of how it can be implemented.

The minimum fixed audit percentages have ranged from Utah's audits of one percent of voting machines to Connecticut's recent audit of twenty percent of precincts using optical scan voting machines.[17] There is a considerable range between these extremes, though most states tend to fall at the lower end of the spectrum. Aside from Hawaii, which requires an audit of ten percent of precincts, the other states that have adopted the fixed-percentage approach require minimum audits of five percent of precincts or machines, or less.[18] In Minnesota, the number of precincts to audit in each county depends on the number of registered voters: counties with fewer than 50,000 registered voters must audit at least two precincts, while counties with more than 100,000 registered voters must audit at least four precincts.[19]

States also differ on the question of whether to audit precincts or individual voting machines. The basic principle in both cases is the same: auditors must tally paper records and compare the results to the electronic tally for the recounted precinct or machine. For the reasons explained by Howard Stanislevic in a paper on determining the proper size of an audit,[20] a machine-level audit can produce the same confidence level as a precinct-level audit with a lower amount of effort. (Alternatively, for the same level of effort, a machine-level audit can produce a higher confidence level than a precinct-level audit.) Most states

[17] *Case Study: Auditing the Vote*. Electionline.org. Mar. 2007. URL: `http://www.pewcenteronthestates.org/report_detail.aspx?id=34140`.
[18] HAW. REV. STAT. Sec. 16-42(b)(3) (2006).
[19] MINN. STAT. ANN. Sec. 206.89 (West 2007).
[20] Stanislevic, see n. 5, at 15.

that conduct fixed-percentage audits do so at the precinct-level, though New York plans to conduct manual audits at the machine-level.[21]

Another variable among these states is the number of contests reviewed in an audit. Connecticut, California, and Illinois check all of the races on a ballot during a post-election audit, which in California, can be as many as 200 races in a single county.[22] In contrast, both Hawaii and New Mexico review just one race in an election during a post-election audit.[23] Arizona requires jurisdictions to review at least 4 contested races, including one federal race, one statewide race, one ballot measure, and one legislative race.[24]

Finally, states vary in how they select the precincts or machines to be audited. In California, for instance, precincts are chosen at the county level, with little direction from the state as to how the precincts should be selected.[25] By contrast, precincts are selected at the state level in Illinois.[26]

State-level audit selection, carries some disadvantages. Some states may be too large—geographically, or in terms of the number of precincts, or both—to select precincts in a reasonable amount of time during a single official event. Selecting precincts or machines to audit in a central location might also make it difficult for local election officials and voters to observe the selection process for their own jurisdiction. This could undermine the transparency that public audit selection should foster. Finally, since audit selections should occur after all ballot types, including absentee and provisional ballots, have been counted, there is a risk that a single jurisdiction with a high proportion of these could hold up statewide audit selection.

Regardless of whether a jurisdiction chooses to audit by precinct or machine, audit one percent or twenty percent, or select precincts or machines at the state or county level, there are certain procedures that must be implemented if this model is to be as effective and efficient as possible. We discuss some of these procedures below.

---

[21] N.Y. ELEC. LAW Sec. 9-211 (McKinney 2007).

[22] CONN. GEN. STAT. ANN. Sec. 9-242b(5) (West 2007); 10 ILL. COMP. STAT. ANN. Sec. 5/24C-15 (West 2007); E-mail from Dean Logan, Chief Deputy Registrar-Recorder/County Clerk, Los Angeles County, California to Lawrence Norden (Mar. 19, 2007).

[23] N.M. STAT. ANN. Sec. 1-14-13.1(A) (West 2007); Lawrence Norden telephone interview with Scott Nago, Counting Center Operations Coordinator, Office of Elections, Hawaii (July 1, 2007).

[24] ARIZ. REV. STAT. ANN. Sec. 16-602(C) (2007).

[25] CAL. ELEC. CODE Sec. 15630, 19253 (West 2007).

[26] 10 ILL. COMP. STAT. ANN. Sec. 5/24C-15 (West 2007).

Audit Model Strengths

The fixed-percentage audit model should detect errors and fraud above a certain threshold (dependent on the size of the audit). Assuming a low, single-digit percentage audit, this type of audit should easily detect a software bug or programming error that affects large numbers of votes on a large number of machines.

Moreover, when an unexplained discrepancy between the paper records and electronic tallies is found, it should be fairly easy for election officials to identify the machine, race and/or ballot type affected by the discrepancy. Thus, we can imagine a scenario where a software bug on certain DREs causes the machines to lose the electronic record of anyone who has voted on Spanish language ballots. The direct comparison of paper records (which have not been lost) to electronic tallies should allow us to identify fairly quickly which types of ballots have been affected. As discussed in greater detail below, this is not necessarily true of other audit methods (see Sections 4.2.2 and 4.2.3).

Finally, under this audit model, jurisdictions will have relatively low and foreseeable administrative costs. Because jurisdictions know in advance what percentage of precincts or machines will be audited, they may make the necessary logistical preparations for a post-election audit, such as hiring auditors and determining how long the audits are likely to take.[27]

Audit Model Weaknesses

While the fixed-percentage audit model has the benefits of detecting widespread discrepancies, yielding detailed information about their possible sources, and of imposing predictable costs and time requirements, it has two major weaknesses. The first weakness has been identified in several academic papers: the closer a race is, the less likely this type of audit can provide confidence that a software bug, programming error, or malicious software attack did not alter the outcome of the election.[28]

As an example of this first weakness, Table 4.1 illustrates the problem of low confidence

[27] This statement is subject to the caveat that a state recount law might require a full recount in the event of a close election; but this is a possible expense regardless of whether there is a mandatory audit at all.

[28] Dopp and Stenger, see n. 5; Rivest, *On Estimating the Size of a Statistical Audit*, see n. 5; Simon and O'Dell, see n. 5; Stanislevic, see n. 5; McCarthy, Stanislevic, Lindeman, et al., see n. 5.

levels in a typical Congressional district of 400 precincts where precincts are assumed to be of roughly equal size for the purposes of simplicity.[29] We have assumed that this state mandates an audit of five percent of all precincts (as is the case, for example, in Illinois). We have further assumed that if more than twenty percent of the ballots in any single jurisdiction were corrupted, election officials and the public would detect the corruption without an audit. This is a common assumption in academic literature on post-election audits.[30]

Number of Precincts	Margin of Victory	Confidence Achieved
400	5%	94%
400	2%	65%
400	1%	40%

Table 4.1: The confidence of detecting one corrupt precinct in a 5% fixed-percentage audit for a model Congressional district with 400 precincts.

The numbers in Table 4.1 were calculated assuming a two-person race, where "margin of victory" is determined by subtracting the total votes for the loser from the total votes for the winner, and dividing by the total number of ballots cast and counted.[31] The smaller the margin of victory, the less confidence we have that the five percent audit will catch a software bug, programming error, or malicious software attack that could have altered the results of an election. The reason for this is simple: in a race decided by more than five percent of the vote, a software bug, malicious attack, or programming error will have to affect a large number of votes to change the outcome of the election. A five percent audit should catch such an error that affects a large number of votes. In contrast, in a race decided by only one percent of the votes, a software bug, malicious attack, or programming error will only have to corrupt a small number of votes to change the outcome. In this case, there

[29]For a brief introduction to the mathematics behind these calculations, see the Primer on Election Audit Mathematics in Appendix D.

[30]Dopp and Stenger, see n. 5 (assuming that a corruption of more than fifteen percent of ballots would be caught); Norden and Lazarus, see n. 4 (assuming that a corruption of more than twenty percent of ballots would be caught); Stanislevic, see n. 5 (assuming that a corruption of more than twenty percent of ballots would be caught); McCarthy, Stanislevic, Lindeman, et al., see n. 5 (assuming that a corruption of more than twenty percent of ballots would be caught).

[31]Note: If a Congressional District has fewer than 400 precincts, confidence levels will be significantly lower. If precinct size varies within a Congressional District, it will be more difficult to obtain a high level of confidence in the results, unless precinct selection is weighted by the number of voters in each precinct. Rivest, *On Auditing Elections When Precincts Have Different Sizes*, see n. 5; Stanislevic, see n. 5

is a small chance that we would find the corrupt machines or precincts if we audited only five percent of them.

In the discussion above, we have assumed that the Congressional district in question is contained within a single election jurisdiction. In practice, many Congressional districts span multiple counties, which are, in turn, responsible for administering their own elections. In such cases, counties will be sampling from an even smaller number of precincts than a jurisdiction would sample if it selected from the entire Congressional district, without regard to county borders. Sampling a fixed percentage of this smaller (county-based) number of precincts will produce an even lower confidence level than the numbers discussed above.

Addressing the Problem of Low Confidence Levels

Appel and others have proposed a remedy to the problem of low confidence levels produced by a fixed-percentage audit: allow candidates to select additional precincts or machines to be audited.[32] This practice of non-random and "targeted" auditing is common in the financial industry and other areas where government has an interest in ensuring honest reporting.[33] It is already effectively enshrined in law in some states, such as New Hampshire and North Dakota, where candidates can ask for recounts in some or all precincts at little or no cost.[34]

We endorse this suggestion for all elections, as it would serve two confidence-building purposes. First, it would give greater assurance to candidates and their supporters that the election results are correct. Second, it would allow candidates to receive audits of results that seem anomalous and might suggest a programming error or miscount. Given the low confidence levels produced by fixed-percentage audits of close elections, this recommendation is particularly important.

Another potential remedy to this weakness would be to increase the level of audits in very close races. Several states that conduct fixed-percentage audits require a *full* recount of

[32] Appel, see n. 5; *Written Statement of Lawrence Norden, Counsel, Brennan Center for Justice at NYU School of Law*. Committee on House Administration, Subcommittee on Elections, United States House of Representatives. Mar. 2007. URL: `http://brennan.3cdn.net/376a9785b68b83c66d_ofm6bnbh2.pdf`

[33] *1994 Audits of Workers' Compensation Insurers, Self-Insured Employers, and Third-Party Administrators*. California Department of Industrial Relations, Division of Workers' Compensation. Mar. 1995. URL: `http://www.dir.ca.gov/dwc/1994REP1.HTM`; *Audits Fact Sheet*. Massachusetts Department of Environmental Protection. URL: `http://www.mass.gov/dep/cleanup/audfs.htm`.

[34] N.H. Rev. Stat. Ann. Sec. 660:2 (2007); S.D. Codified Laws Secs. 12-21-8–12-21-11 (2006).

paper records when the margin of victory between the two leading candidates is very small. Connecticut automatically requires a recanvass of voting machine returns and absentee ballots if the margin of victory between the top two candidates is less than twenty votes or less than one half of one percent of the total votes cast for the office in question (up to 2,000 votes).[35] In Arizona, if the margin between the two top candidates is equal to or less than one tenth of one percent of the number of votes cast for both candidates, a full recount for the affected office will occur.[36] How to implement this remedy is discussed in greater detail in the next section of this paper "The Adjustable-Percentage Audit Model" (Section 4.2.2).

Acting on Discrepancies

The second weakness of the fixed-percentage audit model is that discrepancies that may seem minor (e.g., a three-vote discrepancy between the paper records and electronic tallies in a particular precinct) could indicate far larger problems. This model will be effective only if an investigation and additional action are initiated when discrepancies between the paper records and electronic tallies are found.

The discovery of any discrepancy should prompt two actions. First, additional manual counts should occur to confirm the existence of discrepancies. Of the states that have laws or regulations relating to audit discrepancies, only eight require additional audits when such discrepancies are discovered, and those requirements for further action vary widely.[37] Hawaii audit law requires additional auditing if discrepancies are found, but does not describe how the additional auditing should be conducted.[38] In Minnesota, a difference greater than one half of one percent between the result of a manual audit and the electronic tally triggers the auditing of at least three additional precincts in the affected jurisdiction. If the discrepancy persists, the county auditor must review ballots in the rest of the county.[39] In New Mexico, a difference between the manual count and electronic tally greater than one and one half percent triggers a recount of ballots cast for the affected office in the legislative district where the discrepancy occurred.[40] In Arizona, discrepancies between the paper

[35] Conn. Gen. Stat. Ann. Sec. 9-311a (West 2007).
[36] Ariz. Rev. Stat. Ann. Sec. 16-661(A) (2007).
[37] Electionline Audit Briefing, see n. 17.
[38] Haw. Rev. Stat. Sec. 16-42(b)(4) (2006).
[39] Minn. Stat. Ann. Sec. 206.89 (West 2007)
[40] N.M. Stat. Ann. Sec. 1-14-13.1(B) (West 2007).

records and the electronic vote tallies equal to or greater than a "designated margin" trigger a second manual count. If after a second manual count discrepancies equal to or greater than the accepted "designated margin" persist, the audit is expanded to include twice as many precincts, randomly selected by lot.[41]

Some discrepancies between paper and electronic counts may be caused by human counting errors or by different interpretations of voter intent by a human counter and a voting machine. Although discrepancies are not necessarily proof that there was widespread fraud or error, as the Brennan Center Task Force on Voting System Security noted in *The Machinery of Democracy*, they can indicate a much larger problem with the election.[42] As such indicators, discrepancies should trigger other types of action by election officials.

Our second recommendation for acting on discrepancies is to investigate their causes and to respond appropriately to investigation findings.[43] For example, in Minnesota, if a voting system is found to have failed to record votes accurately and in the manner provided by the Minnesota election law, the voting system must not be used at another election until it has been examined and recertified by the Secretary of State. If the voting system failure is attributable to either its design or to actions of the vendor, the vendor must forfeit the vendor bond and the performance bond as required by Minnesota law.[44]

Generally, our review of state laws and interviews with election officials revealed that the majority of jurisdictions do not have adequate, detailed, and practical procedures for action to be taken when unexplained discrepancies are found. Jurisdictions should conduct a investigation of all machines where the paper records and electronic tallies do not match to try to determine the cause of any discrepancies. In particular, especially for DREs, an investigation should include a review of the software code, as discrepancies may have been caused by a software bug or programming error. As in Illinois, the "State Board of Elections, State's Attorney and other appropriate law enforcement agencies, the county leader of each political party, and qualified civic organizations" should be notified of the discrepancies and have an

[41] ARIZ. REV. STAT. ANN. Sec. 16-602(D) (2007).
[42] Norden and Lazarus, see n. 4.
[43] Norden and Lazarus, see n. 4, make a number of recommendations as to what such procedures and laws might look like in Appendix M at page 147.
[44] MINN. STAT. ANN. Sec. 206.57, 66 (West 2007).

opportunity to send observers to the investigation.[45] Additionally, election officials should create a "discrepancy log" in which to list all discrepancies, identify the precinct and machine where they occurred, describe their causes, and record any actions taken in response to them.[46] The discrepancy log and the findings of any investigation should be made available to the public. The adoption of these two practices would significantly strengthen the fixed-percentage audit model's ability to serve as an effective countermeasure to outcome-changing fraud or error.

Administrative Considerations

Time and Cost of Audit

Because the number of precincts or machines audited rarely changes significantly from one election to the next, the time and cost of fixed-percentage audits should remain stable over time. These factors should only change significantly if discrepancies trigger additional audits. Determinants of the time and cost of an audit include: the percentage of precincts or machines audited, the number of persons staffing the audit, and the number of races audited.

State reporting of the amount of time it takes to complete an audit varies. Counties in Illinois report that five percent audits of ten to twelve races in an election generally take anywhere between two hours to two days.[47] In Hawaii, an audit of ten percent of precincts for a single race is generally completed in less than a week. In Clark County, Nevada, where officials audited dozens of races in two percent of precincts in 2006, the audit was completed in just a few days. In Los Angeles County, California, it has generally taken close to twenty-eight days to audit one percent of all of the contests in a general election (since 2000, that number has been anywhere between 134 and 194 contests).[48]

The largest component of a fixed-percentage audit's cost is likely to be associated with managing and staffing the audit. If states hope to achieve accurate audit results using best practices applied consistently, the preponderance of the costs of audits is likely to lie in re-

[45] 10 Ill. Comp. Stat. Ann. Sec. 5/24C-15 (West 2007).

[46] For example, see: *County Manual Tally Reports*. California Secretary of State. Apr. 2008. URL: `http://www.sos.ca.gov/elections/manual_count_reports.htm`.

[47] Various telephone interviews. See: Norden, Burstein, Hall, and Chen, see n. 1, at 81 (note 44–48).

[48] E-mail from Dean Logan, note 22.

cruiting, paying, and training quality management and covering travel costs—at least in initial years. These costs will vary, depending on the number of auditors required to complete the audit and the magnitude of any financial compensation. During Hawaii's ten percent audit of a single race in 2006, the smallest county required seven auditors while the largest county required forty-five. In many cases, jurisdictions use election workers already on their payroll to avoid incurring additional staffing costs.[49] A typical hand count on election night in 2006 in Walpole, New Hampshire involved nine two-person teams and three managers to count 1,574 ballots, with each ballot having the equivalent of 14 contests.[50]

Despite this variance, for all cases where we have been able to review actual cost data, the overall cost of a fixed-percentage audit has been surprisingly low compared to what is already spent by jurisdictions on elections. Unfortunately, comparing the costs of one jurisdiction to the next is difficult because jurisdictions report costs differently, some on a per ballot basis and others on a per precinct basis. In North Carolina's first audit in 2006, the average cost of the audit of a single race in 260 precincts was sixty-five dollars per precinct.[51] In November 2006, Minnesota examined three contests in 202 precincts at an estimated cost of $135 per precinct.[52] Pima County, Arizona examined four contests in each of nine precincts, plus additional provisional ballots, for a little over thirteen cents per ballot.[53] Had they paid the market rate of $7-10 per hour for counters and $20 per hour for managers, the 2006 Walpole, New Hampshire election night hand count of 1,574 fourteen-race ballots, with nine two-person counting teams, would cost about four cents per ballot, per race.

The Challenge of Matching Paper and Electronic Records

Counting paper records presents at least two related problems. The first is that people

[49] See: Testimony of Deborah Seiler, Elections Manager, Solano County, California; Testimony of John Tuteur, Clerk, Napa County, California from: *Public Meeting, July 2, 2007 of the Post-Election Audit Standards Working Group*. California Secretary of State. July 2007. URL: http://www.sos.ca.gov/elections/post_e/post_election_meet07.htm

[50] Anthony Stevens, Assistant Secretary of State, New Hampshire, *personal communication*.

[51] North Carolina State Board of Elections, Statewide May 2006 Primary Election One-Race Audit Results, URL: http://www.ncvoter.net/downloads/NCSBOE_Primary_Sample_audit_count_short.xls (last visited June 2008).

[52] Mark Halvorson, Director and Co-Founder, Citizens for Election Integrity, Minnesota, *personal communication*.

[53] *2006 Pima County General Election Audit Summary*. Division of Elections, Pima County, Arizona. Nov. 2006. URL: http://www.azsos.gov/election/2006/general/handcount/Hand_Count_06_General_Pima.pdf.

often miscount. Consequently, there are going to be many instances where the hand count of paper records and the electronic tally do not match, not because there was a problem with the machines, but because the auditors made mistakes counting. There has been very little research evaluating different methods of hand-counting, but we discuss directions such research should take in the "Directions for the Future" section of this paper (Section 4.4).

Several jurisdictions partially address the problem of miscounting by having at least two people count the same paper record. For example, San Mateo County, California uses a team of four people to conduct their post-election audit.[54] One person reads and announces the contents of a given paper record, another observes that the paper record has been announced correctly and two people record a running tally of votes for each contest. The recorders announce the end of each ten-vote increment, at which point the team checks for errors in the tally. If the team finds an error, the counting process can be rolled back to the last point of agreement.[55]

Minnesota provides an example of how incremental checking during post-election audits works in practice. Minnesota law requires election judges to count the votes for each race or ballot question by creating piles of voted ballots for each candidate in a race and piles for blank or defective responses.[56] Election judges check the sorted piles of ballots for the particular race or question to ensure that all ballots have been placed in the correct pile. Ballots may be stacked in groups of twenty-five crosswise.[57] After the final count for the race or question is completed, all ballots are returned to a single pile and the process is repeated for the subsequent race or ballot question.

The second, related problem is that auditors are likely to *want* the paper records to match the electronic records. The problems in Cuyahoga County, Ohio in 2004, where audit supervisors rigged the ballot selection so that no discrepancies would be found, exemplify

[54] Hall, "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures", see n. 5; Joseph Lorenzo Hall. *Procedures for California's 1% Manual Tally*. UC Berkeley School of Information. Apr. 2008. URL: http://josephhall.org/procedures/ca_tally_procedures-2008.pdf.

[55] *One Percent Manual Recount Procedures*. San Mateo County Clerk Assessor Recorder Elections. Dec. 2007. URL: http://josephhall.org/procedures/sanmateo_tally_procedure_122007.pdf.

[56] MINN. STAT. ANN. Sec. 204C.21 (West 2007).

[57] The piling method of counting ballots is commended by Citizens for Election Integrity Minnesota. See: Mark Halvorson and Laura Wolff. *Report and Analysis of the 2006 Post-Election Audit of Minnesota's Voting Systems*. Citizens for Election Integrity Minnesota. Apr. 2007. URL: http://www.ceimn.org/files/CEIMNAuditReport2006.pdf

the danger of auditors hoping to find perfect matches and to avoid the difficult questions and additional work that might result if the records do not match.

To counter the understandable temptation to make the paper and electronic records match, we recommend against revealing the unofficial electronic election results to the individuals performing the manual count. The audit teams should not have access to the unofficial results; an audit supervisor or election official can serve as a buffer and inform each team if their audit results match the unofficial electronic results, without revealing the magnitude or direction of any deviation. If the manual count does not match the electronic results, the audit team should conduct additional "blind" recounts of the records of affected races.[58]

Manual counts may sometimes reveal different voter intent than machine counts of ballots. Overvotes, marginal marks, hesitation marks, and other stray markings on manually marked ballots could cause optical scan voting machines to misinterpret voter intent that a human reviewer would be able to discern. This may lead to deviations or explained discrepancies when auditing optical scan paper ballots. Fortunately, these discrepancies are easy to recognize and account for, so they should not cause any serious problem; they qualify as an explained discrepancy and need not trigger any kind of recount or additional audit, except in the case of an extremely close race, where these could make a difference.

