

Probing the Front Lines: Pollworker Perceptions of Security & Privacy

Joseph Lorenzo Hall¹, Emily Barabas², Gregory Shapiro², Coye Cheshire², Deirdre K. Mulligan²

¹*New York University; Department of Media, Culture and Communication*
joehall@nyu.edu

²*University of California, Berkeley; School of Information*
[emilybarabas,gshapiro,coye,dkm]@ischool.berkeley.edu

Abstract

Voting technologies have undergone intense scrutiny in recent years [17]. In contrast, the human components of these socio-technical systems, including the policies and procedures that guide and bind behavior have received less attention. To begin to understand pollworker behavior, we conducted a two stage qualitative investigation in a single jurisdiction to explore the challenges pollworkers face on election day, their recollection of relevant policies and procedures, and their high-level ability to perceive and remedy threats to security and privacy whether they relate directly to policies and procedures or not. We first observed 4 polling places in one California county¹ during the general election in November 2010, recording security and privacy related events. Based on our observations we developed 10 “vignettes” [16], each focusing on a privacy or security risk that we witnessed. In August 2011, we used this instrument to interview twenty pollworkers — recruited from the four polling places we observed the previous year and four additional demographically-similar polling places — in order to understand how they would respond to the vignettes. We report 1) qualitative findings from our observations; and, 2) qualitative findings from our vignette-based interviews of pollworkers. We find that awareness of security-related policies and procedures and comprehension of security risks is low compared with privacy policies, procedures and risks. We find divergent polling place management styles, which we tentatively suggest relate to different perspectives on risk management and trust. We propose that training materials be oriented around the risks they are designed to address, to promote pollworkers’ general knowledge of risks to election integrity as well as the specific policies their roles support in order to mitigate risks on election day.

¹ We cannot name the county with which we worked due to the time-sensitivity of our findings during an election year.

1 Introduction

Every election, tens of thousands of pollworkers become the frontline of election security and privacy in thousands of polling sites scattered across the country. These “engines of democracy” are socio-technical systems — that is, humans and machines working together to facilitate and protect democratic values, such as privacy and security, in the name of free and fair elections. Thousands of temporary staffers — pollworkers — are hired to administer polling places under the supervision of a poll inspector (PI). Officials entrust pollworkers with the responsibility of running a polling place from start to finish — from picking up election day supplies to dropping off voted materials on election night. Pollworkers receive training on policy and procedures — either through a training class or while on the job — designed to ensure the security, privacy, accuracy, and integrity of the election. Given their relative autonomy and importance, pollworker knowledge of policies and procedures directly influences whether these values are translated into practice during an elections. Election officials rely upon pollworkers to police themselves and implicitly each other. Because policies and procedures are inherently incomplete and constantly changing, pollworkers that have more general knowledge and understanding of threats and mitigations will be more effective at responding to known and unknown threats.

Research has shown that voters value smooth, efficient and user-friendly elections and view them as well-run elections (*See* § 2). However, voters have limited knowledge of privacy and security threats to voting systems and the policies designed to mitigate them, therefore elections may be *perceived* as well run — and in fact be largely efficient and smooth — but contain security and privacy flaws.

We sought to probe pollworker awareness and knowledge of privacy and security issues, specific risks, and policies and procedures designed to mitigate them

through observations and interviews.

This paper proceeds as follows: Section 2 provides a review of relevant literature; Section 3 describes our two-part methodology of observation and interviews; Section 4 presents our findings; and, Section 5 synthesizes and analyzes these findings and offers some tentative recommendations.

2 Literature Review

A small but growing area of academic research examines pollworkers and their role in the election process. This research tends to show that pollworker training is a critical part of a successful election, and, in particular, that pollworker confidence and knowledge contributes to voter confidence and trust in both the process and the outcome of an election.

2.1 Training of Pollworkers

Proper pollworker training is important to effective election administration. Inadequate training jeopardizes the success of an election [2, 3, 13, 21]. Poorly trained pollworkers can be a significant source of error — moving ballots and ballot boxes improperly, erasing and changing records, giving out incorrect instructions, hovering over people voting in booths, and transporting sensitive materials without proper supervision [23]. Proper training must cover all relevant voting technologies. Hands-on training with voting equipment can increase pollworkers' confidence and performance on election day [13].

Optical scan voting technology — the technology that is currently being used for polling place voting in most California counties,² is the dominant polling place voting technology in the US [5]. Optical scanners can cause errors or facilitate fraudulent manipulation of results if not properly calibrated, managed, maintained and secured [6, 20].

Certain pollworkers in California — Chief Poll Inspectors (Chief PIs) — are required to attend training, while the law is ambiguous towards the training of other pollworkers (Clerks).³ Survey research finds that more than 20% of pollworkers in California report having not attended training classes.⁴ In a separate

analysis, Glaser et al. found that training can bolster pollworker confidence, and can compensate for lack of experience. The quality and type of pollworker training, and the availability of reference materials improved pollworker confidence despite lack of experience [10].