Other Factors

Jurisdictions that use DREs with voter-verifiable paper records may face an extra challenge in sorting paper records by precinct prior to auditing, creating additional costs. Some jurisdictions locate precincts with different ballots in a single polling place. Voting machines in a polling place may be programmed to store and enable multiple precinct ballot layouts, allowing voters of different precincts to cast ballots on a single machine. As a result, the polling place's set of voter-verifiable paper records will need to be carefully sorted by precinct so that the records for a precinct selected for auditing will not include records corresponding to other precincts. Alternatively, if a precinct in a multiple-precinct polling place is selected for an audit, election officials can automatically add the other precincts in

[58] David Wagner. *Thoughts on the Nov 16, 2006 1% Manual Tally in Yolo County*. UC Berkeley Department of Computer Science. Nov. 2006. URL: `http://www.yoloelections.org/news/snews/reactions.pdf`.

the polling place to the audit to avoid the costs of sorting records.

An additional consideration for all audit methods is the quality of the voter-verifiable paper records. A widely reported problem with the current generation of DREs outfitted with voter-verifiable paper record printers is that some of the records are unreadable. For example, in Cuyahoga County, Ohio's May 2006 primary election, ten percent of the paper records were unreadable due to paper jams and other printer malfunctions. A high proportion of spoiled voter-verifiable paper records could have significant negative consequences on an audit's effectiveness. Quantifying the impact of spoiled paper records is beyond the scope of this paper, but a qualitative example might be helpful. Spoiled paper records could effectively hide discrepancies and thus allow a greater proportion of discrepancies per precinct to go undetected. For an adjustable-percentage audit (Section 4.2.2), this would lead to an underestimate of the audit size. More generally, spoiled voter-verifiable paper records could drown out the effect of more subtle voting system errors, frustrating the goal of collecting data about voting machine performance during audits.

Recommendations to Improve the Model

In addition to the general recommendations for all audit models made above in Section 4.1.4 and which we reiterate here, we also make the following recommendation to strengthen the fixed percentage model:

- **Implement Effective Procedures for Acting on Seemingly Small Discrepancies.** If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for addressing audit discrepancies when they are found. As noted in *The Machinery of Democracy*, a seemingly minor discrepancy between paper and electronic records (of even just a few votes) could indicate far more serious problems.[59] Without protocols for responding to discrepancies, the detection of fraud or error will not prevent them from occurring again. Such protocols should include a required review of system software code.

  Furthermore, given the low-confidence levels that a fixed-percentage audit will some-

[59] Norden and Lazarus, see n. 4, at 7.

times produce, we highlight the following recommendation for the fixed percentage model in particular:

- **Allow Candidates To Select Precinct(s) or Machine(s) To Be Audited.** In addition to using random selection procedures, jurisdictions should allow candidates to pick at least one precinct or machine to be audited. This practice would allow candidates to receive audits of results that seem anomalous to them and give greater assurance that the election results are correct.

4.2.2 The Adjustable-Percentage Audit Model

The adjustable-percentage audit model attempts to address the problem of low confidence levels in close races produced by the fixed-percentage audit model. This audit model requires a state or local jurisdiction to determine what percentage of precincts or machines to audit for each race based on the size of the margin of victory between the two leading candidates. The smaller the margin of victory, the larger the percentage of precincts or machines that will need to be audited. The mathematics behind this method involves calculating a sample size given the margin in the closest race on the ballot and a desired confidence level for detecting error or fraud.[60]

Many recent academic articles endorse variants of the adjustable-percentage audit model—often in conjunction with adjustments for variations in number of voters in different units (e.g., precincts or machines)—and it appears to be gaining currency among legislators and election integrity activists around the country.[61] Congressman Rush Holt proposed a variation of the adjustable-percentage audit model in the "Voter Confidence and Increased Accessibility Act of 2007," which had support from more than a majority in the U.S. House of Representatives, but was ultimately defeated.[62] Legislators and chief election officials in several states are also considering adoption of similar audit methods.[63]

[60] For a basic primer on the mathematics of post-election audit sampling, see Appendix D or: Joseph Lorenzo Hall. *A Quick Primer on the Mathematics of Post-Election Audit Confidence*. Mar. 2007. URL: `http://www.josephhall.org/eamath/eamath.pdf`

[61] S. 507, 212TH LEG., REG. SESS. (NJ 2007).

[62] See: 110th Congress. *H.R. 811—Voter Confidence and Increased Accessibility Act of 2007*. GovTrack.us (database of federal legislation). 2007. URL: `http://www.govtrack.us/congress/bill.xpd?bill=h110-811`.

[63] Notably, the California Secretary of State has required a tiered or "escalated" post-election audit for the

Model Implementation

The goal of an adjustable-percentage audit is to reach a minimum level of "confidence." In this context, confidence refers to a measure of the probability that a full recount of the voter-verifiable paper records would not change the outcome of an election. To make this determination, a jurisdiction will need to know a few things: the number of precincts or machines to be audited, the variation in the number of votes per precinct or machine, the unofficial margin of victory, and the confidence level or "statistical power" the jurisdiction would like to achieve.[64]

With this information and the use of scientifically reasonable assumptions, election officials (with the assistance of statisticians, where necessary) can determine how many precincts or machines to audit to reach a desired minimum level of confidence. To illustrate this more concretely, consider the meaning of an adjustable-percentage audit that yields a ninety-five percent confidence level: holding the assumptions discussed below as true, if an outcome-changing level of error or fraud exists, there is a ninety-five percent chance that this audit will detect it (and, accordingly, a five percent chance that it will not). An audit designed to give a fifty percent confidence level would have an equal chance of finding and not finding such error or fraud.

An adjustable-percentage audit can be implemented in several different ways. We discuss two of the most commonly suggested methods below.

Audits of Additional Precincts or Machines in Close Races

One implementation of the adjustable-percentage audit model is similar to the implementation of the fixed-percentage audit model discussed earlier. If a state requires an audit of a minimum percentage of precincts or machines, selection can begin at the state or county level as soon as the unofficial results are frozen and published. For any close races, election officials will select additional precincts to audit to achieve a desired level of confidence.

The determination of how many additional precincts to select in close races (and their subsequent selection mechanism) is a challenge that is unique to this model. We exam-

past year: *Post-Election Manual Tally Requirements*. California Secretary of State. Oct. 2007. URL: `http://www.sos.ca.gov/elections/voting_systems/ttbr/post_election_req.pdf`.

[64] McCarthy *et al.* define statistical power as "the probability of detecting an outcome-altering miscount", see: McCarthy, Stanislevic, Lindeman, et al., see n. 5.

ine below how a state-level entity could select additional precincts in federal races with small margins of victory. We discuss this arrangement, which deviates from most states' county (or other jurisdiction)-based procedures for two reasons. First, a centralized procedure may ease the coordination of public observation of random selection processes by allowing observers to witness one selection process at the state level, rather than attempt to witness dozens of county-level procedures. Second, the Voter Confidence and Increased Accessibility Act of 2007, mentioned above, would require state-level selection of precincts or machines for an audit.

For audits of close races, the selection of additional precincts over the minimum percentage would work as follows: shortly after the polls close, county election officials would compile the final unofficial election results for all precincts and forward their county-level results to state election officials (as is already done in some states, such as California). Election officials would then determine the unofficial margin of victory in each race and use a confidence-based audit algorithm (discussed below) or table to determine the number of additional precincts that must be audited for each election. Election officials would then randomly select the determined number of additional precincts to audit within their jurisdiction and notify each other county involved in that race. The county would then audit all of the races in the selected precincts. More detailed suggestions on the selection of additional precincts in close races for audits can be found in Appendix C.

Tiered Audit Levels Based On Margins of Victory

Congressman Holt's legislation proposed a variation of the adjustable-percentage audit—a "tiered" approach. For all federal races decided by a five percent margin or greater, an audit of three percent of precincts would automatically occur. For federal races decided by less than a two percent margin, the number of precincts audited will increase from three percent to five percent. When a race is decided by less than a one percent margin, ten percent of a Congressional district's precincts will be audited.

We can see how this tiered approach can increase confidence levels by returning to our model Congressional district, introduced in the previous section of this paper on fixed-percentage audits. We make the same assumptions as we did before, namely, that there are 400 precincts in the Congressional district of roughly equal size, and a vote shift of

more than twenty percent in any precinct would be easily identified, deemed suspicious, and investigated, regardless of any mandated audit.

In this example, we will look at the tiered audit as proposed in Congressman Holt's bill. The highlighted numbers represent the confidence level achieved by the proposal.

Precincts (#)	**Margin (%)**	**Confidence (2% Audit)**	**Confidence (3% Audit)**	**Confidence (5% Audit)**	**Confidence (10% Audit)**
400	0.75%	15%	22%	34%	**58%**
400	1.75%	31%	43%	**61%**	86%
400	5.00%	66%	**80%**	94%	99%

Table 4.2: For a model Congressional jurisdiction of 400 precincts, we calculate the confidence of detecting one corrupt precinct with different sized audits given varying margins of victory.

The numbers in Table 4.2 were calculated assuming a two-person race, where "margin of victory" is determined by subtracting the total votes for the loser from the total votes for the winner, and dividing by the total number of ballots cast, including undervoted ballots and ballots disqualified in that race. Jurisdictions would have greater confidence that result-changing errors were caught by an adjustable-percentage audit than by a fixed-percentage audit because the audit level increases as the margin of victory shrinks.

As some commentators have noted, where Congressional districts have fewer than 400 precincts, or where precincts vary substantially in size,[65] these confidence levels will decrease across the board. In practice, determining the number of precincts that must be audited would require a specific calculation that takes into account the distribution (i.e., actual votes per precinct) in the given Congressional district. Nevertheless, the basic concept remains unchanged: by increasing the audit percentage in close races, we gain greater confidence that result-changing errors will be caught.[66]

Table 4.3 shows the predicted impact of a tiered audit in 2002, 2004, and 2006. "Federal races" includes all Congressional races and Presidential races in the fifty states and the District of Columbia. Although a tiered audit adds some complexity to the process, it would

[65] New Hampshire, where the number of registered voters in a precinct can vary from one to 19,000 voters, provides an extreme example of precinct size variation. Anthony Stevens. *Hand Counting Paper Ballots*. Democracy Fest Annual National Convention. June 2007. URL: `http://www.democracyfornewhampshire.com/files/Hand_count_training_D-fest_July_5_2007.pdf`

[66] Rivest, *On Auditing Elections When Precincts Have Different Sizes*, see n. 5; Stanislevic, see n. 5.

Year	Federal Races Requiring 3% Audit	Federal Races Requiring 5% Audit	Federal Races Requiring 10% Audit
2002	461	3	4
2004	510	5	5
2006	451	7	10

Table 4.3: For Federal races between 2002–2006, we calculate how many races would have triggered audits of 3%, 5% and 10% based on the tiered model discussed in the text.

probably not add significantly to the cost of conducting the audits—at least if only applied to federal races. The cost of a tiered audit as proposed in Congressman Holt's bill would be negligibly greater than a flat audit of 3 percent because few races would be subject to a five or ten percent audit. The extra cost of performing some audits in the second and third tier thus contributes about one-thirtieth of the total audit cost.[67] Tiered audits also increase the public's confidence that election results are correctly reported for all races—even close races.

The Confidence Level Algorithm

To more precisely set the confidence level, some have advocated following a mathematical algorithm that would guarantee a fixed level of confidence (e.g., fifty percent, ninety percent, or ninety-five percent) that a full recount of the paper records would not find error or fraud, if present at a level that would change the outcome of the race being audited.[68]

States might require the assistance of statisticians to review the outcome of various races and tell counties how many precincts or machines they need to audit based on the review. To perform this calculation, election officials would need to know not only the unofficial vote totals, but also the number of precincts or machines in which ballots were cast in the race, as well as the variation in the number of ballots cast in those precincts or on those machines.[69] In *Percentage-Based versus Statistical-Power-Based Vote Tabulation Audits*, several statisticians and political scientists provide an in-depth analysis of how this method could be implemented and detail its various advantages.[70]

A potential advantage of this approach over the tiered audit percentage approach is that

[67] This calculation assumes that costs of increased audits increased linearly with audit percentage.
[68] Stanislevic, see n. 5.
[69] The basic mathematics behind this calculation are covered in Hall's primer. See Appendix D or Hall, *A Quick Primer on the Mathematics of Post-Election Audit Confidence*, see n. 60
[70] McCarthy, Stanislevic, Lindeman, et al., see n. 5.

jurisdictions will not have to audit more precincts or machines than is necessary to gain confidence that the electronic results have the correct candidate winning. For races that are not close, setting the audit size based on confidence level will likely reduce the audit size significantly from the effort required under a mandatory fixed-percentage audit of two or three percent.

Model Strengths

In addition to the advantage of greater confidence (albeit with greater effort) in close races, the adjustable-percentage audit model has many of same strengths as the fixed-percentage audit model.

As already discussed, the adjustable-percentage audit model has one major advantage over the fixed-percentage audit model: it will give jurisdictions and the public greater confidence that there was no error, bug, or attack against the voting system that could change the outcome of a close race, and it will do so more efficiently than requiring a fixed-percentage audit of a large number of precincts or machines in *all* races, regardless of the margin of victory between candidates.

Model Weaknesses

We have identified two major weaknesses of the adjustable-percentage audit model, one of which is shared with the fixed-percentage audit model. As discussed above, audits are effective only if election officials act on the discovery of discrepancies between manual count results and the electronic tally, and even with adjustable-percentage audits, a seemingly innocuous discrepancy of just a few votes between paper and electronic records in one or two precincts could, in fact, indicate far more serious problems.

As recommended in the previous section on the fixed-percentage audit model, when discrepancies are found, election officials should conduct additional manual counts of the paper records, investigate the sources of discrepancies, and resolve them. If appropriate, the election officials should order an expanded recount.

Prior to an election, election officials should determine the size of a discrepancy that

warrants further recounts or other action. It may not be clear how much of a discrepancy should trigger such actions. An analysis of states with trigger mechanisms could provide guidelines. For example, in Minnesota, the discrepancy rate was one half of one percent, but no counties were actually required to perform additional audits.[71] Although small discrepancies may be unavoidable, ignoring them may result in ignoring outcome-changing problems. While additional experience with audits will help to inform the expectations of election officials, jurisdictions should devise plans for acting on discrepancies.

The second weakness of this model is that election officials face uncertainty about the audit prior to an election. The number of precincts a jurisdiction must audit is based on a mathematical formula that relies in part on the unofficial electronic results totaled after the polls have closed. As a result, election officials may not know how many precincts or machines they will have to audit until Election Day is over. In some high profile state and federal races, election officials could use pre-election polls to assist them in estimating what level of auditing scrutiny might be necessary when the unofficial results are reported. Of course, for many races and issues on a given ballot, there will be little, if any, recent public polling data to assist election officials in making such estimates.

The percent of precincts or machines to be audited could vary from one hundredth of one percent to a full recount. The tiered audit approach attempts to limit this uncertainty by providing acceptable minimum audit sizes (i.e., three, five, or ten percent of precincts).[72] Given how infrequently federal races are decided by small margins, it will be relatively rare that election officials would be required to conduct the "stepped-up" audits in federal elections.

The tiered approach partially addresses this concern by allowing election officials to plan and budget for audits by providing some certainty about audit levels prior to an election. Such certainty does not exist for other variations of the adjustable-percentage audit model. The public and losing candidates, however, could feel less confident in the results of very close races. For instance, in our model Congressional district, a ten percent audit of a close

[71] Halvorson and Wolff, see n. 57, at 3.

[72] Still, it is worth noting that the Holt Bill allows states to use audits that are "at least as effective" as the scheme proposed in the bill. Thus, a state could probably choose to adopt something close to the adjustable-percentage audit method in its pure form. H.R. 811, 110TH CONG. Sec. 5 (2007). *But see* the main text for reasons that a fixed-percentage minimum audit may be desirable, even if the margin of victory is very large.

race (the maximum audit rate under the Holt proposal) will only have a fifty-eight percent chance of finding an error or fraud that could alter the outcome of a race decided by three-quarters of one percent (and even less of a chance of discovering smaller errors or fraud). In actual Congressional districts with fewer than 400 precincts or where the number of votes cast in precincts varies greatly, the chances of finding such an error would be even smaller.

Finally, if a jurisdiction adopts an adjustable-percentage audit model *without a base percentage or number of audits for all races*, it will likely miss some errors or problems with voting machines that a fixed-percentage audit might catch when there are no close races. Moreover, without such a minimum audit, election officials are less likely to record, review, and make publicly available information about the votes cast in an election that could assist them in improving the performance of their machines and ballot design in the future. Thus we can imagine a situation where a poor ballot design led a significant number of voters to undervote or cancel their votes upon examining the final DRE review screen, or where a significant number of votes were misread as undervotes because some pens supplied at polling places were not read by the optical scanners. These problems might not be substantial enough to change the outcome of a landslide victory; an audit of just one or a few machines in such landslide races might be all that was necessary to ensure that a winning candidate actually won his race, but such a limited audit is unlikely to reveal the kinds of problems that could presage greater problems if not caught and corrected for future, closer elections.

Accordingly, jurisdictions that implement an adjustable-percentage audit model should audit a minimum percentage or number of precincts or machines automatically.

Administrative Considerations

adjustable-percentage audits are more complex than fixed-percentage audits, and because jurisdictions have little experience with the adjustable-percentage audits, there are few well-tested procedures. It may be challenging to explain and train staff of an adjustable-percentage audit, opening opportunities for human errors.

Time and Cost of Audit

The cost of conducting an adjustable-percentage audit depends heavily on which races are being audited and the margins of victory in those races. Obviously, if there are many close races, a larger percentage of precincts and machines would be audited. On the other hand, this audit method promises to handle audit costs efficiently and fairly. Where races are decided by large margins, it will not be necessary to audit many precincts to obtain a high level of confidence that a full recount would not change the election outcome. Only close races would require a large percentage of precincts or machines to be audited. If a state or the federal government has a role in paying for audits, it would be able to distribute the savings in large-margin (i.e., small audit size) jurisdictions to those with small-margin races that must conduct large audits.

The major administrative burden associated with the adjustable-percentage audit model may not be the cost of performing the audits, but the cost of planning for an audit when the number of precincts that might be audited is unknown. The necessity of planning for a large audit might lead jurisdictions to incur expenses for resources (e.g., work space, staffing, etc.) that they ultimately do not use.

The adjustable-percentage audit model also may impose unequal financial burdens on election jurisdictions. A jurisdiction that happens to have a race where the two leading candidates are separated by a narrow margin will incur greater expenses than a jurisdiction in which the margin for the same race is relatively wide. Therefore, from a system-wide perspective, it might be necessary to distribute funds on the state or national level to adequately fund jurisdictions that have close races.

Other Factors

As discussed in the fixed-percentage audit model section, the voter-verifiable paper records produced by printer attachments to current DRE voting machine models present unique challenges for jurisdictions that use them. Paper records spoiled by paper jams and printer malfunctions could effectively mask discrepancies. For an adjustable-percentage audit, this would lead to an underestimate of the audit size. More generally, spoiled voter-verifiable paper records could drown out the effect of more subtle voting system errors, frustrating the goal of collecting data about voting machine performance during audits.

Recommendations to Improve the Model

We encourage jurisdictions considering this model to adopt the general recommendations (Sections 4.1.4 & 4.3) and recommendations to improve the fixed-percentage audit model (Section 4.2.1) made in this paper. In addition, we recommend and/or reiterate the following to jurisdictions that adopt an adjustable-percentage audit model:

- **Audit a Minimum Percentage or Number of Precincts or Machines for Each Election, Including At Least One Machine Model and/or Precinct in Each County.** One of the chief benefits of the adjustable-percentage audit model is that it allows jurisdictions to reach a relatively high level of confidence that a full recount would not change the outcome of an election in a very efficient manner (i.e., by auditing just enough precincts, machines or other units to ensure that the desired level of confidence is reached). Jurisdictions employing this model might be tempted to audit only one or very few precincts or machines in elections decided by large margins, but doing so would sacrifice several important post-election audit goals related to improving future performance (and, relatedly, the ability to fix problems that could have a greater impact on election outcomes in close races in the future). This includes detecting significant errors that would not change the result of an election, errors that only affect a particular machine model or ballot-type, and errors that might shed light on how voters interact with certain ballot designs. Accordingly, we recommend that jurisdictions employing this method also audit a minimum percentage or number of precincts or machines, including at least one machine model and/or precinct in each county.

- **Account for Precinct Size Variability in Audit Selection and Sample Size Calculations.** Methods to deal with precinct size variability can be as simple as sorting precincts into bins of certain sizes ("small," "medium," and "large"), conducting random selection within each bin or listing precincts in order of size, and ensuring that auditors select a certain number of large precincts. Any analysis, legislation, or administrative procedures that do not take into account the varying number of votes in different precincts are likely to over-estimate the statistical power of uncovering irregularities that could change the outcome of an election.

4.2.3 The Polling Audit Model

In contrast to the fixed-percentage and adjustable-percentage audit models, where all of the paper records for a given number of precincts or machines are manually counted in their entirety, there is another class of post-election auditing proposals that we refer to as instances of a "polling" model.[73]

Under this model, a randomly chosen, small sample of ballots is recounted in *every* precinct and the total of these samples is compared to the unofficial electronic results. We are not aware of any jurisdictions that have adopted this approach, though some election integrity advocates have developed arguments for this audit method.[74]

Model Implementation

In practice, election officials would conduct a polling audit on election night after the polls close or on the following day. Audit teams would randomly select a small percentage of all paper records in each precinct. The auditors in each precinct would manually count the votes in each race for these sampled records, and a jurisdiction- or state-level official would then total the precinct-level results together. According to the statistical model on which this proposal relies, the hand-counted sample should provide a highly accurate and precise projection of the full electronic tally of the votes (unless that count is errant has been corrupted). The proportion of votes for each candidate in each race of the sampled ballots should very nearly match the proportion of votes for each candidate in the full electronic tally. More specifically, Jonathan D. Simon and Bruce O'Dell, the authors of this proposal, argue that a tally based on a random sample of ten percent of ballots would be within one percent of the full electronic tally ninety-nine percent of the time. In their view, a deviation in the sample count of more than one percent would indicate that the full electronic tally was inaccurate.

The polling audit model presents a few logistical considerations that are quite different from the fixed-percentage and adjustable-percentage audit methods discussed above. First, because a polling audit examines individual paper records rather than voting machines or

[73] Simon and O'Dell, see n. 5.
[74] Simon and O'Dell, see n. 5.

precincts, auditors will likely need to select far more records under this model.

Second, all paper records must have an equal chance of being selected for the recount. Auditors must select the paper records at random, otherwise, the sample of paper records could be biased. For example, selecting the first ten percent of paper records cast could lead to a sample of paper records from voters whose decision to vote early in the day is correlated with certain political preferences. A projection of the full vote tally based on this sample would reflect this bias and accordingly might fall outside the margin of error and call the official results into question. In other words, a failure to draw a random sample of paper records could lead to a falsely positive identification of a significant discrepancy between the paper records and the full electronic tally. As was the case with the fixed-percentage and adjustable-percentage audit methods, the polling audit must include all ballot types. Excluding certain kinds of ballots (e.g., absentee ballots, provisional ballots) would bias the audit sample and leave open several opportunities to attack or hide error in the official count.

Third, a jurisdiction must develop a means to identify and retrieve the paper records that the auditors randomly select. A conceptually simple method for achieving this end is to mark each paper record with a unique number, and to randomly select paper records from that set of numbers. For paper ballots, such as those read by optical scanners, this process is likely to be straightforward, since the marking process basically amounts to stamping consecutive sheets of paper with sequential numbers.[75] For DREs, which typically use continuous paper rolls for voter-verifiable paper records, the marking and retrieval process could be extremely cumbersome.[76] To mark individual ballot records on these paper rolls would require scrolling through the entire roll, identifying the boundaries of each record, and stamping a number on the record. In any event, this step must occur *after* ballots are cast in order to avoid compromising ballot secrecy.

[75] A slightly more complex method—but one that obviates stamping each ballot—is to stack the ballots in a systematic fashion. For example, the ballots could be separated into 100-ballot piles. For each pile, poll workers would place the first ten ballots in "portrait" orientation. The next ten would be in "landscape" orientation (rotated by 90 degrees). By repeating this pattern for the rest of the 100-ballot pile, poll workers would create a pile in which it is easy to identify any ballot with a number between 1 and 100. Additional 100-ballot piles would contain ballots 101–200, 201–300, etc. It is unclear whether this method would save time compared to the sequential labeling method discussed in the main text.

[76] Simon and O'Dell suggest that the easiest way around this difficulty is simply to replace DREs with other voting systems. Simon and O'Dell, see n. 5, at 5-6.

The second and third requirements are in some tension with a fourth consideration: a polling audit should occur as soon as possible following an election. The polling audit model is principally intended to address the threat of intentional tampering with centralized ballot-counting equipment in order to produce a desired outcome.[77] To avoid detection, attackers would need to rig the sampling of paper records or corrupt the manual count results of the sampled paper records in order to bring it within the desired margin of error of the full official count. Using publicly verifiable random selection processes and conducting an audit in public work to mitigate this kind of threat. In addition, authors of the polling audit proposal suggest conducting the audits in precincts rather than at a central location.[78] According to the proposal's authors, such a widely distributed audit would require attackers to rely on a larger number of co-conspirators, making it more difficult to maintain the secrecy of an attack and successfully complete it. Finally, the effects of conducting a widely distributed audit on the accuracy of the manual count are unclear; comparing the error rate for this audit design to a centrally conducted audit is an area that may warrant further research.

Model Strengths

We have identified two major benefits of the polling audit model. First, it promises to allow jurisdictions to confirm that the correct candidate has been declared the unofficial winner with a great degree of certainty without requiring jurisdictions to staff an entire manual count event. This is true in close races as well as landslides.

Second, unlike the fixed-percentage and adjustable-percentage audit models discussed above, the polling audit model would greatly reduce the need to decide whether a discrepancy is large enough to justify additional action. The hand count will or will not produce a result within one percent of the full electronic tally. If it does, Simon and O'Dell argue, we can be ninety-nine percent confident that the electronic tally was correct. On the other hand, if the hand count results are not within one percent of the full electronic results, a full recount or investigation would be necessary. There is little room in this scenario for election official discretion, as there is under the fixed-percentage and adjustable-percentage

[77] Simon and O'Dell do not address precinct-level tabulation.
[78] Simon and O'Dell, see n. 5, at 7.

audit models.

Model Weaknesses

The polling audit model will not necessarily help jurisdictions discover specific errors or fraud. Only when such errors are large and consistent enough to significantly change the number of votes received by each candidate will a polling audit alert jurisdictions of such problems.

Similarly, when auditors do find discrepancies, this audit will provide little information about the source of a discrepancy, since the audit is detached from specific precincts and specific machines, and even particular ballot types. This is especially notable for a number of audit goals that use auditing as a feedback mechanism to reform voting systems, procedures, or personnel conduct.

Finally, a consequence of the statistical model underlying the polling audit approach is that it will probably produce some "false positives." The model contemplates that, one percent of the time, the hand count of sample paper records and full electronic count will be significantly different, despite the fact that there was no error or fraud. In such cases (in particular, where a false positive indicates that the wrong candidate won in the unofficial results), jurisdictions may be forced to conduct a full recount, only to find that the paper and electronic records match exactly.

Administrative Considerations

Time and Cost of Audit

It is difficult to compare the costs of polling audits to the costs of fixed-percentage audits. While fixed-percentage audit costs increase roughly in proportion to the audit percentage, it is not clear how costs vary in the polling audit model. On one hand, the statistical model underlying the polling audit holds that, while the number of ballots that must be sampled varies somewhat with the number of ballots cast in an election (holding other things equal, particularly the confidence level), this variation is minimal.[79] On the other hand, the fact that these audits must be conducted in disparate locations may introduce costs that

[79] Simon and O'Dell, see n. 5, at 3.

vary substantially among jurisdictions. Additionally, these audits might be conducted by teams of poll workers fatigued from working at a polling place for several hours. A more realistic staffing scenario would involve hiring additional poll workers or a specialized force of auditors in order to avoid over-burdening polling place staff.

Requiring the audit to occur as soon as possible after an election is itself a potential source of administrative burden. Election officials have many responsibilities unrelated to auditing after an election, and audits that require their immediate attention and oversight might distract them from their other duties.

Another ill-defined cost in polling audits is that of not knowing where error or fraud may lie. If a polling audit indicates that there is a discrepancy, it yields little information about what the source might be. Election officials would only know that the hand count result of sampled paper records is out of the agreed-upon error bounds. In contrast to the fixed-percentage audit model, there is no helpful precinct-level or ballot-type-specific information that could be helpful in any subsequent investigation. polling audits are not useful in deterring attacks on voting systems. In the worst case, the discrepancy would be detected, but not the source. The only recourse election officials have to uncover the source of discrepancies is to conduct a precinct-specific or full fixed-percentage audit.

Recommendations to Improve the Model

- **Develop and Test Paper Record Selection Procedures Well Before an Election.** Random selection of paper records is critical to the validity of a polling audit. We recommend the ten-sided dice procedure proposed by Cordero, Wagner and Dill, which is easily adapted to this application.[80] Rapid completion of the audit is equally important, as discussed above. Therefore, a jurisdiction that implements a polling audit model should have developed and tested procedures for randomly selecting paper records before the audit occurs—the audit logistics are too complicated, and time is too short, to allow for experimentation after an election.

[80] Note: for large precincts, this might require upwards of 100 rolls of the dice (assuming a ten percent audit in a precinct with 1,000 ballots cast). A reasonable modification would be to roll two ten-sided dice 1/10 as many times and select each corresponding 10-ballot stack from each larger stack (*e.g.*, a roll of a "9" and a "2" would select ballots 921–930). See: Cordero, Wagner, and Dill, see n. 5

- **Develop a Plan for Elections Not Confirmed by Polling Audit.** As discussed above, a polling audit will provide few clues about whether an unofficial count that differs significantly from the audit count is simply a false positive or whether it is the result of error or fraud. Finding a way to distinguish these two situations might be an area for further research. In addition, if election officials conclude that error or fraud caused the difference, they must have a plan in place to investigate more thoroughly the cause(s). A means for examining ballots and voting equipment to determine whether a certain kind of voting system or ballot type might account for a discrepant result is important.

4.3 Audit Best Practices

Our review of the audit procedures and other security measures currently in place in most states has led us to conclude that there is a substantial likelihood that such procedures would not detect a cleverly designed software-based attack program. Currently, only eighteen states that require voter-verifiable paper records also mandate regular audits of those paper records.[81] Moreover, even those states that have mandated regular audits have not developed the best practices and protocols that are necessary to ensure their effectiveness in discovering attacks or failures in the voting systems, or in using audits to improve elections in the future. Below we discuss best practices for conducting audits, regardless of what audit model a jurisdiction has chosen, as well as the reasons for instituting such practices:

4.3.1 Practices for Selecting Votes To Be Audited

The method and manner employed by a jurisdiction for choosing votes to audit will have a tremendous impact on whether the audit itself is administratively burdensome, engenders public confidence in election results, detects errors, and provides feedback that will allow jurisdictions to improve elections in the future.

[81] Kibrick, see n. 2.

Use Transparent and Random Selection Processes for All Auditing Procedures.

Audits are more likely to prevent fraud and produce greater voter confidence in election results if the public can verify that the paper records, machines or precincts to be audited are chosen in a truly random manner. As noted in *electionline.org*'s March 2007 briefing, *Case Study: Auditing the Vote,* there is "broad agreement among academics, policymakers, computer scientists and advocates" on this point.[82]

The danger of non-transparent and non-random audits is exemplified by a corrupted recount in Cuyahoga County, Ohio, which took place following accusations of problems in the 2004 general election. The state mandated a hand count of ballots cast in three percent of the county's precincts and a full recount if the three percent audit revealed discrepancies between the punch-card and electronic records. "Seeking to avoid a vast hand-count of thousands of punch-card ballots, election workers broke state law by pre-sorting the ballots to ensure they matched the final tally."[83] In other words, the audit was rigged to ensure that no problems were revealed.

To avoid repeating the problems of Cuyahoga County's 2004 audit, the selection of precincts or machines to be audited must be observable by the public and conducted in a truly random manner. In addition, specific guidelines are needed to ensure that observers will be able to actually see each vote counted.

In an ideal transparent and random selection process:

- The whole process is publicly observable and ideally videotaped and archived.
- The random selection is publicly verifiable, *i.e.*, anyone observing is able to verify that the sample was chosen randomly.
- The process is simple and practical within the context of current election practices so as to avoid imposing an unnecessary burden on election officials.[84]

There is today a significant body of literature that addresses ways in which election officials can accomplish these goals. Researchers Arel Cordero, David Wagner and David Dill

[82]Electionline Audit Briefing, see n. 17, at 5.
[83]Electionline Audit Briefing, see n. 17.
[84]Norden and Lazarus, see n. 4.

explained how dice could be used to select precincts randomly in *The Role of Dice in Election Audits*.[85] In the *Machinery of Democracy,* the Brennan Center Task Force on Voting System Security offered its own suggestions for the random selection of precincts or machines to be audited. These methods are preferable to using a pseudo-random generator on a computer, which is rarely a transparent method for selecting precincts or machines, particularly to observers who do not understand technology.[86] Moreover, as some commentators have noted, because of their opacity, such generators are themselves vulnerable to fraud.[87]

The randomness and transparency of audit selection processes vary in the states that currently conduct audits. In Arizona and Minnesota, precincts and races to be audited are selected by lot (at the county seat in Minnesota).[88] Other states, such as Colorado, New Mexico, Washington, and West Virginia, require jurisdictions to select precincts to audit randomly, but the relevant laws and regulations fail to define "randomness" or describe the selection processes.[89] In New York, Parties entitled to appoint poll watchers within the jurisdiction are also entitled to appoint representatives to observe the selection of machines for an audit and the audit itself.[90] In Connecticut, the Secretary of State determines and announces the procedures for randomly selecting DREs to audit, and the selection of machines and the conduct of the audit may be observed by the public.[91] Similarly, in Illinois, the State Board of Elections is charged with designing "a standard and scientific random method" to select five percent of precincts in each jurisdiction to audit "so that every precinct in the election jurisdiction has an equal mathematical chance of being selected."[92] California provides public notice of the time and place of the selection of precincts to be audited and of the audit itself at least five days before either event is scheduled to occur[93] and suggests that election officials use "a random number generator or other methods specified in regu-

[85] Cordero, Wagner, and Dill, see n. 5.

[86] But compare with: Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. "In Defense of Pseudo-random Sample Selection". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008).

[87] Cordero, Wagner, and Dill, see n. 5; Norden and Lazarus, see n. 4.

[88] ARIZ. REV. STAT. ANN. Sec. 16-602(C) (2007); 2007 ARIZ. LEGIS. SERV. 295 (West) (pending legislation to update audit requirement); MINN. STAT. ANN. Sec. 206.89 (West 2007).

[89] COLO. REV. STAT. ANN. Sec. 1-7-514(1)(a)(I) (West 2007); N.M. STAT. ANN. Sec. 1-14-13.1(A) (West 2007); WASH. REV. CODE ANN. Sec. 29A.60.185 (West 2007); W.VA. CODE ANN. Sec. 3-4A-28(d) (West 2007).

[90] N.Y. ELEC. LAW Sec. 9-211(1) (McKinney 2007).

[91] CONN. GEN. STAT. ANN. Sec. 9-242b(5) (West 2007).

[92] 10 ILL. COMP. STAT. ANN. Note: this scheme doesn't allow one to weight precincts based on size to account for precinct size variation. Sec. 5/24C-15 (West 2007).

[93] CAL. ELEC. CODE Sec. 15360(d) (West 2007).

lations" to select precincts to audit.[94] In Alaska and Washington, appointed representatives of political parties are permitted to observe an audit, but the opportunity to observe the audit does not extend to members of the general public.[95] Post-election audits in Colorado and in Minnesota are publicly observable.[96]

The time period between the selection of precincts or machines to be audited and the actual audit is security-sensitive. An attacker with the goal of corrupting vote counts could target only those that were not chosen for the audit. Arizona requires jurisdictions to begin post-election audits within the twenty-four hours after the closing of polls.[97] New Mexico conducts a post-election audit within five days of county canvasses.[98] Election officials should minimize this period of time and enforce strict chain-of-custody requirements over election materials used in an audit.

Audit a Minimum Percentage or Number of Precincts or Machines for Each Election, Including At Least One Machine Model and/or Precinct in Each County.

Much of the recent academic literature on post-election audits focuses on catching error or fraud that could change the outcome of an election. But finding an error that has changed the outcome of an election is in many ways a worst case scenario; most would agree that if we are going to find such problems, it would be far better to find (and correct) them in landslide elections where they could have no effect on the outcome of an election. Put another way, in most races, a software bug, attack on vote tallies, or other problem that affected just two percent of the votes would not alter the outcome of an election. Nevertheless most election officials and voters would prefer to find such problems and correct them *before* an audit of an exceptionally close election, rare as they may be. An audit that targets a fixed percentage (e.g., three percent) or minimum number of precincts or machines in each race will assist jurisdictions in detecting widely distributed error or fraud, regardless of whether such error or fraud was substantial enough to change the outcome of the particular election being audited.

[94] CAL. ELEC. CODE Sec. 15360(c) (West 2007).
[95] ALASKA STAT. Sec. 15.15.420 (2006); WASH. REV. CODE ANN. Sec. 29A.60.185 (West 2007).
[96] COLO. REV. STAT. ANN. Sec. 1-7-514(1)(a)(I) (West 2007); MINN. STAT. ANN. Sec. 206.89 (West 2007).
[97] ARIZ. REV. STAT. ANN. Sec. 16-602(J) (2007).
[98] N.M. STAT. ANN. Sec. 1-14-13.1(A) (West 2007).

Additionally, the inclusion of at least one machine model and/or precinct in each county in an audit should help jurisdictions find discrepancies caused by fraud or error limited to a particular machine or ballot definition file; ballot designs that caused voters to make mistakes; or other problems that might not have been wide-spread enough to change the outcome of a race in the election being audited, but could have such a dramatic affect in future, closer elections.

Consider Auditing by Machine Rather Than by Precinct.

In many states, it will be more efficient to audit by machine or ballot batches, rather than by precinct. Particularly in states that use touch-screen voting machines, jurisdictions will be able to achieve the same level of confidence in their results by auditing a smaller percentage of machines. Auditing is fundamentally a numbers game: the more distinct the sample of individual units audited, the higher the associated confidence can be and the more efficient the audit.

Freeze and Publish Unofficial Results Before Selecting the Precincts or Machines To Be Audited.

Election officials should freeze and publish unofficial election results once all returns are received from jurisdictions. The random selection of precincts or machines to be audited should only occur afterwards. Published results should be broken down by precinct or other audit unit (such as voting machine), and further separated into the ballot types that are audited (e.g., if absentees are audited separately from polling place votes, then results should list absentees separately from polling place tallies). If the random drawing is conducted too soon after the close of polls, election workers processing ballots will know in advance which ones will be part of the audit and which will not. For instance, they might be extra-careful when processing ballots from the precincts they know will be audited. Someone intent on committing fraud will be free to do so, knowing that as long as she doesn't touch the ballots that are part of the sample, the audit will have no chance of catching them. Additionally, without the publication of the unofficial results, audit observers cannot verify for them-

selves that the votes were accurately counted. As a result, election officials supervising the audit may be convinced or assured by its findings, but observers would not necessarily feel similarly confident about the audit.

4.3.2 Practices for Conducting the Audit

There are specific steps that every jurisdiction can take to make it far more likely that the audit as a whole is accurate, useful to election officials, and likely to catch errors that could change the outcome of specific races.

Don't Just Match—Count! (Record and Publicly Release Meaningful Data on Votes Cast).

Audits that record and detail the number of overvotes, undervotes, blank ballots, spoiled ballots, and, in the case of DREs, paper record cancellations, could be extremely helpful in revealing software attacks and software bugs and in identifying problems in ballot design and ballot instructions.

Most discussions about post-election audits focus on ensuring that the paper and electronic totals of the sampled precincts or machines match. However, a match between paper and electronic records may not reveal the presence of some kinds of problems. These problems may include some types of outcome-changing software bugs, fraud against a voting system, bad ballot design, or machine miscalibration that may have resulted in the disenfranchisement of voters.

Jurisdictions may gain significant information about the performance of their voting machines and ballot design by reviewing and detailing the number of overvotes, undervotes, blank votes, spoiled ballots, and, in the case of DREs, cancellations. This is information that would allow jurisdictions to improve future elections. This type of election data should be tabulated and published, broken down by precinct or machine, and by ballot type (e.g., polling place, absentee, or provisional), if possible. If data on these types of votes deviate from normal values, or are distributed in an uneven manner, a jurisdiction can take action to correct these problems. For example, an anomalously high number of overvotes in a polling place could indicate that it lacks the appropriate feedback to alert voters to

how election tabulation equipment is interpreting their ballots. Similarly, an unusually high number of undervotes could point to screen miscalibrations, poor ballot design, poor ballot instructions or other problems.

There are several ways in which such a review would be helpful. First, in the case of DREs, a review of cancellations could show that there were problems with *both* the voter-verifiable paper record and the machine. At least one study has shown that the vast majority of voters do not thoroughly check their voter-verifiable paper records.[99] If a voter does not check her paper record, the paper record does not provide extra security for that voter. A vote could be misrecorded on both the paper and electronic record, and both the voter and election officials would not realize votes were incorrectly recorded.

However, if even a small percentage of voters (e.g., twenty percent) check their paper records thoroughly, the identification of an unusual number of cancellations on the paper trail would provide evidence that there was some problem with the mechanism that captures voters' selections on the paper record.[100]

During the 2000 elections in Lake County, Florida, 376 voters' selections for Presidential candidate were disqualified because approximately two-thirds of them displayed a selection of "Gore" from the listed candidates as well as "Gore" in the write-in line.[101] Studies have shown that some voting populations have high rates of overvotes and undervotes on certain types of voting machines. Low-income and minority voters are especially susceptible to this kind of mistake.[102] Now, voters using precinct count optical scan voting machines benefit from those systems' protections against over- and undervotes. If a voter skips a race or

[99] Sarah P. Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. Rice University PhD Thesis. May 2007. URL: http://chil.rice.edu/alumni/petersos/EverettDissertation.pdf.

[100] Norden and Lazarus, see n. 4, at 70. If twenty percent of voters thoroughly check their paper records and notice errors on them, there would be an unusually high number of cancellations.

[101] See *e.g.*, David Damron and Gwyneth K. Shaw. "Probe Shows Florida County Erred by Tossing Write-ins". In: *Orlando Sentinel* (2001). URL: http://www.courant.com/news/nationworld/sns-ballots-lakecounty-os,0,7595823.story; Scott Shuger. "Air Apparent?". In: *Slate* (Dec. 2000). URL: http://www.slate.com/id/1006723/ (reporting that the *Orlando Sentinel*'s examination of 6,000 disallowed Lake County ballots found 376 overvotes, which, if counted, would have given Gore a net 130-vote increase in that county).

[102] Lawrence Norden. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*. Brennan Center for Justice at NYU School of Law. Oct. 2006. URL: http://www.brennancenter.org/content/resource/the_machinery_of_democracy_voting_system_security_accessibility_usability_a; Michael Tomz and Robert P. Van Houweling. "How Does Voting Equipment Affect the Racial Gap in Voided Ballots?". In: *American Journal of Political Science* 47 (2003). 46–60. URL: http://www.stanford.edu/~tomz/pubs/ajps03.pdf.

selects two candidates in a race, the machine informs the voter of the error and allows her to correct her ballot so that her intention will be accurately recorded.

A software attack that shut off this protection (or a software "bug" that accidentally shut it off) could disproportionately affect certain communities of voters. In *The Machinery of Democracy,* the Brennan Center demonstrated that a state-wide shutdown of this protection could result in the loss of tens of thousands of votes, mostly in low-income and minority communities. A review of the number of over- and undervotes in an audit would provide evidence that something went wrong with this protection and allow election officials to address it.[103]

High overvote and undervote rates may also indicate that ballots were badly designed and caused voter confusion. By recording these data in audits, election officials and the public can gain insight into the effectiveness and usability of various ballot designs.

For precinct count optical scans, auditing of overvote and undervotes can provide election officials with critical information about why some voters' votes aren't recorded. For instance, in Minnesota, a post-election audit report drafted by an election integrity group revealed that the vast majority of discrepancies between hand counts of the paper ballots and the electronic tallies occurred because "the voter used an odd-colored pen, or pressed too lightly with a pencil, in which case the vote was misread as an undervote" or "the ballot got jammed in the optical scanner."[104] Some votes were recorded as undervotes because voters "circled an oval as opposed to filling it in as directed."

Having this kind of information should be extremely useful to election officials. For instance, the Minnesota examples discussed above could help election officials determine: what kind of voter education to focus on to ensure accurate recording of voter intent is maximized; how to improve procedures to ensure that voters are using the right kind of pens; and whether there is some problem with the size or thickness of ballots that might produce an unusually high number of paper jams.

We are aware of only two states, North Carolina and California, that have collected and made this type of information publicly available, in the hope that it could improve future

[103]Norden and Lazarus, see n. 4, at 81.
[104]Halvorson and Wolff, see n. 57, at 5.

audits, elections and machines. In reports to the North Carolina State Board of Election on the May 2006 and November 2006 elections, the University of North Carolina at Chapel Hill, School of Public Health included data that detailed the level of discrepancy between electronic tallies and recounts on each type of machine used, and measured the accuracy of voting machines by reviewing their relative under and overvote counts.[105] For the February 2008 Presidential Primary, the California Secretary of State published post-election audit reports, including discrepancy and other information.[106]

Audit All Methods of Voting.

In conducting post-election audits, election officials should not exclude any category of votes (e.g., absentee ballots, provisional ballots, damaged ballots). Audits must be comprehensive to ensure that both error and fraud can be readily detected. Although voters cast the majority of ballots on polling place equipment, many jurisdictions increasingly see significant numbers of other ballot types, including early, absentee, provisional and emergency ballots. Fifteen states allow "no-excuse" early voting.[107] In 2004, more than forty percent of all votes cast in Arizona, Nevada, Tennessee, and Texas were received during early voting periods.[108] Voters in twenty-eight states take advantage of "no-excuse" absentee voting by mail. Oregon conducts all elections with mail-in ballots.[109] All but four states have provisional balloting at polling places.[110] The exclusion of any of these ballot types compromises the effectiveness of a post-election audit. To be comprehensive, all ballot types should be included in audit processes. Ballot types should be sorted and stored by precinct, machine, or other unit and randomly selected for auditing.

While the majority of state laws are silent on the inclusion or exclusion of other vote

[105] William D. Kalsbeek and Lei Zhang. *An Assessment of the May 2006 Election Recount and a Proposed Permanent Recount Sample Design*. University of North Carolina at Chapel Hill, School of Public Health's Survey Research Unit. July 2006. URL: http://www.ncvoter.net/downloads/Kalsbeek_May2006_Recount_Assessment.pdf; William D. Kalsbeek and Lei Zhang. *An Assessment of the November 2006 Election Recount*. University of North Carolina at Chapel Hill, School of Public Health's Survey Research Unit. May 2007.

[106] See n. 46.

[107] *Early and Absentee Voting Laws*. Electionline.org. July 2006. URL: http://www.pewcenteronthestates.org/uploadedFiles/e%20and%20a%20voting%20laws.pdf.

[108] EDS 2004 Election Day Survey Report, see n. 13.

[109] Electionline's Early and Absentee Voting Laws, see n. 107.

[110] *Provisional Ballot Verification*. Aug. 2006. URL: http://www.pewcenteronthestates.org/uploadedFiles/ballot%20verification.pdf.

records in a post-election audit, several Western states—where a particularly large number of votes are cast outside the polling place and/or prior to election dates—are not. Specifically, California and New Mexico include absentee ballots cast on electronic voting machines in their audits.[111] In addition to its audit of polling place ballots, Arizona reviews the lesser of one percent of the total number of early ballots, or 5,000 early ballots, randomly selected at the county level from sequestered batches of early ballots from each machine used to tabulate them. Provisional, conditional provisional and write-in votes, however, are excluded from the audit.[112]

4.3.3 Practices for Ensuring Audit Effectiveness

If the audit is to be effective, there are certain basic policies and practices that jurisdictions should have in place. Among the most important are the following:

Ensure the Physical Security of Audit Materials.

Effective auditing of voter-verifiable paper records will serve to deter attacks on voting systems and identify problems only if states have implemented solid procedures to ensure the physical security of election materials used in a post-election audit, such as records of the vote, voting machines, and tally servers. Sound security measures should include a clear chain-of-custody of these materials. Missing or damaged paper or electronic records will make the reconciliation of audits all but impossible.

In *The Machinery of Democracy*, the Brennan Center examined some of the best chain-of-custody practices in jurisdictions across the country. Among the practices cited approvingly in the report were:

- Between elections, voting systems for each county are locked in a single room, in a county warehouse.
- The warehouse has perimeter alarms, secure locks, video surveillance and regular visits by security guards.

[111] CAL. ELEC. CODE Sec. 15360(b) (West 2007); N.M. STAT. ANN. Sec. 1-14-13.1(A) (West 2007).
[112] ARIZ. REV. STAT. ANN. Sec. 16-602(C) (2007).

- Access to the warehouse is controlled by sign-in procedures, possibly with card keys or similar automatic logging of entry and exit for regular staff.

- Some forms of tamper-evident seals are placed on machines before and after each election. Election officials should place seals over all sensitive areas including vote data media compartments, communication ports and the seams of the voting system case.

- At the close of polls on Election Day, all audit information (i.e., event logs, voter-verifiable paper records, paper ballots, machine printouts of vote totals) that is not electronically transmitted as part of the unofficial upload to the central election office is hand-delivered in official, sealed information packets or boxes. All seals are numbered and tamper-evident.

- The transportation of information packets is completed by two election officials representing opposing parties who have been instructed to remain in joint custody of the information packets or boxes from the moment it leaves the precinct to the moment it arrives at the county election center.

- Once the sealed information packets or boxes have reached the county election center, they are logged. Numbers on the seals are checked to ensure that they have not been replaced. Any broken or replaced seals are logged and the reason for broken or replaced seals is investigated, where necessary. Intact seals are left intact.

- After the packets or boxes have been logged, they are provided with physical security precautions at least as great as those listed for voting machines, above. They should be stored in a room with perimeter alarms, secure locks, video surveillance and regular visits by security guards and county police officers; and access to the room is controlled by sign-in, possibly with card keys or similar automatic logging of entry and exit for regular staff.

All jurisdictions should detail their chain-of-custody practices for their voting system software, hardware, and audit records (including paper and electronic), in a document that

is subject to public review and comment. Public review and comment would increase transparency and accountability for the physical security of audit materials, as members of the public would become invested in the process. The documentation of chain-of-custody requirements allows observers to determine when officials deviate from agreed procedures. Such a document should explain why these procedures are necessary; this would reduce the likelihood of local deviation from the guidelines and ensure that necessary deviations (in the case of an unforeseen incident) held to the spirit of the procedures.

States practices to ensure the physical security of election materials used in an audit vary greatly. In Arizona, election officials at the county level maintain custody of ballots and are responsible for their security during post-election audits.[113] County officials in New Mexico are similarly charged with the secure transport and storage of voting machines after an election.[114] California requires precinct boards to seal and sign containers and packages of ballots and other election materials in the presence of members of the public.[115] At least two members of each precinct board then deliver the sealed containers and packages to election officials at central counting centers.[116] Colorado and Hawaii specify that voted ballots may be handled only in the presence of representatives of different political parties.[117] In Colorado, the receiving election official is required to provide personnel and facilities to preserve and secure election materials.[118] Connecticut requires the collection and storage of voting machines as soon as possible after the completion of an election.[119] Minnesota law requires county auditors to securely store sealed envelopes of voted ballots after an election.[120] In Washington, teams composed of representatives of at least two major political parties pick up sealed containers of voted, untallied ballots from polling places to deliver to the counting center.[121] If ballots are tabulated at the polling place, and if the tallied ballots are sealed in a container, only one elections employee is required to transport them to the

[113] ARIZ. REV. STAT. ANN. Sec. 16-602(I) (2007).
[114] N.M. STAT. ANN. Sec. 1-13-22 (West 2007).
[115] CAL. ELEC. CODE Sec. 15201 (West 2007).
[116] CAL. ELEC. CODE Sec. 14434 (West 2007).
[117] COLO. REV. STAT. ANN. Sec. 1-7-505(2) (West 2007); HAW. REV. STAT. Sec. 11-154 (2006).
[118] COLO. REV. STAT. ANN. Sec. 1-7-507(7) (West 2007).
[119] CONN. GEN. STAT. ANN. Sec. 9-266 (West 2007).
[120] MINN. STAT. ANN. Sec. 204C.28 (West 2007).
[121] WASH. REV. CODE ANN. Sec. 29A.44.050 (West 2007).

elections department.[122]

Implement Effective Procedures for Addressing Evidence of Fraud or Error.

If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for addressing audit discrepancies when they are found. Without protocols for responding to discrepancies, the detection of fraud will not prevent attacks from succeeding. Recommended responses include investigating causes of discrepancies, making corrections where necessary, disallowing results if an appropriate remedy cannot be determined, and ensuring accountability for discrepancies (by for instance, banning the voting system in question from further use until the discrepancy has been explained and/or the system is recertified). Jurisdictions should create discrepancy logs that will be made public, and include the results of any investigations undertaken after discrepancies between paper and electronic records were discovered.

Audit the Entire Voting System, Not Just the Machines.

Although this study focuses only on post-election audits of voter-verifiable paper records, jurisdictions should conduct audits of the entire voting system to catch errors or fraud in other parts of the voting system. Historically, incorrect vote totals often result from aggregation mistakes at central vote tally locations.[123] Accordingly, good audit protocols will mandate that the entire system—from early and absentee ballots to aggregation at the tally server—be audited for accuracy. Among other procedures, we recommend the following:

- **Ensure That Polling Places Compare Vote Tallies and Sign-in Sheets.** At close of the polls, vote tallies for each machine should be totaled and compared with number of persons that have signed the poll books. A comparison of these numbers should be made publicly available.

- **Ensure Individual Voting Machine and Precinct Totals Are Accurately Reflected in**

[122] WASH. REV. CODE ANN. Sec. 29A.60.110 (West 2007).
[123] Anna M. Tinsely and Anthony Spangler. "Vote Spike Blamed on Program Snafu". In: *Fort Worth Star-Telegram* (Mar. 2006) (noting that a programming error in the tally server software caused an extra 100,000 votes to be initially recorded in Tarrant County, Texas).

Tally Server Calculations. A copy of totals for each machine should be posted at each polling place on election night and taken home by poll workers to check against what is posted publicly at election headquarters, on the web, in the papers, or elsewhere. This countermeasure allows poll workers and the public to ensure that corrupt or flawed software on a county's central tally server does not incorrectly add up machine vote totals.

Although the adoption of these recommended audit principles may create new financial and administrative considerations for election officials—particularly in states that currently do not conduct any post-election audits—they are necessary costs to ensuring the integrity of election results. The procedures in the few states that currently conduct post-election audits would be substantially improved by the adoption of all of these recommendations.

4.4 Directions for the Future

The interest of academics and election integrity experts in post-election audits shows no sign of abating. We offer a few suggestions for further study and approaches that, we hope, will add to this research agenda.

4.4.1 Work with Election Officials

Our interviews with election officials have left us convinced that many are eager to use the information developed by academics and election integrity experts to improve their post-election audits. Many ideas discussed in the papers we have reviewed may not be realistic in the context of actual elections, given the financial, logistical and political restraints that election officials face. Ultimately, the best way to develop ideas that can help election officials improve their post-election audits is to work with them, observing the actual conditions under which elections are held. (*E.g.*, see the next chapter.)

4.4.2 New Audit Methods

Auditing by Ballot

The statistics associated with auditing prove that auditors can gain higher confidence in their audit results with a larger audit sample. While this report discusses precinct-level, full recount audit methods as well as machine-level methods, the highest amount of statistical confidence available in our elections would be an audit of individual ballots. If auditors could randomly select a sample of ballots and associate those ballots unequivocally with their corresponding electronic records, auditors would need to examine a smaller amount of ballots in total to reach a similar level of confidence compared to precinct-level or machine-level audits. There are a number of open questions with this style of model. The mapping between paper records and electronic records could compromise ballot secrecy and might be illegal in some states. Also, retrieving individual paper records could be a labor-intensive activity.

History-Dependent Audit Models

Some statisticians advocate using historical information to inform audits. For example, in a study of recounts commissioned by the State of North Carolina, Kalsbeak *et al.* recommend calculating a statistic based on historical levels of discrepancy in the chosen precincts.[124] Kalsbeak's method would require a preliminary random selection of at least two precincts per jurisdiction and then a supplementary random selection of a number of additional precincts based on historical data on the level of discrepancies found in previous elections in the precincts chosen in the preliminary selection. These kinds of audit models are interesting, but need more study in order to fully understand what historical data are most useful in modifying audits and how these kinds of audit models can be successfully incorporated into current election regulations and practices.

[124] Kalsbeek and Zhang, *An Assessment of the May 2006 Election Recount and a Proposed Permanent Recount Sample Design*, see n. 105.

4.4.3 Sharing of Audit Information

We are hopeful that election officials around the country will begin sharing information with each other about how to conduct post-election audits and steps that successfully reduce audit discrepancies. In our interviews with election officials, it was all too often apparent that many were struggling with issues that others had already resolved. Given the importance of this issue, and the fact that there appears to be growing acceptance by jurisdictions across the country that post-election audits are a necessity, we believe it would be particularly helpful if national organizations of election officials such as NASED, NASS and NACO began holding meeting and trainings related to post-election audits, where election officials could share information with academics, election integrity experts, statisticians, auditors and each other. Researchers have also just begun to study procedural issues with conducting manual counts.[125]

4.4.4 Future Research

In the course of researching and writing this white paper, we noted a number of topics for future research ripe for exploration. The science of election auditing would be improved immensely by research into counting methods and audit procedures as well as research into the suitability of election technology to support audits.

Manual Counting Methods

There has been very little research to date examining the effectiveness of different methods for recounting votes. The CalTech/MIT Voting Technology Project (VTP) published two working papers on the subject of hand-counted ballots in January 2004 and September 2005, and North Carolina sponsored a statistical analysis of recount discrepancies in May 2006. VTP's first paper examined the frequency with which recounts confirm results in jurisdictions that use optical scan, compared to hand-counted paper ballots in New Hampshire. They found that jurisdictions that used hand-counted paper ballots had a higher rate of tabulation er-

[125] See work presented in next chapter and: Goggin, Byrne, Gilbert, Rogers, and McClendon, see n. 5.

ror.[126]

The second VTP paper and the North Carolina study both consisted of statistical analyses of discrepancies between machine and hand counts of ballots.[127] These analyses found small, mostly positive, discrepancies where the magnitude of such discrepancies is larger for hand-marked voting technologies (e.g., punch-card and optical scan ballots) compared to electronic voting machines.

Unfortunately, the specific techniques and procedures associated with the process of manually counting votes have not been studied. There is a widespread belief that humans cannot count as well as computers. However, this criticism depends critically on the procedures used in hand counting and whether or not there is significant variation in how humans and the vote tabulation equipment judge voter intent. Given clear procedures for what constitutes a valid vote and detailed safeguards and checks during the counting process, similar to those used in San Mateo County,[128] vote counts will be consistently accurate.

There is another technical impetus for further study of hand counting processes: a manual count that matches the electronic tally does not establish the absence of a discrepancy. The error rate of blind manual counts is independent of any discrepancies between the paper records and the electronic tallies. Thus, if there is a one-vote discrepancy between the paper records and the electronic tallies, auditors will face an equal chance of making a mistake that cancels the discrepancy and one that turns it into a two-vote discrepancy. The mistake that cancels out the discrepancy is a false agreement ("false negative")—the recount indicates no discrepancy when, in fact, one exists. One way to guard against false negatives is to conduct additional blind recounts whether there is an apparent discrepancy or not. Additionally, increasing the size of a manual counting team from two people to three or more people would further protect against false negatives. The rate at which these false negatives occur is unknown and likely depends on the manual counting method employed.

[126]Stephen Ansolabehere and Andrew Reeves. *Using Recounts to Measure the Accuracy of Vote Tabulations: Evidence from New Hampshire Elections 1946-2002*. 2004. URL: `http://www.vote.caltech.edu/media/documents/wps/vtp_wp11.pdf`.

[127]Michael J. Alvarez, Jonathan N. Katz, and Sarah A. Hill. *Machines versus Humans: The Counting and Recounting of Pre-Scored Punchcard Ballots*. CalTech/MIT Voting Technology Project. Sept. 2005. URL: `http://www.vote.caltech.edu/media/documents/wps/vtp_wp32.pdf`; Kalsbeek and Zhang, *An Assessment of the May 2006 Election Recount and a Proposed Permanent Recount Sample Design*, see n. 105.

[128]Hall, "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures", see n. 5; Hall, *Procedures for California's 1% Manual Tally*, see n. 54.

Quantifying the likelihood of false negatives, and devising other means to address them, are areas for further research.

Election officials need guidance and detailed scientific analyses of manual counting procedures. Members of the NSF ACCURATE center have been working with California counties to document and develop robust manual counting procedures, but this work does not involve controlled experimentation. However, there is a need for an experimental analysis that compares different methods of manual counting procedures for accuracy, efficiency and rates of false negatives.

Suitability of Election Technology To Support Audits

Another promising area of research would analyze the effectiveness of currently deployed election technologies. The primary drivers for the design of election technologies cluster around ease-of-use, configurability, speed and durability. Design for voter verification has only been incorporated recently and design for auditability currently meets only a very narrow notion of auditing.

Currently, voter-verifiable paper records produced by electronic voting machines are difficult to handle during a post-election audit. Most, if not all, currently deployed designs for DRE with voter-verifiable paper record printers include a reel-to-reel thermal paper feed for paper records that print using a heat-activated pigment on one side of the paper. Stephen N. Goggin and Michael D. Byrne of Rice University discuss in detail the difficulty of using this printed paper (which is similar to paper used in cash register receipt printers) in post-election audits.[129]

Among other problems, these reels of paper records do not protect ballot secrecy; individual records should be cut apart and shuffled. Additionally, because of the reel-to-reel configuration, the individual records may tend to curl and don't stack well, which makes handling them during a manual recount cumbersome. Finally, although voting system vendors claim that states can preserve the thermal paper records for the twenty-two month period as required by federal law, it is uncertain whether or not this type of paper is sufficiently durable to withstand a manual recount of multiple races on a single ballot. Research

[129] Goggin and Byrne, see n. 5.

into vote counting methods using thermal paper and research benchmarking the durability of the different kinds of paper that vendors use would reduce election officials' uncertainty as to the types of auditing activities they can undertake.

The software tools provided by vendors play a key role in election auditing. Election databases need to maintain the integrity of the ballots they store and they must also produce reports and output suitable for supporting audits. For example, to do a machine-based audit, auditors would need machine-level results that include aggregate numbers of ballots cast per machine and contest. Each vendors' election database product produces some type of aggregate vote tally output, but not all produce per-machine or per-precinct results separated by each type of ballot (e.g., absentee, early, provisional, regular, etc.). Also, some vendors' products do not provide electronic output in formats that can be provided to citizen's groups for analysis and oversight. Research that catalogs what auditing support each vendor's product provides, what auditors need and what types of capabilities should be standard would eliminate a growing need felt by election officials and potentially eliminate risky ad hoc practices election officials use to cope with current deficiencies.

Using Technology to Automate Post-Election Audits

A paper by Joseph A. Calandrino, J. Alex Halderman and Edward W. Felten of Princeton University describes at how jurisdictions could use recounting machines to conduct most of the work of auditing, reducing the time and money associated with auditing.[130] The authors state that the output of the recounting machines could be "manually audited," and that their proposal would "achieve equal or greater confidence than precinct-based auditing at a significantly lower cost while protecting voter privacy better than previous ballot-based auditing methods." Certainly, the time, labor and financial savings promised by this and similar proposals make the subject of partial automation of post-election audits worthy of further exploration.

[130] Calandrino, Halderman, and Felten, "Machine-Assisted Election Auditing", see n. 5.

CHAPTER 5

INCREASING THE EFFECTIVENESS, EFFICIENCY AND TRANSPARENCY OF POST-ELECTION AUDITS

California jurisdictions have an extensive history of conducting post-election manual tallies of ballot records; they have performed this type audit since the 1960s when the use of lever and punchcard voting technologies became common statewide.[1] We report findings from studying manual tally procedures in a handful of California counties. Through a combination of iterative procedure development and observation of manual tally activities, we designed new procedures that better promote security, transparency and efficiency. We have since generalized these procedures for use in any California County.[2]

5.1 Introduction

Election auditing works to ensure agreement between what the voter sees, what the voting system records and what is counted by back-end tabulation systems. A key concept in voting system security and auditability is that of *software independence* whereby an "undetected error or fault in the voting system software is not capable of causing an undetectable change

[1] Note: this chapter is based on a paper originally published in Summer 2008. See: Joseph Lorenzo Hall. "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008). URL: `http://josephhall.org/papers/jhall_evt08.pdf`

[2] Due to space limitations, the detailed procedures are presented in a separate document: Joseph Lorenzo Hall. *Procedures for California's 1% Manual Tally*. UC Berkeley School of Information. Apr. 2008. URL: `http://josephhall.org/procedures/ca_tally_procedures-2008.pdf`. These procedures are also available as Appendix E to this thesis.

in election results."[3] Practically, this is achieved by testing the voting system before an election and checking the election results after the election.

In terms of testing, more than 40 states require voting systems be federally certified by independent laboratories before they can be used in live elections. These laboratories perform a series of tests and audits of the software, equipment and documentation to ensure that a given voting system conforms to the federal standards. Some states have found this process to be lacking and have decided to employ their own experts to further evaluate systems.[4]

In terms of post-election auditing, the dominant form of auditing currently in use involves comparing hand-counts of paper audit records with the electronically-recorded and tabulated results.[5] A small minority of states, only 12, allow voting systems that do not produce a paper record.[6] However, only a handful of States have provisions that require routine hand-counts of these records to audit the electronic results. Even amongst the States that do this type of post-election auditing, they typically mandate a flat-percentage audit of 1%-20% of precincts, machines or election districts, randomly chosen. The state-of-the-art in post-election auditing, in practice, involves tuning the size of the audit to a desired level of confidence (or statistical significance) while taking into account the size of the units being audited and the margins of contests on the ballot.[7] This type of "tuned" audit can help

[3] Ronald L. Rivest and John Wack. *On the Notion of "Software Independence" in Voting Systems*. July 2006. URL: http://vote.nist.gov/SI-in-voting.pdf.

[4] *Top-To-Bottom Review of California's Voting Systems*. California Secretary of State. Aug. 2007. URL: http://www.sos.ca.gov/elections/elections_vsr.htm; Patrick McDaniel, Matt Blaze, Giovanni Vigna, et al. *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing (Academic Final Report)*. Dec. 2007. URL: http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf; *Software Reviews and Security Analyses of Florida Voting Systems*. Florida State University's Security and Assurance in Information Technology Laboratory. Feb. 2008. URL: http://www.sait.fsu.edu/research/evoting/index.shtml.

[5] Lawrence Norden, Aaron Burstein, Joseph Lorenzo Hall, and Margaret Chen. *Post-Election Audits: Restoring Trust in Elections*. Brennan Center for Justice at The New York University School of Law and The Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley School of Law (Boalt Hall). 2007. URL: http://www.brennancenter.org/dynamic/subpages/download_file_50227.pdf.

[6] The Verified Voting Foundation keeps an up-to-date list of state paper record laws on its front page (see: http://www.verifiedvoting.org/). Many researchers believe that paper is currently the only feasible form of such an audit record, while others advocate for "end-to-end" verification systems or take issue with the lack of verifiability of most paper-based systems for people with disabilities. See: Ben Adida and C. Andrew Neff. "Ballot Casting Assurance". In: *USENIX/ACCURATE Electronic Voting Technology 2006 (EVT'06) Workshop* (2006). URL: http://www.usenix.org/events/evt06/tech/full_papers/adida/adida.pdf; Daniel Tokaji. "The Paperless Chase: Electronic Voting and Democratic Values". In: *Fordham Law Review* 57 (2005). URL: http://ssrn.com/abstract=594444

[7] Philip B. Stark. "Conservative Statistical Post-Election Audits". In: *The Annals of Applied Statistics* 2 (2008). 550–581. URL: http://arxiv.org/abs/0807.4005; Javed A. Aslam, Raluca A. Popa, and Ronald L. Rivest.

to ensure that jurisdictions do not needlessly waste time and effort. In the context of this article, audits based on statistical confidence will simply mean more or less hand counting.

5.2 Background and Motivation

5.2.1 The Manual Tally Process in California

California has been performing post-election manual tallies for over 43 years.[8] At that time in the early 1960s, punchcard voting equipment, after lever machines, had become the next major voting technology. The type of punchcard that was best suited for large jurisdictions, like Los Angeles County, maximized the number of ballot positions per ballot; these punchcards had no candidate or choice names printed on the face of the punchcard. The new "automatic manual recount" process would serve as a check on the punchcard tabulation machinery in order to ensure that the ballot position number on the paper punchcard corresponded to the correct candidate in the tabulation program.[9] In fact, while the emphasis in current law is that the manual tally is not a recount (vote totals do not change in the tally but do in a recount), the original provision called for a "public manual recount" of ballots in 1% of precincts or no fewer than 6 precincts.[10]

California law specifies very little directly about the conduct of the manual tally. The legal definition of the "one percent manual tally" is:

> [The] "One percent manual tally" is the public process of manually tallying votes in 1 percent of the precincts, selected at random by the elections official, and in one precinct for each race not included in the randomly selected precincts. This

"On Auditing Elections When Precincts Have Different Sizes". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008). URL: http://www.usenix.org/events/evt08/tech/full_papers/aslam/aslam.pdf.

[8] California's 1% manual tally was introduced in 1965. See: California Statutes 1965, c. 2040, p. 4659, Sec. 1.

[9] Saltman provides interesting cases of historical punchcard mishaps. See: Roy G. Saltman. *Effective Use of Computing Technology in Vote-Tallying*. National Bureau of Standards. Mar. 1975. URL: http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf

[10] Note that the current manual tally statute, CA Elec. Code Sec. 15360, was consolidated from a number of historical statutes. See: Former Sec. 15645, enacted by CA Stats. 1994, c. 920, Sec. 2, (derived from: former Sec. 15281 (added by CA Stats. 1976, c. 246, Sec. 3), former Sec. 15417 (added by CA Stats. 1965, c. 2040, p. 4659, Sec. 1), and former Sec. 17190 (added by CA Stats. 1978, c. 847, Sec. 5, amended by CA Stats. 1986, c. 1277, Sec. 14.).

procedure is conducted during the official canvass to verify the accuracy of the automated count.[11]

For electronic voting systems, the law considers the voter-verified paper audit trail (VVPAT) the record of the vote for tallying purposes and the VVPAT governs if there is a discrepancy between the electronic and paper records.[12] Finally, Sec. 15360 of the California's Election code specifies a number of high-level requirements for the tally:

- It is conducted over all races in 1% of precincts (or at least one precinct), randomly chosen.
- For races not chosen in the 1% selection, election officials must choose, not necessarily randomly, 1 additional precinct for that race and are required to tally only that race.
- It must include vote-by-mail (VBM) and early voting ballots.
- The elections official must use either a random number generator or a selection method specified in regulations by the Secretary of State.
- The tally is a public process and election officials must provide a minimum five-day public notice.
- The elections official must issue a report as part of its certification of the official canvass that identifies any discrepancies found and that includes a description of how they were resolved.

In addition to these legal requirements, the California Secretary of State, under her authority as chief election official of California, has imposed additional requirements including escalating the size of the audit and increasing scrutiny of certain types of voting systems. These additional requirements are a result of the California Secretary of State's Top-To-Bottom Review (TTBR) of Voting Systems and the Post-Election Audit Standards Working Group.[13]

[11] CA Elec. Code Sec. 336.5.
[12] CA Elec. Code Sec. 19253(b)(2).
[13] California Top-To-Bottom Review, see n. 4; David Jefferson, Elaine Ginnold, Kathleen Midstokke, et al. *Evaluation of Audit Sampling Models and Options for Strengthening California's Manual Count.* California Secretary of State. July 2007. URL: `http://www.sos.ca.gov/elections/peas/final_peaswg_report.pdf`; *Post-Election Manual Tally Requirements.* California Secretary of State. Oct. 2007. URL: `http://www.sos.ca.gov/elections/voting_systems/ttbr/post_election_req.pdf`.

In practice, the hand-counting method used by counties in California seems very similar. The typical tally team uses four people consisting of two talliers, one caller and one witness:

- The **caller** speaks aloud the choice on the ballot for the race being tallied (e.g., "Yes... Yes... Yes..." or "Lincoln... Lincoln... Lincoln...").
- The **witness** observes each ballot to ensure that the spoken vote corresponded to what was on the ballot and also collates ballots in cross-stacks of ten ballots.
- Each **tallier** records the tally by crossing out numbers on a tally sheet to keep track of the vote tally.[14]

Talliers announce the tally at each multiple of ten ("10", "20", etc.) so that they can roll-back the tally if the two talliers get out of sync.[15]

5.2.2 Motivation

This type of post-election audit—the manual tally of paper records against results in the election database—has become increasingly important now that many states have adopted requirements that voting systems produce independent paper records. Such records do not serve their role as an audit trail if the records are not routinely examined as part of an audit.[16]

[14] See n. 50 for examples of blank tally sheets.

[15] We are not certain why these counties had such similar counting methods. Upon asking, for example, about the size and make-up of tally teams, election officials tended to respond that this is how they have counted in the past. One hint to this particular question came when we observed one county, Alameda County, using three-member tally teams instead of the more-standard four-member teams. Upon questioning, the county said that the election code did not require them to use four-member teams for the manual tally. This is correct; the election code does not contain much detail about specific procedures for manual tallying. Where might Alameda have thought that the election code speaks at all about, for example, the structure of a tally team? CA Elec. Code 15102 does specify, in a section titled *Vote By Mail Processing*, that hand tallying of vote by mail ballots shall be done by a team of four people:

> When the tally is done by hand, there shall be no less than four persons for each office or proposition to be counted. One shall read from the ballot, the second shall keep watch for any error or improper vote, and the other two shall keep the tally.

[16] Of course, voters must actually check that the contents of the paper record match their intent and what is displayed on the voting system screen. Recent evidence suggests that few voters do this. See: Sarah P. Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. Rice University PhD Thesis. May 2007. URL: `http://chil.rice.edu/alumni/petersos/EverettDissertation.pdf`. This concern does not apply to technologies where voters directly-mark the paper record, such as optical scanners.

In California, there have been problems in the past due to underspecification in existing legislation. While a catalog of such deficiencies due to regulatory underspecification is beyond the scope of this work, we provide a few illustrative examples. For example, only recently did the manual tally law explicitly specify that VBM ballots be included. With many counties in California now reporting 40-50% of ballots cast as VBM ballots, this had meant that a large fraction of cast ballots went unaudited. Also, the law only recently specified a method for random selection of precincts to be manually tallied.[17] Jurisdictions have in the past used, and continue to use, opaque methods of generating pseudorandom numbers—such as via software provided by the voting system vendor for this purpose—instead of publicly verifiable methods like those described by Cordero et. al.[18]

In addition to the underspecification alluded to above, there are other serious constraints related to timing and resources imposed upon jurisdictions that affect their manual tally. The most significant constraint is due to the time period in which the manual tally must be completed. California law specifies that the canvass, which includes the manual tally, must be complete 28 calendar days after the election.[19] For smaller jurisdictions that do not have to count many ballots, the timing of the manual tally can occur promptly after election day. For very large counties, such as Los Angeles County, the manual tally process can take weeks. This is a serious constraint because, as we explain later, the integrity of the audit critically depends on all initial counting being complete before the tally begins; otherwise, the numbers being audited will change *during* the audit. Performing a high-quality audit also depends on resource constraints such as a jurisdiction's budget and available staff and space.

As our goal was initially to increase the security and transparency of the manual tally process, we recognized that our efforts would exacerbate these tensions. Our new procedures needed to be optimized, in a sense, to take advantage of possible efficiencies where

[17] Note that this election law (CA Elec. Code Sec. 15360(c)) now specifies that election officials must use a "random number generator or other method" from regulations adopted by the Secretary of State. This means that there is no prohibition on computer-generated pseudorandom numbers, as we would prefer.

[18] Arel Cordero, David Wagner, and David Dill. "The Role of Dice in Election Audits—Extended Abstract". In: *IAVoSS Workshop on Trustworthy Elections 2006 (WOTE 2006)* (June 2006). URL: `http://www.cs.berkeley.edu/~daw/papers/dice-wote06.pdf`. But compare with: Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. "In Defense of Pseudorandom Sample Selection". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008).

[19] CA Elec. Code Sec. 15372.

election officials could save time and resources.

5.3 Methodology

In order to develop improved post-election audit procedures that could be used by California counties, we chose a non-standard and somewhat exploratory methodology. We go in more detail below, but essentially we did the following:

- We examined the manual tally procedures for a few California jurisdictions interested in improving their procedures.
- We developed an initial set of improved procedures through a series of iterative meetings with one such jurisdiction, San Mateo County.
- This jurisdiction then incorporated our improvements into their own procedures and used them in actual elections.
- We observed our collaboratively-generated procedures in action and noted deviations, improvisations and new issues that came to light only during an actual tally. We also observed the manual tally in a few other counties with which we have had only limited contact, Alameda County and Marin County, and worked closely with a fourth county, Yolo County.[20]
- Finally, we generalized the improved set of procedures into one set of procedures that can be used by any California county.[21]

We have been fortunate enough to collaborate with a number of election officials to improve their audit processes. Over the past year, we have worked closely in a larger multidisciplinary team[22] with election officials in California's Alameda County, Marin County,

[20] We met twice with Yolo county to discuss how what we were learning would apply to Yolo, a much smaller county. This author did not have the opportunity to observe the manual tally in Yolo County, although we benefited from the observations of collaborators: David Wagner. *Thoughts on the Nov 16, 2006 1% Manual Tally in Yolo County*. UC Berkeley Department of Computer Science. Nov. 2006. URL: `http://www.yoloelections.org/news/snews/reactions.pdf`.

[21] See Appendix E or Hall, *Procedures for California's 1% Manual Tally*, see n. 2

[22] Others involved in this work include David Dill (Stanford Computer Science), David Wagner (UC Berkeley Computer Science), Arel Cordero (UC Berkeley Computer Science), Aaron Burstein (UC Berkeley Law) and Kim Alexander (California Voter Foundation).

San Mateo County and Yolo County.

These counties were interested, to different extents, in incorporating academic input about security and auditability into their post-election process. Our interaction with some of these counties was more indirect in some cases, when the county was interested in academic input on specific elements of their manual tally procedures.[23]

We decided to collaboratively redesign of the post-election audit procedures for one county, San Mateo. San Mateo County was willing to work closely with us to re-evaluate their procedures, was a fairly large county and was located close to our home institution. Our multidisciplinary team met with the election officials and staff of San Mateo over the Fall of 2006 and Spring of 2007 and this author observed the random selection and manual tally processes over a number of election cycles and developed the written procedures.

Our aim was to have a rich, iterative interaction where researchers learned about the issues involved in running elections and election officials learned about security, transparency and auditability while we both worked to align our two sets of expertise into concrete election procedures. As our collaboration progressed, our research team was able to highlight what we felt were the best practices in election auditing, from a scientific and policy perspective. In late Fall 2006, we drafted a first set of post-election audit procedures specific to San Mateo County that we modified as a group. These audit procedures were used as a model by San Mateo in the post-election audits of their 2006 and 2007 elections.[24]

5.4 Findings

We were able to make a number of improvements to the procedures in terms of security, transparency and efficiency.

[23] For example, Alameda County worked with Arel Cordero, David Wagner, David Dill and members of their public advisory committee to design a random selection process using a tumbler with numbered ping-pong balls. We provided a research memo describing how imperfections in their random selection process resulted in non-uniform random selection. We describe this case in Section 5.4.1.

[24] For the earlier draft of our procedures, see: Joseph Lorenzo Hall. *The 1% Manual Audit in California: Proposed Procedures and Rationale*. Nov. 2006. URL: `http://www.josephhall.org/papers/manual_audit_procedures-final.pdf`. Also, see: Rebekah Gordon. "Elections Office gets tips from experts". In: *San Mateo County Times* (Nov. 2006). URL: `http://www.shapethefuture.org/press/2006/insidebayareacom113006.asp`.

5.4.1 Security

The manual tally serves multiple security-relevant roles: as an audit process, a deterrent process and a tamper-evidence process. Given the heightened attention to security in elections in recent years, election officials are eager to learn about threats, possible attacks and mechanisms to neutralize exploitable opportunities that could allow subverting the elections process. We recommended a number of security-based improvements to existing procedures and subsequently observed other security-critical behavior that could be improved.

Timing of random selection and tally: Since the purpose of the tally is to compare two sets of independent vote counts, the random selection and manual tally *must* take place after the count has been completed. That is, a given ballot type cannot be audited until all the ballots of those type are counted.[25] From a security perspective, attackers should not be able to predict which precincts will be audited while they still have an opportunity to influence vote totals. There is evidence that many jurisdictions perform their random selection very soon after election day, before they could possibly have completed counting VBM and provisional ballots.[26] Unfortunately, for very large jurisdictions like Los Angeles, it is not possible to wait until counting is completed before commencing the selection and tally; the tally process would take longer than the time permitted for the canvass. One possible solution for very large jurisdictions is to treat each ballot type as a sampling stratum in a stratified sampling regime.[27]

Timing of retrieval of tally materials: Related to this last point is the preservation of the chain of custody for the audit materials once the selection is finished. As soon as the audited precincts have been chosen, the ballot materials to be audited become particularly sensitive.

[25] By "ballot types" we mean ballots cast using a distinct type of voting technology such as in-precinct optical scan ballots, DRE ballots, paper-based provisional ballots, etc.

[26] The Secretary of State has published manual tally reports that show many counties performing random selection very soon after election day. See: *County Manual Tally Reports*. California Secretary of State. Apr. 2008. URL: `http://www.sos.ca.gov/elections/manual_count_reports.htm` In one case, a county seems to have even performed the selection *before* election day (February 5, 2008). See: *Summary Information—Post-Election Manual Tally*. County of Fresno County Clerk / Registrar of Voters. Mar. 2008. URL: `http://www.sos.ca.gov/elections/county_manual_count_reports/Fresno/Fresno.pdf`

[27] This allows beginning the manual tally for ballot types where counting is completed *before* all ballot types are counted. In February 2008, we participated with Philip Stark (UC Berkeley Statistics) and Elaine Ginnold (Marin County Registrar of Voters) in the first statistical confidence-based audit of an election. In this pilot, each ballot type was sampled in separate strata so that the tally could begin for ballots where counting was completed.

A window of opportunity exists here during which attackers who have tampered with the electronic count could avoid detection by manipulating the audit trail. It is important to minimize the amount of time between the selection and tally and particularly to protect sensitive ballot materials used in the audit.

The feasibility of collecting audit materials quickly depends on the size of the county. Notably, it was difficult for San Mateo, a relatively large county, to initially comply with this recommendation as different ballot materials needed for the tally were stored in physically separated warehouses across the county. They have since been able to store all materials on site for the selection and tally at their main warehouse. In contrast, Marin, a smaller county, stores such materials on-site. The time between the selection and tally for both of these counties is now very brief, about one hour. However, in Alameda, another large county about twice the size of San Mateo, three days elapsed between their selection and tally, considerably widening the window of opportunity for tampering with audit trail materials.

Seal verification: Election officials have to pay increasing attention to tamper-evident security seals due to studies that have shown physical access to voting systems can be an important prerequisite for exploiting serious vulnerabilities. Of course, the importance of maintaining the integrity of this seal-based custody chain does not disappear after election day. We observed inconsistent attention to seal verification during the manual tally. While one jurisdiction placed appropriate weight on seal verification, others performed more casual verification to assess that the seal was not broken (but without verifying the serial number on the seal). Attention to seal verification and seal integrity is a critical step for detecting tampering.

Blind counting: To eliminate the possibility of conscious or unconscious influence on the tally by the tally team, the team should operate under blind counting rules. That is, the tally team will conduct the tally without knowing the ballot totals for the tallied precinct. When the tally is complete for a particular ballot type in one precinct, a supervisor compares their totals to those from the election management system (EMS) database. If the totals do not reconcile, the tally team must count the ballots again to make sure there was not a counting mistake.[28]

[28]When counting optical scan ballots—where the ballot marking can be less definitive—we observed that it

While observing, we noted some issues with blind counting and observers' interaction with tally team members. To support transparency, as we note below, observers must have a copy of the electronic results for the precinct being audited. In one case, however, an observer told the tally team the correct electronic tally result when the hand tally was incorrect. This was a violation of two procedural rules: observers are forbidden to interact directly with tally teams and the tally must proceed under a blind counting protocol. To prevent this, observers must be reminded explicitly about the rules of engagement between observers and the tally team and about the importance of conducting a blind count.

Problems with randomness: We observed how slight changes in the random selection method resulted in imperfect randomness.

In San Mateo county, an observer who rolled a set of three ten-sided dice mis-read the roll as being invalid; that is, not corresponding to a valid precinct. Despite the rolled digits in fact being valid, the observer immediately picked up the dice and re-rolled them, effectively ruining that roll. From a security perspective, one could imagine attackers might take advantage of such a situation to ensure that certain precincts are not chosen. In this case, the presiding election official had to explicitly reiterate that observers must not pick up the dice unless directed to by an elections official.

In another case, the county followed their selection protocol perfectly but the protocol itself was flawed. Alameda County performs random selection of precincts using a rotating hopper and a set of 10 ping-pong balls with the digits 0–9 written on them. An election official draws a ping pong ball from the hopper and this digit serves as the ones place of a random number. Balls are drawn, corresponding to successive digits, until the random number chosen corresponds to a number between one and approximately 1200 (there are ~ 1200 precincts in Alameda). One quirk in this selection method results in imperfect randomness: only when the hundreds place digit is 0, 1 or 2 do they draw a fourth digit. This results in non-uniform random selection. Because any random number where the hundreds place is larger than 2 can correspond to only precincts numbered from approximately 300-999, this ultimately results in those precincts being chosen with twice the probability of the

helped to relax the blind counting requirements after two discrepant tallies. This allowed the talliers to try and determine which ballot had been read (or not read) by the machine but not seen (or seen) as a valid vote by the talliers.

remaining precincts. Upon inquiring about this with Alameda, we were told that the original method devised to select random numbers required starting with the thousands digit and *starting over from scratch* when the result would have been an invalid precinct number. We have recommended to Alameda county that they return to discarding invalid random numbers entirely rather than conditionally discarding specific digits. We highlight this case along with two illustrative solutions in a separate research memorandum.[29]

This highlights a compelling finding for procedural research: certain procedures, especially those related to technical security matters, are very sensitive to changes in the protocol. Small changes to procedures may seem trivial to those not familiar with the technical background but could have severe consequences. In order to avoid these kinds of imperfections, experts and observers with domain knowledge need to be involved when procedures change. In the longer term, it makes sense for these types of sensitive procedures to be specified in law or regulation so that such deviance is minimized.

Tallying and reporting appropriate records: Tallying the proper records of the vote as well as reporting meaningful data about the tally are critical security-relevant aspects of tally audits. Previous security work has emphasized that keeping track of data such as undervotes, overvotes and spoiled ballots/VVPATs can serve to aid detection of particularly subtle dynamic attacks. For example, a dynamic attack that misprints VVPAT records could be detected during an audit via an unusual amount of spoiled VVPAT records.[30] Election officials must track these numbers by hand-counting undervotes, overvotes and spoiled ballots as part of the manual tally. Counties do this inconsistently now, but new reporting requirements for the 1% manual tally require counties to report this information to the Secretary of State. To support collection of this data, we assisted the Secretary of State in designing a reporting instrument that includes reporting, among other data, quantities of overvotes, undervotes and spoiled ballots.[31]

---

[29] Joseph Lorenzo Hall. *Research Memorandum: On Improving the Uniformity of Randomness with Alameda County's Random Selection Process.* UC Berkeley School of Information. Mar. 2008. URL: `http://josephhall.org/papers/alarand_memo.pdf` Note: we did not discover this independently; two public observers, Meg Holmberg and Tim Erickson, brought this to our attention.

[30] Lawrence Norden and Eric Lazarus. *The Machinery of Democracy: Protecting Elections in an Electronic World: Brennan Center Task Force on Voting System Security.* Brennan Center for Justice at NYU School of Law. 2006. URL: `http://www.brennancenter.org/dynamic/subpages/download_file_39288.pdf`.

[31] Kim Alexander (California Voting Foundation), Philip Stark (UC Berkeley Statistics) and myself assisted the Office of the California Secretary of State in developing the reporting instrument. See: *Post-Election Man-*

We observed that one county did not appear to be counting the actual paper records but the totals tapes.[32] At least, the method that they used to perform their tally of VVPAT records was very different from the other counties. The tally must be over the records verified by the voter or the necessary confirmation of voter intent is never possible and opportunities for mischief and/or error increase. Like other counties we observed, this particular county started by cutting VVPAT records off of the VVPAT roll. However, they immediately placed the cut VVPATs into manila folders and began cutting up the totals tape for each VVPAT roll, race-by-race. The tally proceeded by the caller calling out phrases like, "McCain, 0... Obama, 0..."; that is, instead of calling out votes off of individual VVPATs, the caller appeared to be reading totals off of the totals tape. When we asked election officials about this, they stated that they were "counting individual votes and not just the summary". In addition to the security-related concern that voters do not verify the totals tape information the law is very specific that the VVPAT must be used for the manual count.[33] We have been unable to confirm what we observed.[34]

Resistance to insider modification of voted ballots: We observed inconsistent attention to insider attacks on voted ballots during the tally process. When we did see provisions meant to mitigate certain types of insider attacks, we were often surprised by their existence. For example, each of the counties we observed had tally teams use pencil for marking tally documents. We found this puzzling as this permitted talliers to erase marks instead of the more standard accounting process for correcting mistakes: crossing out errors and initialing corrections.[35] When we inquired about this, officials responded with an obvious security-based answer: pens could be used to indelibly change voted ballots. In fact, San Mateo's procedures included a prohibition on any indelible marking device in the tally area. While

---

ual Tally Log: Suggested Instructions for Post-Election Manual Tally Requirements (CCROV-08048). California Secretary of State. 2008. URL: `http://josephhall.org/ccrov/CCROV-08048.pdf`

[32] We have been unable to confirm with this particular county how they count VVPAT records.

[33] CA Elec. Code Sec. 19253(b)(1) which says, in part, "The voter verified paper audit trail shall be considered the official paper audit record and shall be used for the required 1-percent manual tally [...]".

[34] For example, one explanation is that there were very few ballots cast on the VVPAT rolls we observed. In that case, most of the candidates on the ballot would have zero votes. Tallying would entail a brief tally of any candidates that do have votes with a lengthy tally of zero votes for each of the remaining candidates. Without pre-filled tally sheets, the task of tallying votes on VVPAT records becomes more a task of confirming the lack of votes.

[35] For example, we observed a tallier in Alameda erasing tally marks after they had to retally a specific candidate. See: `http://www.flickr.com/photos/joebeone/2295569830/sizes/l/`.

we were surprised by this particular case, there did not seem to be more systematic attention to insider threats to the tally process. Obviously, as is the theme of this work, exhaustive attention to insider threats will undoubtedly conflict with other constraints and priorities. Research examining insider threats to election office activity is a promising area for future work.

5.4.2 Transparency

As we have stressed in previous work,[36] electoral transparency requires supporting *access*, *oversight*, *accountability* and *comprehensibility* of election processes. In terms of access and oversight, procedural improvements that impact transparency relate mostly to to publication of notice, procedures and data so that members of the public can observe the process in an informed manner and perform their own calculations, if necessary. In terms of accountability and comprehensibility, we found it was important to have clear lines of communication for asking questions or alerting officials to procedural anomalies.

Public notice: Observers wishing to witness the manual count need to have public notice of the time and location of the tally process. When we began this work, it was difficult to know when and where a given jurisdiction's manual tally would be conducted. With a recent addition to the manual tally law, a minimum of 5-day public notice is now required.[37] This has largely alleviated such frustrations and we have been able to find such notice for the jurisdictions that we have wanted to observe. However, in addition to traditional means of posting notice, like newspaper advertisements, we recommend wide, varied posting of such notice, such as on the jurisdiction's web site, via press release or op-ed in local community publications.

Procedures publication: Along with knowing when and where the tally will take place, observers will need information about the tally procedures themselves as well as any observer guidelines. Observers might not be familiar with the intricacies of the tally procedure and should be provided with a document that summarizes the process and then goes into

[36] Joseph Lorenzo Hall. "Transparency and Access to Source Code in Electronic Voting". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2006* (June 2006). URL: `https://www.usenix.org/events/evt06/tech/full_papers/hall/hall.pdf`.

[37] CA Elec. Code Sec. 15360(d).

detail about how the tally is conducted. The few written tally procedures we have seen, from the counties we observed, range from very detailed to providing a high-level overview.[38] Also, observers may be unfamiliar with how they should behave while observing the tally, as was the case mentioned above where an observer inadvertently broke the blind counting rule (see 5.4.1). We encountered this ourselves in San Mateo when we were told that no discussion is allowed amongst observers during the tally process per their observer guidelines.[39] San Mateo seems to have the best practice here in terms of providing observation guidelines for all observable events in a typical election cycle.[40]

Data publication: In addition to procedural information, observers need be provided with various data. For the random selection, observers need a hardcopy (or read-only copy) of the mapping between possible random numbers to precinct identifiers.[41] This allows observers of the random selection to verify that the selected number indeed corresponds to the correct precinct identifier. In our observations, these materials were made available to observers in Alameda and Marin but not in San Mateo. San Mateo instead had the mapping spreadsheets on a laptop—a medium that is decidedly not read-only—and would turn the laptop towards observers so that they could verify the selection.[42]

For the tally, observers should have hardcopy (or read-only) copies of the unofficial statement of the vote as well as the detailed precinct results reports for each selected precinct. We have recommended that jurisdictions provide the statement of the vote during the ran-

[38] *One Percent Manual Recount Procedures*. San Mateo County Clerk Assessor Recorder Elections. Dec. 2007. URL: http://josephhall.org/procedures/sanmateo_tally_procedure_122007.pdf; *Procedures for One Percent Manual Tally*. Marin County Registrar of Voters. Feb. 2008. URL: http://josephhall.org/procedures/marin_tally_procedure_022008.pdf; *Process Overview of the 1% Manual Tally*. Alameda County Registrar of Voters. Feb. 2008. URL: http://josephhall.org/procedures/alameda_tally_procedure_022008.pdf.

[39] San Mateo's guidelines required observers to ask to be escorted out of election headquarters before they could engage in discussion. To adequately observe audit activities, observers need to be able to effectively communicate with one another. In this case, instead of talking to each other, we had to resort to passing notes.

[40] See: *Election Observer Handbook*. San Mateo County Clerk Assessor Recorder Elections. Feb. 2008. URL: http://josephhall.org/procedures/sanmateo_obsprocs_022008.pdf In addition, the California Secretary of State requires counties to publish an Election Observation Panel Plan (see: http://www.sos.ca.gov/elections/eop.htm) and the California Election Code imposes certain requirements to facilitate public observation in certain cases. See CA Elec. Code Sec. 15104.

[41] We call this hardcopy mapping a Master Selection Spreadsheet. Recall that once the 1% selection is complete, additional selection may be necessary as there may be races for which no precinct was selected for auditing. If a jurisdiction has decided to follow best practice, rather than the letter of the law, and select precincts randomly for these additional races, they will need to provide similar mapping spreadsheets for each race in the election (we call these Contest Selection Spreadsheets).

[42] See the image linked in n. 45.

dom selection process so that the jurisdiction "commits to" or "vouches for" the vote totals before any precinct is selected. Observers need detailed precinct reports wile observing so that they can confirm the tally totals in the same manner as the tally supervisor confirms each tally team's manual count results. Again, these materials were available in Alameda and Marin counties but were not present in San Mateo.

Clear lines of communication: Observers need effective lines of communication for asking questions in a timely manner and also escalating issues that they feel are contrary to written procedures or otherwise anomalous. During our observations, we were able to easily ask questions of even the most senior elections personnel. We consistently received thoughtful and considerate responses to our queries and concerns. This notion of transparency seems to be something that counties support well already.

5.4.3 Efficiency

Efficiency—that is, minimizing waste during the tally in terms of time and resources—was a major concern during this work. We approached this research project knowing that we could not simply make demands of election officials in terms of security and transparency and expect them to adopt our ideas without question. Accordingly, we felt that we should work equally as hard at giving something back. During our initial conversations with elections officials, it became clear that recommending steps that could make their processes more efficient would be greatly appreciated.

The manual tally, as we have mentioned above, can be problematic in terms of time, space and staff. The tally is a time- and resource-intensive effort that requires a significant amount of work from election staff (and/or temporary employees) during a crucial time in which these staff could be assisting with other canvass-related activities. Most of the recommendations we have made in terms of efficiency relate to time efficiencies; that is, if we could find a way to do a task in less time, it would free up staff and other resources.

Randomness can be inefficient: Often our preferred methods of publicly-verifiable random selection can be inefficient. For example, in San Mateo during the random selections in November 2006 and 2007, using 10-sided dice to select the 1% sample went fairly quickly

but selecting precincts for races not included in the 1% sample took a considerable amount of time—on the order of an hour—due to the high frequency of invalid rolls. During these selection events with many mis rolls, we found ourselves (observers and election officials) making up rules as we went along. For example, if there were two precincts to choose from, we would roll one die and specify that even numbers corresponded to one precinct and odds to the other. But this ad-hoc rule creation was troubling and became difficult to do easily on-the-fly with larger numbers of precincts. Among the recommendations of Cordero et. al, they advised "binning" random numbers into equal sized bins to increase the frequency of valid rolls.[43] We created a web-accessible script written in PHP to do this for an arbitrarily-large jurisdiction with an arbitrary number of 10-sided dice.[44] This script does one thing: given a number of precincts to choose from and a number of 10-sided dice, it calculates the appropriate binning to minimize the frequency of misrolls (it also displays the bin mapping in a format that is easy for election staff to cut-and-paste into a spreadsheet program). San Mateo county used this script for their random selection in the manual tally for their February 2008 election and considerably shortened the time it took to do the selection as well as streamlined the process.[45]

Vote results reports should be fine-grained: In some cases, the vendors' EMSs will not report machine-specific results within a precinct. Unfortunately, this often means that a manual tally of, say, four to five VVPAT rolls for a given precinct can be compared only with aggregate precinct totals, instead of on a machine-by-machine basis. Considering that we observed that it might take one tally team of four people over 4 hours to tally one full VVPAT roll, finding a discrepancy after all that effort is ineffective and inefficient; if there is a discrepancy, the EMS report contains no information that would be helpful in locating on which VVPAT roll the discrepancy might be contained. This was the case in San Mateo which uses Hart InterCivic voting systems; each precinct had 4-5 VVPAT rolls but the Hart system only reports results at the precinct level. This can result, due to blind counting rules mentioned above, in the tally team having to redo the tally for *each* of that precinct's VVPAT

[43] Cordero, Wagner, and Dill, see n. 18.

[44] Joseph Lorenzo Hall. *Dice Binning Calculator for Post-Election Audits*. Mar. 2008. URL: `http://www.josephhall.org/dicebins.php`.

[45] To see our `dicebins.php` calculator "in action" in San Mateo, see: `http://www.flickr.com/photos/joebeone/2293490290/sizes/l/`.

rolls. If the EMS had reported vote totals for each machine in the precinct, the tally team would have instead had to retally a small number of VVPAT rolls.[46]

State-of-the-art auditing methodologies can also place distinct requirements on voting systems. For example, statistically conservative audit schemes[47] start with a flat percentage audit, then require the auditor to calculate a statistical confidence value and, if needed, increase the sample size of the audit. However, some vendors' EMSs will produce meaningful results only in PDF format, a format useful for presentation of information but not useful for computation. To quickly calculate a statistical quantity with data from hundreds of precincts in such an unusable format would require an army of transcribers. If EMSs had the capability to output vote totals in an open, machine-readable and machine-processable format, such as the OASIS standard Election Markup Language,[48] they would better support more sophisticated forms of election audits.

Adverse effects of good team demeanor: We observed subtle effects of tally team members becoming gradually more comfortable with one another. We noticed that, quite naturally, the members of a tally team tended to get progressively more comfortable with each other as tallying progressed and increasingly reluctant to assert certain conflicting aspects of their tally team roles.[49] It is natural for a working group to converge, socially or otherwise, on a more comfortable working state, but often it seemed that objections were self-silenced to avoid derailing or slowing down the tally. However, this posed a few unique problems. We noted that occasionally, a tallier would either forget to call out on every multiple-of-ten vote or call out earlier than another tallier. More often than not, this was dealt with informally rather than with a more formal procedure of backing up ten votes and redoing the tally to this point. We also noted that the witness would occasionally question the vote de-

[46] We observed one team quickly recounting stacks of ballots to make sure that they arrived at the result they got with the slower tally process. This might have been developed in response to having to retally an entire precinct.

[47] Stark, "Conservative Statistical Post-Election Audits", see n. 7.

[48] *See:* `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election`.

[49] We note that, in one exceptional case, one tally team member was a supervisor working in the local elections department. We found the interaction between this tally team member and the other members of the team to be particularly different from other teams. We were uncertain if the other team members were directly supervised by this individual. If so, this obviously highlights an undesired point of friction. Election officials need to be conscious of these kinds of power dynamics and seek to neutralize them. One option would be to only place supervisors on teams of people that they do not directly supervise (such as temporary employees). Another possible solution is to emphasize in training that all tally team members have equal authority for the period of time in which the tally is conducted.

termination made by the caller or mis-stack ballots into a stack of 9 ballots. These hiccups were also often dealt with informally instead of with a more formal challenge procedure for questioning the determination of a caller or rolling back the count to correct for mis-stacking. To help solve this problem, tally team training should emphasize that that talliers must feel comfortable stopping the process at any point for clarification or to question a determination made by other team members.

Using pre-filled tally sheets: A big time saver observed in Marin County's tally was the use of pre-printed tally sheets. In other jurisdictions such as Alameda and San Mateo, tally teams had to fill out generic tally sheets by hand for the precinct they were tallying.[50] In a primary election with many candidates and many races, this can take a significant amount of time; e.g., in San Mateo, we observed that this took about one hour or 20 person-hours.[51] In contrast, Marin used a digital tally sheet template in which they had one staff member fill out the candidate names and then print copies for the tally team. To save time in terms of person-hours, pre-filled printed tally sheets should be made for all jurisdiction-wide races and then races unique to a particular ballot style can be filled in by hand.

Innovative uses of RFID technology: Finally, Alameda county exposed us to very innovative uses of radio-frequency identification (RFID) technologies in their chain-of-custody procedures. Alameda applied RFID chips to the election media and the pollbook for each precinct. When pollworkers returned precinct materials to drop-off locations, an election staffer with a RFID reader would read the RFID chips from within a sealed security bag, *without breaking the seal*. This shortened the time needed to check the presence of critical items drastically—from about 30 minutes to less than 5—while preserving one link in the chain of custody. While this use of RFID technology was not in the context of the manual tally, it shows increasing promise in the use of RFID chips for elections-related chain-of-custody. Given the poor quality of current security seal technology,[52] we recommend that researchers

[50] For images of these types of tally sheets in Alameda and San Mateo, see the following images, respectively: `http://www.flickr.com/photos/joebeone/2266221884/sizes/l/` and `http://www.flickr.com/photos/joebeone/2240342264/sizes/l/`.

[51] This observation was based on San Mateo's VVPAT tally area which used 5 tally teams of 4 people each. San Mateo did photocopy the filled-out tally sheets once each tallier had completed them so that they could be reused when the team started a new VVPAT roll.

[52] Roger G. Johnston. "Tamper-Indicating Seals". In: *American Scientist* 94 (Nov. 2006). 515–523. URL: `http://ephemer.al.cl.cam.ac.uk/~rja14/johnson/newpapers/American%20Scientist%20(2006).pdf`.

combine the inventory-tracking capability of RFID technology, the tamper-evidence of sensitive security seals and recent innovations in uncloneable RFIDs to provide the a type of security seal that can be read and cryptographically verified quickly at a distance but that will also "self-destruct" upon physical tampering, so that no forged replacement could be crafted.

5.5 Conclusion

We analyzed the manual tally process as used in a number of California counties to design a generic set of tally procedures that California counties can use. In the process of iterating on the design of procedures with San Mateo as well as observing elections in San Mateo, Alameda and Marin Counties, we developed a number of improvements in terms of security, transparency and efficiency. We also discovered some issues outside the scope of procedure design; for example, the challenges that large counties face in meeting the 28 day canvass deadline or how voting systems could better support manual tally audits. The current procedures resulting from this work exist specifically for San Mateo[53] or in a generic form, designed for use by any California county in improving their 1% manual tally process.[54] We have attempted to note in the generic procedures where certain ideas are not specific to California.

[53] San Mateo 1% Manual Tally Procedures, see n. 38.
[54] See Appendix E or Hall, *Procedures for California's 1% Manual Tally*, see n. 2

CHAPTER 6

CONCLUSION

This dissertation started by defining the concept of electoral transparency. Each of the substantive chapters focused on a specific project dealing with various notions of transparency: the role of disclosed and open source software, the role of contractual agreements between jurisdictions and voting system vendors, the role of audit design and the role of detailed procedures for conducting post-election audits. This work has directly resulted in increased transparency of our voting systems: through disclosure of voting system source code to qualified individuals in state-level voting system analyses, through better contract negotiations that result in contracts friendly to the public interest and through more rigorous and better specified post-election audits of software-independent audit records.

There is quite a bit of work remaining to be done. Researchers must work directly with election officials to fully incorporate their expertise and environment into applied and fundamental election science. Voting system vendors must also work more openly with other members of the elections ecosystem so that their products perform to a myriad of expectations and so they get the critical input they clearly need during early stages of product development. While the federal and state regulatory environment is in much better shape than it was at the beginning of this decade, we must continue to explore ways to make it faster, better and cheaper.

We also can apply a good deal of what we learn about voting systems to other areas of scholarship. Applications such as applied cryptography, procedures research, combinatorial auctions and whistleblower policy all share critical features of the problems faced by secret ballot elections mediated by computerized technologies.

While funding for election administration has historically been lacking, we've seen foundations and government agencies begin to increase opportunities for the research needed to improve election administration. For example, I have been fortunate, along with 10 PIs and a many other students, to be supported by the National Science Foundation through the NSF ACCURATE CyberTrust center. Elections research can be difficult and unforgiving, so I'm excited that there are now more smart and capable minds focusing on elections research than ever before. One thing will continue to ring true: This is the best time ever to cast a ballot in America.

Appendices

Appendix A
October 28, 2003 Cease & Desist Letter

(This page intentionally left blank.)

Walker & Jocke
a legal professional association

Ralph E. Jocke
Patent
&
Trademark Law

October 28, 2003

DMCA Administrator
University of California, Berkeley
IST-AVCO, Room 235 #3812
Berkeley, CA 94720

policy@uclink.berkeley.edu

Re: Copyright Infringement

Dear Administrator:

We represent Diebold, Incorporated and its wholly owned subsidiaries Diebold Election Systems, Inc., and Diebold Election Systems ULC (collectively "Diebold").

Diebold is the owner of copyrights in certain correspondence and other material relating to its electronic voting machines, which were stolen from a Diebold computer ("Diebold Property").

It has recently come to our clients' attention that you appear to be hosting a web site that contains Diebold Property. The web site you are hosting infringes Diebold's copyrights because the Diebold Property was reproduced, placed on public display, and is being distributed from this web site without Diebold's consent.

The web site and Diebold Property are identified in a chart attached to this letter.

The purpose of this letter is to advise you of our clients' rights and to seek your agreement to the following: (1) to remove and destroy the Diebold Property contained at the web site identified in the attached chart and (2) to destroy any backup copies of the Diebold Property in your possession or under your control.

Please confirm, in writing, that you have complied with the above requests.

330 • 721 • 0000 MEDINA | 330 • 225 • 1669 CLEVELAND | 330 • 722 • 6446 FACSIMILE | rej@walkerandjocke.com E-MAIL
231 South Broadway, Medina, Ohio U.S.A. 44256-2601

To the best of my knowledge and belief the information contained in this notification is accurate as of the time of compilation and, under penalty of perjury, I certify that I am authorized to act on behalf of Diebold.

Our clients reserve their position insofar as costs and damages caused by infringing activity with respect to the Diebold Property. Our clients also reserve their right to seek injunctive relief to prevent further unauthorized use of Diebold Property, including reproduction, distribution, public display, or the creation of derivative works, pending your response to this letter. We suggest you contact your legal advisors to obtain legal advice as to your position.

We await your response within 24 hours.

Very truly yours,

Ralph E. Jocke

330 • 721 • 0000 MEDINA | 330 • 225 • 1669 CLEVELAND | 330 • 722 • 6446 FACSIMILE | rej@walkerandjocke.com E-MAIL

231 South Broadway, Medina, Ohio U.S.A. 44256-2601

INFRINGING MATERIALS POSTED ON:
sims.berkeley.edu

Web site/page	Infringing material/activity at site/page
http://sims.berkeley.edu/~jhall/nqb/archives/lists.tgz	This site consists of Diebold Property, stolen from Diebold, reproduced and placed on public display on this web site, and distributed from this web site without the consent of Diebold.

330 • 721 • 0000 MEDINA
330 • 225 • 1669 CLEVELAND
330 • 722 • 6446 FACSIMILE
rej@walkerandjocke.com E-MAIL
231 South Broadway, Medina, Ohio U.S.A. 44256-2601

Appendix B

Brennan Center/Samuelson Clinic Audit Panel

The Brennan Center and the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall School of Law (University of California Berkeley) convened a blue ribbon panel (the "Audit Panel") of statisticians, voting experts, computer scientists and several of the nation's leading election officials to assist them in reviewing and evaluating both existing post-election audit laws and procedures, and the papers of academics and election integrity activists that have frequently criticized such laws and procedures as inadequate. Based on input from the Audit Panel, the Brennan Center and Samuelson Clinic then made a number of conclusions and recommendations about best audit practices. These conclusions and recommendations are those of the authors alone, and should not necessarily be ascribed to audit panel members. The members of the Audit Panel are listed below:[1]

- Kim Alexander, president and founder, California Voter Foundation
- Georgette Asherman, independent statistical consultant, founder of Direct Effects
- Ted Bromley, Legislation and Elections Administration, Connecticut Secretary of State
- David Dill, Professor of Computer Science and Electrical Engineering, Stanford University
- Mark Halvorson, Director, Citizens for Election Integrity Minnesota
- S. Candice Hoke, Director, Center for Election Integrity, Cleveland State University

[1] Organizational affiliations are shown for identification purposes only.

- David Klein, Elections Research and Operations Specialist, Ohio Secretary of State
- Michael Kozik, Managing Attorney, Legislation and Elections Administration, Connecticut Secretary of State
- Lesley Mara, Administrative Office, Connecticut Secretary of State
- Walter Mebane, Jr., Professor of Government, Cornell University
- Marisa Morello, Administrative Office, Connecticut Secretary of State
- Rene Peralta, PhD, former Research Scientist at Yale University Department of Computer Science
- Ronald Rivest, Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology
- David Robin, Member, Chicago Bar Association Election Law Committee
- Warren Slocum, Chief Elections Officer & Assessor-County Clerk-Recorder, San Mateo County, California
- Anthony Stevens, Assistant Secretary of State, New Hampshire
- David Wagner, Professor of Computer Science, University of California, Berkeley

APPENDIX C

SELECTION OF ADDITIONAL PRECINCTS IN CLOSE ELECTIONS

Although we attempted to make the discussion in the main text of Chapter 4 non-technical, some readers might like additional details about the statistical models that underlie our discussion of full-precinct audits.

A. GETTING TO THE "CONFIDENCE LEVEL"

The basic question that many published studies of post-election auditing tackle is, "If there are b discrepant precincts out of a total of N precincts, how many precincts must be sampled to have x percent chance of finding at least one of the discrepant precincts?" A probability model, widely known as "sampling without replacement," answers this question exactly. Instead of going through the mathematics involved, and reviewing those exact answers, we describe some general features of this model as applied to the post-election auditing context. For a layman's primer on audit mathematics, see the next appendix.

1. **Input:** The total number of precincts, the number of discrepant or miscounted precincts, and the number of precincts audited (i.e., audit size).

2. **Output:** Once the three variables in paragraph 1 are specified, the sampling without replacement model reveals the probability of finding a specific number of discrepant precincts. It is a common auditing approach to discussing detection in terms of finding at least one discrepant precinct, rather than detecting an exact number of discrepant precincts. Since detecting at least one precinct aligns with the practical goals of a post-election audit, this is how we will frame the rest of our discussion.

3. **A few simple rules:**

   (a) For a given total number of precincts and a fixed audit size, a greater number of discrepant precincts creates a greater probability that at least one of them will be detected through the audit.

   (b) For two jurisdictions with different numbers of precincts, an audit size of the same *percentage* of precincts will have an equal chance of detecting the same *number* of discrepant precincts. Thus, for example, if Jurisdiction A has 100 precincts and Jurisdiction B has 1,000 precincts, a five percent audit of both jurisdictions would have an equal chance of detecting twenty discrepant precincts.

   (c) Note that Jurisdiction A has a discrepancy rate of twenty percent, while the discrepancy rate in Jurisdiction B is two percent; yet a five percent audit of both jurisdictions produces the same probability of detecting at least one discrepant precinct.

   (d) For a given discrepancy rate (e.g., twenty percent of precincts have discrepancies), a jurisdiction with a small number of precincts must audit a *higher percentage* of its precincts if it is to have the same chance as a larger jurisdiction of detecting at least one discrepant precinct. In terms of the example in 3.b, for a discrepancy rate of twenty percent and a ninety-five percent probability of finding at least one discrepant precinct, Jurisdiction A must audit a higher percentage of its precincts than Jurisdiction B.

4. **"Confidence level":** The chance of finding at least one discrepant precinct is commonly referred to as the *confidence level*. For example, an audit that is designed to provide a ninety-five percent chance of finding at least one discrepant precinct is said to have a ninety-five percent confidence level. We are making an assumption about the probability of detection with the audit method. This is not "confidence level" as used in hypothesis testing for statistical significance.

B. Estimating the Number of Discrepant Precincts

As discussed in Chapter 4, applying the sampling-without-replacement model to post-election auditing requires a having a way to estimate the number of discrepant precincts, since it is impossible to know in advance how many there will be.

To estimate the number of discrepant precincts:

1. Assume that a switch of more than twenty percent of the votes in any given precinct would be detected without an audit (as previously discussed, *supra* at 77, this is a common assumption made in academic papers that address post-election audits).

2. Then calculate *b* by assuming that there are just enough discrepant precincts (with no more than twenty percent of any given precinct's votes corrupted, as discussed in step 1) to reverse the unofficial margin of victory. In a simple two-candidate race, a switch of twenty percent of the votes in all precincts in a jurisdiction would swing the margin of victory forty percent. This is the maximum overall vote shift; each precinct would show discrepancies. For example, an election whose actual count is sixty-five percent in favor of Candidate A and thirty-five percent in favor of Candidate B would end up as forty-five percent for A, fifty-five percent for B. Stanislevic provides a formula for calculating *b* for an arbitrary vote-switching maximum as well as an algorithm for calculating *b* when precincts are of different sizes.[1]

To summarize, this method specifies the assumed distribution of discrepant precincts that an audit should search for. A race with a relatively narrow margin of victory must be assumed to have few corrupt precincts. Conversely, this method holds that, for a wide-margin race, an audit should be designed to detect a relatively large number of discrepant precincts, because reversing a wide-margin race would require corruption in many precincts.

[1] Howard Stanislevic. *Random Auditing of E-Voting Systems: How Much Is Enough?* 2006. URL: `http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf`.

APPENDIX D

A QUICK PRIMER ON THE MATHEMATICS OF ELECTION AUDITING

(Note: This paper is perpetually in draft form.[1]*)*

D.1 Introduction

There has been a considerable amount of discussion surrounding post-election manual audits of paper records produced by voting systems.[2] One thing is certain: manually counting a small, fixed percentage of paper records is not sufficient for very close races. Stated differently, in close races the number precincts (for example) that could contain discrepancies and affect the outcome of the race become fewer and fewer.

The literature of post-election audits talks about the "confidence" obtained by manually tallying a certain percentage of paper records. But how is this calculated? What are the parameters that go into this kind of a calculation? This short paper answers these questions and aims to give lay persons the mathematical tools they need to calculate the confidence given by a manual audit of a certain percentage of paper records.

[1] This is version 1.2 as of July 20, 2007. The latest version of this paper is always available at: `http://josephhall.org/eamath/eamath.pdf`.

[2] Joseph Lorenzo Hall. *Post-Election Manual Auditing of Paper Records Bibliography*. 2006. URL: `http://josephhall.org/nqb2/index.php/2006/11/26/pea_biblio`.

D.2 Sampling Without Replacement

The problem of calculating the confidence of a certain audit is an application of what is called "detection probability given sampling without replacement". This a fancy way of saying, for example, how probable would it be for you to choose "bad" apples out of a bin of apples (assuming you don't put each apple back in the bin after each choice).

A classic way to set up this kind of problem is to imagine that you have a jar filled with white and black marbles. If you draw 5 marbles, what is the probability that they will all be white (that is, that you don't draw even a single black marble)? Of course, this depends on the number of black and white marbles as well as the total number of marbles.

Mathematically speaking, the probability of drawing a certain amount of white and black marbles is given by an equation called the **hypergeometric distribution**. You don't need to know much about what it is exactly, but to calculate probabilities, you'll need to know how to use it.

Let's say you know there are N marbles total in the jar and that you will draw n (*i.e.*, little "n") marbles from the jar which contains C black marbles. You want to know what the probability is that k out of the n marbles you draw will be black. With these variables, the hypergeometric distribution is typically written like this:

$$f(k;N,C,n) = \frac{\binom{C}{k}\binom{N-C}{n-k}}{\binom{N}{n}} \tag{D.1}$$

Where the things in parentheses are references to something called the **binomial coefficient** (and not matrixes!). The binomial coefficient is calculated like this[3]:

$$\binom{x}{y} = \frac{x!}{y!(x-y)!} \tag{D.2}$$

If we take the equation D.2 and plug it into equation D.1 we get a very nasty looking

[3]The symbol $x!$ means to take the **factorial** of x. The factorial operation in mathematics means to simply multiply an integer by all smaller integers, that is, $x! = 1 \cdot 2 \cdot 3 \ldots x$.

thing:

$$f(k;N,C,n) = \frac{\frac{C!}{k!(C-k)!} \cdot \frac{(N-C)!}{(n-k)!(N-C-n+k)!}}{\frac{N!}{n!(N-n)!}} = \frac{C!n!(N-C)!(N-n)!}{N!k!(n-k)!(C-k)!(N-C-n+k)!} \tag{D.3}$$

Despite its nastiness, you can now, given a jar and a certain number of marbles in two colors, calculate the probability of drawing a certain number of each color of marbles. But, wait... what about elections?

D.3 OK, But What About Elections?

Manually tallying precincts after an election is very similar to our jar with marbles in it. You have a certain number of precincts in total and a certain number of precincts that could contain discrepancies due to tabulation error or fraud. The trick with post-election audits is that you may have no idea how many precincts contain discrepancies (the "corrupt" precincts); that is, you don't know C.

Here's where the closeness of the race in question comes in to the picture. Given the margin in the closest race on the ticket, we can calculate the minimum number of "corrupt" precincts, C, that could change the outcome in that race. That value is:

$$C = \frac{M \cdot N}{2 \cdot m} \tag{D.4}$$

Where M is the margin in the closest race (for a 5% margin this would be 0.05), N is the total number of precincts and m is what is called the within-precinct-miscount.[4] This last value is the largest percentage of votes that could be switched in a precinct and escape detection. That is, we assume that if a precinct traditionally votes for one party, but another party suddenly has an increase of twice this percentage of votes ($2 \cdot m$), the error or fraud would be automatically detected.

[4]See: Kathy Dopp and Ron Baiman. *How Can Independent Paper Audits Detect and Correct Vote Miscounts?* 2005. URL: `http://electionarchive.org/ucvAnalysis/US/paper-audits/Paper_Audits.pdf`. Note that the audit unit might be something other than a precinct (polling place, machine, etc.). More generally, m should be called something like a within-audit-unit-miscount.

So, we now know C and we know N and n (the total number of precincts and the number of precincts we draw for a sample, respectively), what about k? Recall that equation D.1 gives you the probability of drawing k "corrupt" precincts in your sample. In election auditing we want to know what the probability would be that we will detect *one or more* corrupt precincts. That probability is just one minus the probability that we *do not* detect any corrupt precincts ($k = 0$). So, k is zero and we now want one minus the probability in equation D.3.

This simplifies equation D.3 a bit. Setting k to zero, simplifying a bit and subtracting from one gives:

$$1 - f(0;N,C,n) = 1 - \frac{(N-C)!(N-n)!}{N!(N-C-n)!} \tag{D.5}$$

While this final equation is simple compared to the previous ones, you'll probably want to use a software package like Microsoft Excel or OpenOffice to calculate such probabilities. Also, researchers have worked to take the size of precincts into account[5] as well as addressing the problem of how to choose a sample size given a margin and a target confidence level.[6]

D.4 Calculating Probabilities Using Spreadsheet Software

Microsoft Excel and the free software OpenOffice have a special function for the hypergeometric distribution (`HYPGEOMDIST(k,n,C,N)`) that you can use to calculate these kinds of election audit probabilities. You'll have to define each of the parameters k, n, C and N as well as the margin of the race (M) and within-precinct-miscount percentage (m). I've done this for you and have made available both an Excel Spreadsheet (`*.xls`) and Open Document Spreadsheet (`*.ods`). You can find these files here:

[5] Kathy Dopp and Frank Stenger. *The Election Integrity Audit*. National Election Data Archive. 2006. URL: `http://electionarchive.org/ucvAnalysis/US/paper-audits/ElectionIntegrityAudit.pdf`; Howard Stanislevic. *Random Auditing of E-Voting Systems: How Much Is Enough?* 2006. URL: `http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf`; Ron Rivest. *On Auditing Elections When Precincts Have Different Sizes*. 2007. URL: `http://theory.lcs.mit.edu/~rivest/Rivest-OnAuditingElectionsWhenPrecinctsHaveDifferentSizes.pdf`.

[6] Dopp and Stenger, see n. 5; Ron Rivest. *On Estimating the Size of a Statistical Audit*. Available at: `http://theory.csail.mit.edu/~rivest/Rivest-OnEstimatingTheSizeOfAStatisticalAudit.pdf`. 2006.

- Excel: `http://josephhall.org/eamath/eamath.xls`
- OpenOffice: `http://josephhall.org/eamath/eamath.ods`

Appendix E
Procedures for the 1% Manual Tally in California

(Note: If using this appendix as a guide or recipe, readers should have the most current version.[1]*)*

E.1 Purpose of This Document

For many California counties, the November 2006 General Election was one of the first elections in which they used Direct Recording Electronic (DRE) voting systems with Voter-Verified Paper Audit Trail (VVPAT) capabilities. In addition to the complexities of changing all or parts of their voting system, counties also had to include VVPAT records in the 1% manual tally (manual audit) mandated by law, in which tallies of paper records of ballots cast in polling places must be reconciled with the electronic tallies from the equipment on which the ballots were cast.[2] In an effort to help a number of California counties think about the proper process and necessary changes involved with this 1% manual tally, members of ACCURATE, the Verified Voting Foundation, and the California Voter Foundation have de-

[1] This version current as of April 24, 2008 (v13). The most current version of this document is available at: `http://josephhall.org/procedures/ca_tally_procedures-2008.pdf`. An editable version—at least, *more* editable—of this document is also available in Rich Text Format: `http://josephhall.org/procedures/ca_tally_procedures-2008.rtf`.

[2] The "one percent manual tally" is defined in Sec. 336.5 of the CA Elec. Code as: "[The] public process of manually tallying votes in 1 percent of the precincts, selected at random by the elections official, and in one precinct for each race not included in the randomly selected precincts. This procedure is conducted during the official canvass to verify the accuracy of the automated count.

Elections Code Sec. 15360 states how to conduct the conduct the manual tally: "During the official canvass of every election in which a voting system is used, the official conducting the election shall conduct a public manual tally of the ballots tabulated by those devices, including vote by mail voters' ballots, cast in 1 percent of the precincts chosen at random by the elections official. If 1 percent of the precincts is less than one whole precinct, the tally shall be conducted in one precinct chosen at random by the elections official. . . . "

veloped this policy document in direct consultation with the staff of these Counties.[3] We hope that this document will help other counties develop their own policies, processes and best practices going forward.

This document is structured as partially a narrative rationale with a set of procedures for conducting the 1% manual tally. Section E.2 describes the nature of the manual tally in the larger canvass process. Section E.3 covers the legal requirements for performing the manual tally, the random selection process and the role and responsibilities of observers. The procedures for the manual tally are presented in section E.4. Finally, section E.5 outlines the prerequisites for the final certification of the vote.

E.2 Canvass

The 1% Manual Tally is one part of a more complicated post-election counting and reconciliation process called the Official Canvass of the Vote. The Official Canvass of the Vote is strictly governed by the California Elections Code.[4] The canvass shall commence no later than the Thursday following the election, shall be open to the public, and, for state or statewide elections, shall result in a report of results to the Secretary of State. The canvass shall be continued daily, Saturdays, Sundays, and holidays excepted, for not less than six hours each day until completed, and it must be completed within 28 calendar days after the election.[5] The components tasks of the official canvass are provided in the Code, and additional requirements are specified by guidelines from the Secretary of State. Tasks of the Official Canvass The official canvass shall include, but not be limited to, the following tasks (these apply to all votes, precincts, etc., not just the 1% sample):

(a) An inspection of all materials and supplies returned by poll workers.

(b) A reconciliation of the number of signatures on the roster with the number of ballots recorded on the ballot statement.

[3] We worked closely with San Mateo and Yolo counties and more indirectly with Alameda and Marin Counties. See: Joseph Lorenzo Hall. "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures". In: *USENIX/ACCURATE Electronic Voting Technology Workshop 2008* (July 2008). URL: http://josephhall.org/papers/jhall_evt08.pdf

[4] CA Elec. Code Sec. 15300 et seq.

[5] CA Elec. Code Sec. 15302, Sec. 15372

(c) In the event of a discrepancy in the reconciliation required by subdivision (b), the number of ballots received from each polling place shall be reconciled with the number of ballots cast, as indicated on the ballot statement.

(d) A reconciliation of the number of ballots counted, spoiled, canceled, or invalidated due to identifying marks, overvotes, or as otherwise provided by statute, with the number of votes recorded, including absentee and provisional ballots, by the vote counting system.

(e) Processing and counting any valid absentee and provisional ballots not included in the semifinal official canvass.

(f) Counting any valid write-in votes.

(g) Reproducing any damaged ballots, if necessary.

(h) Reporting final results to the governing board and the Secretary of State, as required.

E.3 One Percent Manual Count

When a voting system is used to count votes, the official canvass must also include a manual tally of a portion of the total votes cast, as a means of verifying the accuracy of the system count. The Elections Code specifies how the tally is performed:

Section 15360. Manual Tally When Using a Voting System

(a) During the official canvass of every election in which a voting system is used, the official conducting the election shall conduct a public manual tally of the ballots tabulated by those devices, including absent (vote by mail) voters' ballots, cast in one percent of the precincts chosen at random by the elections official. If one percent of the precincts is less than one whole precinct, the tally shall be conducted in one precinct chosen at random by the elections official.

In addition to the one percent manual tally, the elections official shall, for each race not included in the initial group of precincts, count one additional precinct. The manual tally shall apply only to the race not previously counted.

Additional precincts for the manual tally may be selected at the discretion of the elections official.

(b) If absent (vote by mail) ballots are cast on a direct recording electronic voting system at the office of an elections official or at a satellite location of the office of an elections official pursuant to CA Elec. Code Sec. 3018, the official conducting the election shall either include those ballots in the manual tally conducted pursuant to subdivision (a) or conduct a public manual tally of those ballots cast on no fewer than one percent of all the direct recording electronic voting machines used in that election chosen at random by the elections official.

(c) The elections official shall use either a random number generator or other method specified in regulations that shall be adopted by the Secretary of State to randomly choose the initial precincts or direct recording electronic voting machines subject to the public manual tally.

(d) The manual tally shall be a public process, with the official conducting the election providing at least a five-day public notice of the time and place of the manual tally and of the time and place of the selection of the precincts to be tallied prior to conducting the tally and selection.

(e) The official conducting the election shall include a report on the results of the one percent manual tally in the certification of the official canvass of the vote. This report shall identify any discrepancies between the machine count and the manual tally and a description of how each of these discrepancies was resolved. In resolving any discrepancy involving a vote recorded by means of a punchcard voting system or by electronic or electromechanical vote tabulating devices, the voter verified paper audit trail shall govern if there is a discrepancy between it and the electronic record.

E.3.1 Random Selection of the Precincts for the Manual Tally

The random selection and manual tally *must* take place only after unofficial counting has been completed. This is important because attackers intent on hiding evidence of fraud (or

simple error) will have the opportunity to change vote totals in precincts they know will not be audited, once the random selection is complete.[6]

The random selection of precincts for the Manual Tally shall be conducted in a publicly verifiable, random selection process. The date and time for the selection of precincts will be announced in advance via press release, or comparable methods.

The materials for the random selection include:

- Master Selection Spreadsheet—A spreadsheet of precinct numbers. This spreadsheet simply consists of two columns: one column listing integers from 0 to the number of precincts and another column listing each precinct's identifier or precinct number.

- Contest Selection Spreadsheets—Spreadsheets listing an integer index and the precinct numbers for the precincts that are permitted to cast ballots in each race an measure in the election.

- A publicly verifiable random selection mechanism—We recommend using three clear, colored, 10-sided dice (red, white, and blue).[7]

The presiding election official should announce the number of precincts in the jurisdiction and the number of precincts that will be chosen for audit. To assure themselves of the legitimacy of the selection materials, the observers will be allowed to inspect the dice, the cup, and the box, (or similar items when using a different random selection mechanism) and to compare the observers' copies of the spreadsheets to the official copies.

The election official (or an observer) will roll all the dice once to select each precinct to be audited. If a precinct row number is chosen that doesn't exist, the dice will be rolled

[6] Large jurisdictions or jurisdictions that have very tight canvass timelines might not be able to wait until all unofficial counting is completed for all types of ballots. In these cases, we suggest using each ballot type as a sampling stratum and sampling ballot types as soon as unofficial counting is complete. See: Hall, "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures", see n. 3; Philip B. Stark. "Conservative Statistical Post-Election Audits". In: *The Annals of Applied Statistics* 2 (2008). 550–581. URL: http://arxiv.org/abs/0807.4005

[7] Some jurisdictions would prefer a publicly verifiable selection method that does not use dice, for example using a rotating hopper and numbered balls. For more on methods of publicly verifiable random selection, see: Arel Cordero, David Wagner, and David Dill. "The Role of Dice in Election Audits—Extended Abstract". In: *IAVoSS Workshop on Trustworthy Elections 2006 (WOTE 2006)* (June 2006). URL: http://www.cs.berkeley.edu/~daw/papers/dice-wote06.pdf

again.[8] If a die falls off the table or otherwise misses the box or designated location, the dice will be rolled again. When a valid roll is made, the election official will read off the digits from the roll and record and witness the precinct row number in the master spreadsheet. The election official should then identify each precinct chosen on the contest spreadsheets to keep track of the contests included in the Manual Tally.[9]

After the initial one percent of precincts is chosen, additional precincts will be chosen so as to include all contests in the election.[10]

When finished with the random selection process, the presiding election official should publicly announce the precinct row numbers, precinct numbers and whether or not the selection of that precinct was off of the master spreadsheet or a contest spreadsheet. To preserve the chain of custody of materials to be tallied in the manual count, the retrieval of ballot materials for the tally should happen as quickly as possible after the random selection is complete.

E.3.2 Observers

The manual tally will be conducted in public view. All interested parties are welcome to observe.

Observers must sign in with the jurisdiction's reception desk. Each observer will receive a visitor's badge, to be worn by the observer at all times while in the elections facility—in order to distinguish them as observers to tally staffers—and the observer group shall be accompanied by at least one elections staff member at all times. No observer shall interfere with the orderly process of any phase of the canvass. Observers shall not touch ballots or interfere in any way with the counting, but observers will be permitted to watch the process in a manner that allows them to meaningfully verify the count. Before and during the pro-

[8] In some cases, many rolls will not correspond to a valid precinct. We've developed a small computer program that can be used to "bin" the random numbers to maximize the chance of a good roll: Joseph Lorenzo Hall. *Dice Binning Calculator for Post-Election Audits*. Mar. 2008. URL: `http://www.josephhall.org/dicebins.php`

[9] If using a selection method other than 10-sided dice, the jurisdiction will need to have procedural rules such as those in this paragraph to specify the exact rules for what does and does not count as a valid selection.

[10] Note that this isn't technically required by California law. That is, the law doesn't require jurisdictions to choose the additional precincts past the 1% selection in a random manner. However, we feel this is best practice and highly recommend it. For this process, the Dice Binning Calculator mentioned in n. 8 is highly recommended.

cess, observers may quietly ask questions of the attending supervisor or manager, but are prohibited from directly communicating with any member of the tally board.[11] Once the tally is started, no disruptive conversation or comments are allowed in the observation area. Observers may submit questions or comments in writing to the Tally Supervisor throughout the counting process.

E.4 Manual Tally Procedures

The members of the manual tally board are selected from elections office staff and poll workers, but no poll worker may serve on the board if the pollworker served at a precinct that has been randomly selected for the tally.

The manual count of paper records should be a blind count. Those doing the counting should be unaware of the "expected" result (i.e., of the electronic tallies) or they might have a conscious or unconscious incentive to arrive at the "expected" result. The tally board is kept "blind" to the preliminary results obtained in the voting system count until the tally process is complete; to ensure accuracy, the Tally Supervisor holds this information in private. The Tally Supervisor rules on any changes to be made to the preliminary system totals.

The tally board receives the list of randomly selected precincts that it will be tallying, from which it prepares the tally sheets.[12] An Adjustment Log is used to document the any necessary changes in the system count as a result of the manual tally.[13]

California law requires that vote-by-mail ballots be included in the manual tally. This requires the elections official to either sort vote-by-mail ballots by precinct or be able to quickly locate the vote-by-mail ballots for chosen precincts after the selection has been completed. For large counties, searching through batches of ballots for all vote-by-mail ballots corresponding to a list of a dozen or so chosen precincts is impractical, and these counties should sort their vote-by-mail ballots by precinct. For smaller counties, searching

[11] This is very important. We have observed cases where observers communicated vote totals to the tally team, breaking the "blind count" rules for the tally.

[12] Some counties wisely choose to pre-fill electronic tally sheets so that the tally board doesn't have to do this step by hand. We recommend this especially in large counties where this might consume a large amount of tally board staff time.

[13] Some counties do not change their totals based on the totals from the manual count. These counties stress that the manual tally is "not a recount" so vote totals should not change. Whatever the interpretation of the manual tally laws, the jurisdiction needs to, at a minimum, report discrepancies that they find.

through batches of vote-by-mail ballots might be a viable option if they don't find it to be too time-consuming or difficult.

The ballots and other paper records for the selected precincts are located and removed from storage areas. The storage seal is verified,[14] broken and the ballots are removed, and, if the full ballot consists of more than one ballot card, the cards are separated. The board will count the number of ballot cards and the number of votes. Any discrepancies from the system count will be investigated and reconciled and logged.

One final note before we get into specific procedures. The following procedures assume a cut-sheet sort-and-stack counting methodology; that is, VVPATs are cut individually off of their rolls before counting in stacks. If the jurisdiction uses reel-to-reel VVPAT technology, it should consider cutting any VVPAT records off their rolls. This will make the VVPAT records much easier to recount. To do this, have one person on the tally team hold the paper roll, one person pull out one ballot on the VVPAT tape and another cut and stack the VVPAT records. The final tally team member should serve as an observer in order to make sure the process is witnessed and that no VVPAT records are misplaced, mis-cut, etc. Be careful to retain valid and voided VVPAT records but set the voided records aside. If the VVPAT roll cannot be sliced, the reader will have to roll and unroll the VVPAT tape. We strongly suggest that jurisdictions cut VVPATs off the roll, unless they are only counting one race per precinct and have past experience with rolling and unrolling VVPAT rolls during a recount and/or tally.

E.4.1 Preparation

A considerable amount of preparation is needed for a smooth and sound manual tally. The following steps take place anywhere from a few months to directly before the manual tally.

[14] In order to preserve the chain of custody on the paper records, the reader in each tally team should check the tamper-evident seals on paper record containers, VVPAT canisters, etc. against the appropriate seal log in front of the rest of the tally team acting as witnesses, before beginning the tally. The reader should then break the seal and place the paper records on the tally table in full view of observers.

Review Last Tally Experience

1. Months before the next election, the Jurisdiction should review their experience tallying the last election:

   (a) Identify any problems that resulted in discrepancies or inefficiencies and address them in procedural changes, poll worker training, revision of the technology, etc.

   (b) Changes in procedures should be done carefully. Technical changes, such as to the method of random selection, should be reviewed by domain experts.[15]

Procedural Commitments

1. In election planning, many months before an election, special care should be taken to ensure that the voting system and poll workers are capable of keeping the evidence necessary for the 1% manual tally. The jurisdiction needs to design policies and procedures that ensure that a paper record that can be included in the manual tally is stored for each ballot that is cast.

   (a) Ensure that their voting systems will not allow electronic ballots to be cast when the VVPAT subsystem is not operational or not recording VVPATs.

   (b) Ensure that poll worker documentation and training emphasizes that the VVPAT records are equally as important as the memory card "ballot boxes" and that there are clear guidelines about what to do in case of a printer jam, failure or other contingency that might affect the paper record of a voter's ballot.

2. At least one week before the selection and manual audit tally process, the jurisdiction should publish the policy and procedures that will govern the selection and audit tally process:

   (a) The tally should be the very last step before certifying the vote.

   (b) The jurisdiction should include all types of ballots in the manual tally.

[15] Note that we have observed cases in which very small changes in procedures resulted in drastic effects on the integrity of the process. See: Joseph Lorenzo Hall. *Research Memorandum: On Improving the Uniformity of Randomness with Alameda County's Random Selection Process.* UC Berkeley School of Information. Mar. 2008. URL: `http://josephhall.org/papers/alarand_memo.pdf`

(c) The selection of precincts for the manual audit and the manual audit tally for classes of ballots (precinct-machine, precinct-provisional and absentee) should only begin after those ballots have been counted.

(d) Precinct Totals Master List. The jurisdiction will need to publish electronic tallies for ballots being audited before the random selection of precincts is performed.

i. The jurisdiction could run an unofficial Statement of Vote (or other report that shows the totals for ballots by precinct in numbers that make sense for the tally) and make it available on their web site in both PDF and CSV formats. They could also hand it out on write-once media (CD-ROM or DVD-ROM) to observers.

ii. This should be done before the start of the random selection, to make certain that the tally is committed to a single set of tallies and cannot be changed depending on which precincts are chosen.

(e) The manual count of paper records should be a blind count:

i. Those doing the counting should be unaware of the "expected" result (i.e., of the electronic tallies) or they might have a conscious or unconscious incentive to arrive at the "expected" result.

ii. The reader during the manual tally tally process should not tell the recorders the expected result.

Personnel

1. Depending on the different paper records produced by a jurisdiction's voting systems (e.g., precinct paper ballots, VVPATs, vote-by-mail), it should set up a series of tally areas. Each tally area is assigned two permanent employees from the County Elections Office. These staff will be appointed as the Canvass Board by the Chief Elections Official, and are responsible for decision-making and documentation.

2. Seasonal temporary workers or poll workers will be assigned to work in one of the three areas. Hours of counting will be within their scheduled workdays.

3. Each tally board will have four members:

   (a) One **Reader** who calls out the voter's choice in a given contest: "Yes", "Yes.", "Yes" or "Lincoln", "Lincoln", "Lincoln"

   (b) One **Witness** who watches that the reader to confirm the voting choice as voted. The Witness also collates the ballots into groups of 10.[16]

   (c) Two **Talliers**, who tally the votes being called out using tally sheets.[17]

Facilities

1. Each of the tally areas will have its own designated area. In the case of a small election, the tally may be consolidated into one room.

2. The areas will need to have enough room to accommodate two large tables for the supervisors, and a table and four chairs for each of the tally teams.

3. Elections Officials will need access to precinct paper ballots, VBM ballots, provisional ballots, spoiled ballots and remade ballots.

4. Boxes of ballots, VVPAT rolls and vote-by-mail mail trays will need to be staged on separate tables.

5. Note that voting systems that print their totals tape on the VVPAT roll require additional processing to preserve the blind count of the tally team. In the case of the totals tape printed on the VVPAT roll—such as in the case of Sequoia's AVC Edge DRE with VeriVote printer or ES&S' iVotronic with RTAL—the VVPAT rolls should be removed from their canisters or printer housing in a separate staging area. This will preserve the blind counting rule.[18]

6. Provide a tally board schedule indicating actual counting hours, lunches and breaks.

[16] The Witness has two other very important duties: 1) the witness must be comfortable enough to stop the tally when their reading of a ballot choice differs from what the reader calls out; and, 2) the witness must roll back the tally by 10 ballots if the two talliers fail to both call out a multiple of ten or begin to tally out of sync.

[17] To see examples of tally sheets used in San Mateo and Marin Counties, respectively, see: `http://www.flickr.com/photos/joebeone/2240342264/sizes/l/` and `http://www.flickr.com/photos/joebeone/2266221884/sizes/l/`.

[18] See section E.4 for a discussion of blind counting.

Reports and Supplies

1. Staff is to be provided with print outs of the manual tally procedures and other instructions they may need (e.g., instructions for removing VVPAT rolls from their canister or printer housing).

2. Prepare and provide spreadsheets and reports to appropriate supervisors

   (a) Reports to be printed from the vote count software system (the Election Management System)

      i. Precinct Turn-out Report—a report listing the number of voters of each party that cast ballots in the election in the precinct.

      ii. Precinct Totals Report—a report listing the totals for each option on the ballot, including undervotes and overvotes.

      iii. Precinct Write-in Report—a report listing the results for write-ins cast in the precinct.

      iv. Provisional Count/No Count Report—a report listing the number of provisional ballots cast in the precinct, their disposition and any identifying information needed to separate out anonymous, valid provisional records from invalid records.[19]

      v. Precinct vote-by-mail Report—a results report for vote-by-mail ballots, including overvotes and undervotes.

      vi. Precinct Canvass Report—a report listing the number of ballots of each type counted in the canvass.

      vii. Others as necessary

   (b) It can be helpful to create a spreadsheet that contains a number of different resources. A spreadsheet (e.g., called "1% Manual Precinct Reports") could contain many of the checklists and reports required.

[19] If the jurisdiction's voting system allows casting provisional ballots on DREs in precincts other than the precinct the DRE is located, this provisionals report should be supplemented by a list of precincts in which DRE provisionals were cast so that those provisional ballot paper records can be located and included in the tally.

i. Adjustment Log Template—for any needed adjustments to the unofficial count after the tally, if applicable.

ii. VVPAT Summary Sheet—a log containing the list of VVPAT printer serial numbers, security seal serial numbers, security-tape-intact verification field.

iii. Precinct Selection List—list of selected precincts.

iv. Supply List—list of supplies needed per tally team.

v. Polling Location List with precinct numbers and consolidations.

vi. Tally team assignments and schedule.

vii. Linear Reports—lists showing which precincts vote for which contests on the ballot for this election.

viii. Precinct Summary Report—listing precinct number, number of physical ballot boxes (if applicable), VVPAT serial numbers, number of DRE ballots cast, number of paper ballots cast, number of vote-by-mail ballots cast, total number of ballots cast, notation or reference to spreadsheet with serial numbers of other voting system equipment that interacts with precinct equipment.

3. Supplies, additional to supply list above or in the Supply List

   (a) No ballot marking pens are to be in the immediate vicinity of the tally area.[20]

   (b) Mail trays for tally teams with all supplies such as adjustment logs, tally sheets, staplers, etc.

   (c) At the discretion of the supervisors: mail trays and file folders for required reports, observer guidelines, team lists, office cell phone, election code book.

E.4.2 The Tally

When preparations are completed and the random selection is finished, the tally begins.

1. Obtain ballots to be tallied:

   (a) Precinct paper ballots from both polling place and provisional.

[20] Pens that could indelibly mark ballots should never enter the tally area. Such marking instruments could be used, inadvertently or intentionally, to change voted ballots.

(b) VVPAT tape: (paper-trail) from each DRE.

(c) Vote-by-mail ballots

(d) Paper records from provisional ballots cast on DREs.[21]

2. Prepare for the tally.

(a) Obtain all ballots for that precinct.

(b) Within each precinct, divide the ballots by ballot card if using a multi-page ballot.

(c) Count quantity of voted ballots in that precinct and check the aggregate totals with the Tally Supervisor.

(d) Within each contest, divide the ballots by candidate or option (for measures).

(e) For each contest separate over-voted and under-voted/blank ballots. Set aside. These will not be a part of the tally but can be helpful during the tally process.

3. Begin the tally. Tally all ballots for one candidate/option before moving to the next candidate (or option).

(a) On the tally sheet write the names of the candidates (or choices for measures) in the order in which they appear on the ballot.

(b) The Reader calls out the name of the candidate/choice to be tallied.

(c) The Witness watches to make sure the Reader reads correctly and collates the ballots, cross-stacked in groups of ten (10).[22]

(d) The two remaining team members mark their own tally sheets each time the name (or option) is called.

4. After every tenth tally mark, the two team members doing the tally will call out: "10", "20", etc. Switch the direction of the hash mark at every line.[23]

---

[21] See discussion in n. 19.

[22] By "cross-stacking" we mean stacking groups of 10 ballots while changing the orientation of each group by 90 degrees (from portrait to landscape orientation and back again).

[23] Talliers have tally sheets (see n. 17) with numbers written on them (1, 2, 3,...) in rows. The tallier draws a line through each number (a "hash mark") when the reader reads a candidate choice or option. When the tallier has to move to the next line (after 50, for example), they should switch the direction of the hash mark for clarity.

(a) If the team members are out of sync, go back to the last multiple of ten that was in sync, not to the beginning.

(b) Talliers announce and mark the last number tallied and line out the rest of the numbers on that line for that candidate (or option). 'X'-out the rest of the tally box. Write the total in the column to the right—both in number and written form.

(c) Completion of that Contest: call a supervisor to verify totals tallied against the system results. Discrepancies shall be justified, resolved, and recorded on the Tally Summary Sheet. If no changes are made, record that as well. If necessary the race is manually re-tallied. (See 7b for more on resolving confirmed discrepancies.)

5. Moving to the Next Contest.

(a) When each contest is complete, draw a line through the next "candidate" row. That will separate one contest from the next.

(b) Sign and certify the bottom of each tally sheet.

(c) The tally team may use many tally sheets for one precinct, depending on the number of contests and the number of candidates/options in the contest.

(d) Number the pages on the bottom right hand side. Do not commingle two sets of tally sheets.

(e) The tally board may not proceed with another precinct unless all required contests have been tallied and all discrepancies are resolved.

6. Tally Supervisor Duties

(a) Review the certified tally sheets and placed them in a manila envelope. Once all precincts have been tallied for that contest, discrepancies will be noted on the Adjustment Log.

(b) Use the Adjustment Log as needed (e.g., voter's intent clearly seen by tally board but not by system). Any ballot resulting in an adjustment will be kept separate from other ballots for that precinct. The log shall consist of:

i. The manual count procedure documentation.

ii. Results of each round of manual counting for each precinct in the sample.

iii. How discrepancies were resolved.

iv. A detailed account of any actions taken which are contrary to written protocols.

v. The log must be made available to the public.

(c) Tape the Summary Sheet to the front of the envelope.

7. Resolving or Justifying Discrepancies:

(a) Resources available to resolve discrepancies: Ballot Accountability Report,[24] Polling Place and Consolidation Lists, Spoiled and Surrendered Ballots, Official Rosters, Access to Provisional Envelopes (both Counted and Not Counted), Vote By Mail ballots.

i. Undervotes, overvotes, and canceled/voided DRE ballots must be tracked and reported as part of the manual count process. (Spoiled ballots are not included here, because they are not electronically tallied. However, since spoiled ballots are re-created and then electronically tallied, the re-created ballots become part of the manual count if they come from precincts in the manual count sample.)

(b) If a discrepancy is confirmed by the supervisor, an additional re-count is conducted.

i. If the discrepancies between the final manual count and the electronic count still exist, election officials must take the following steps to resolve the discrepancies:[25]

A. The percentage of discrepancies found in the manual count sample for a given race must be presumed to exist in the remaining ballots cast in the

[24]The Ballot Accountability Report is a spreadsheet reconciling the amount of ballot materials sent to each precinct, the amount returned, spoiled, etc.

[25]These requirements are derived from the California Secretary of State's post-TTBR post-election audit requirements. See: *Post-Election Manual Tally Requirements*. California Secretary of State. Oct. 2007. URL: http://www.sos.ca.gov/elections/voting_systems/ttbr/post_election_req.pdf

race.

B. Supervisor shall calculate the discrepancy percentage for each race by comparing the total number of discrepancies found in the manual count sample for the race to the total ballots cast for that race in the manual count sample.

C. If the discrepancy percentage represents 10% (one-tenth) of the margin of victory for that race, then additional precincts must be manually counted for that race. Additional precincts must be counted in randomly sampled blocks of 5% until the total number of discrepancies presumed to exist—re-calculated using the method above—is smaller than 10% of the overall margin of victory in that race tallied electronically.

D. If any discrepancy is found between manually counted VVPAT records and corresponding electronic vote counts that cannot be accounted for by some obvious mechanical problem, then all relevant VVPAT records, memory cards and devices, and DRE machines must be preserved and the Secretary of State must be notified in order to allow for a technical investigation to determine the cause of the problem.

E. For multi-winner elections, the margin of victory is the difference between the candidate (or option) who had just enough votes to win a seat and the next candidate below. For example, for a race with three open seats, the margin of victory would be the difference between the third and fourth place candidates.

ii. Prepare Discrepancy Reports according to the "Post-Election Manual Tally Log" from the Secretary of State.[26]

E.5 Certification

The election is prepared to be certified upon completion of the following:

[26] *Post-Election Manual Tally Log: Suggested Instructions for Post-Election Manual Tally Requirements (CCROV-08048)*. California Secretary of State. 2008. URL: `http://josephhall.org/ccrov/CCROV-08048.pdf`.

1. All rosters are reconciled with vote totals.[27]

2. All votes are tallied in the EMS, including any manual adjustments as needed based on the manual tally, if applicable.

3. Canvass Report is printed and proof-read.

4. Statement of the Vote is printed and ready for certification by the Chief Elections Officer.

5. Official certified results are adopted by the governing bodies of the election, such as the County Board of Supervisors, City Councils, School Boards and other Special District governing boards.

6. In statewide elections, certified results are reported to the Secretary of State.

[27] San Mateo uses a "Master Ballot Accountability Spreadsheet" to aid this reconciliation.

APPENDIX F

CREATIVE COMMONS LICENSE

This is the text of Creative Commons' Attribution-NonCommercial-NoDerivs License, version 3.0.[1]

F.1 License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. **Definitions**

   (a) **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with one or more other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

[1] *See:* `http://creativecommons.org/licenses/by-nc-nd/3.0/us/`.

(b) **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

(c) **"Licensor"** means the individual, individuals, entity or entities that offers the Work under the terms of this License.

(d) **"Original Author"** means the individual, individuals, entity or entities who created the Work.

(e) **"Work"** means the copyrightable work of authorship offered under the terms of this License.

(f) **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. **Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. **License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

(a) to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works; and,

(b) to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved, including but not limited to the rights set forth in Sections 4(d) and 4(e).

4. **Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

(a) You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of a recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. When You distribute, publicly display, publicly perform, or publicly digitally perform the Work, You may not impose any technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by Section 4(c), as

requested.

(b) You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

(c) If You distribute, publicly display, publicly perform, or publicly digitally perform the Work (as defined in Section 1 above) or Collective Works (as defined in Section 1 above), You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear, if a credit for all contributing authors of the Collective Work appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this clause for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Au-

thor, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

(d) For the avoidance of doubt, where the Work is a musical composition:

i. **Performance Royalties Under Blanket Licenses.** Licensor reserves the exclusive right to collect whether individually or, in the event that Licensor is a member of a performance rights society (e.g. ASCAP, BMI, SESAC), via that society, royalties for the public performance or public digital performance (e.g. webcast) of the Work if that performance is primarily intended for or directed toward commercial advantage or private monetary compensation.

ii. **Mechanical Rights and Statutory Royalties.** Licensor reserves the exclusive right to collect, whether individually or via a music rights agency or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions), if Your distribution of such cover version is primarily intended for or directed toward commercial advantage or private monetary compensation.

(e) **Webcasting Rights and Statutory Royalties.** For the avoidance of doubt, where the Work is a sound recording, Licensor reserves the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions), if Your public digital performance is primarily intended for or directed toward commercial advantage or private monetary compensation.

5. **Representations, Warranties and Disclaimer**

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND ONLY TO THE EXTENT OF ANY RIGHTS HELD IN THE

LICENSED WORK BY THE LICENSOR. THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MARKETABILITY, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. **Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Termination**

   (a) This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works (as defined in Section 1 above) from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

   (b) Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. **Miscellaneous**

(a) Each time You distribute or publicly digitally perform the Work (as defined in Section 1 above) or a Collective Work (as defined in Section 1 above), the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

(b) If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

(c) No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

(d) This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

F.2 Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark “Creative Commons” or any related trademark or logo of Creative Commons without the

prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of this License.

Creative Commons may be contacted at `http://creativecommons.org/`.