2.2 Voter Confidence in Pollworkers

The literature also reports that voter confidence in the security and integrity of the election process correlates with expressions of confidence in specific pollworkers and polling place operations [8, 14]. The more helpful and competent pollworkers are, the stronger the confidence that votes will be successfully counted [3].

The overall efficiency of the voting process affects voter assessment of pollworkers. A 2008 study found that voter perceptions of pollworkers was related to the amount of time that it took to complete the voting process: the longer it took, the more negative the evaluation of the pollworker [8].

2.3 Voting System Security and Privacy

Researchers have found that the security and integrity of a voting system can depend on the pollworkers' ability to follow specific procedures, and that pollworker fidelity to those specific instructions is more essential to the security of voting systems than current technical mechanisms that might exist to protect them [4, 6, 12, 20]. This research finds that seals and other physical mechanisms currently imposed upon voting systems can be bypassed easily, placing increased pressure on pollworker-mediated procedures.

Cumulatively, this research finds that: pollworkers are an essential element of elections; pollworker adherence to policies and procedures significantly affects these system properties; training improves the confidence and competence of pollworkers; and, pollworker performance affects both public perception of elections as well as the technical level of vulnerability.

Our work is designed to provide insight into the security and privacy issues arising on election day, and how well pollworkers handle them based on awareness and knowledge of governing policies and procedures.

3 Methodology

We employed a two-part methodology to study risks,

Elections in California, 77.3% attended formal training. The primary reason for the 22.7% who did not attend was due to the belief that training sessions were unnecessary [11]. However, another survey of pollworkers in the 2006 General Election found that 86.2% attended and that other conflicts with the training day dominated reasons for non-attendance [19].

² Orange and San Mateo counties — 10% of all registered voters in California — use the Hart eSlate DRE voting system [7].

³ CA Election Code § 19340 specifies that all members of a precinct board must attend training that covers pollworker duties and the use of voting systems. However, CA Election Code § 12309 mandates specifically that inspectors must receive instruction in the conduct of elections, but is silent as to other types of pollworkers. It appears that many California counties, like the one we studied, operate under the latter rule, such that only inspectors are required to attend training.

⁴ According surveys of pollworkers who served in the 2006 Primary

knowledge and understanding of security and privacy practices. We first observed pollworkers during an election to identify issues relevant to security and privacy. We designed 10 vignettes [16] that address privacy and security risks based on cases from our observational data; these served as the core of a qualitative interview instrument. We used that instrument to interview twenty pollworkers to probe their perceptions and recollections.

3.1 Observations

To better understand privacy and security issues in the polling place, we observed a number of polling places during a real election. Our team had prior experience with the privacy and security issues of election technology.⁵ From this previous work we knew that the socio-technical system — i.e., people, policy and technology — was the right unit of study to understand privacy and security issues in practice.

We observed four polling places. Four polling places allowed ample time to observe many interactions at each site in a single day. We observed polling place operations during the general election in November 2010 from poll opening (07:00) to poll closing (20:00) and then observed the return of sensitive balloting materials to a drop-off site after poll closing. We observed each polling place for a few hours,⁶ with a break for lunch and discussion of our observations.

We did not design our sample to provide generalizable or representative results. We sought instead to sample varied polling place interactions relevant to security and privacy with a good understanding of each polling place. From past experience working with election officials we determined the greatest variations in polling place environments would vary along socioeconomic lines — that is, polling places with fewer problems would be located in more educated and affluent neighborhoods. Consulting with the County election official, we selected sites that were demographically distinct: two relatively affluent, mostly-white polling places and two relatively poor and more racially diverse polling places.⁷

The observers on our team specifically paid attention to issues of security, privacy, trust and trustworthiness (we hope to report trust and trustworthiness results in a future paper). We observed issues concerning

procedural accuracy, chain of custody of sensitive materials, chain of command within the pollworker force and privacy impacts of interactions and technologies used in the polling place.

The majority of polling site interactions we observed were unremarkable; the election proceeded smoothly with few issues. Our observations did reveal a variety of security and privacy issues. To our knowledge none of the risks we observed resulted in poor outcomes. Regardless, they can put election integrity at risk. We detail our observational findings in Section 4.1.

3.2 Interviews

Our observations provided evidence of security and privacy risks that arise on election day. Interviews with pollworkers would allow us to probe deeper into understanding and perception. Interviews centered on ten vignettes — short descriptions of a scenario that could happen in a polling place — built from specific privacy and security issues we observed on election day.⁸ These vignettes were designed to elicit pollworker understanding and awareness of security and privacy issues by asking them to react to scenarios in which such issues would arise.

We embedded these vignettes in a semi-structured qualitative interview instrument. To begin the interview, we prepared subjects for the task of imagining themselves in a polling place by administering a “warm up” section of the instrument, designed to initiate thinking about their most recent pollworker experiences. The interviewer next asked them to imagine working as a pollworker and then read each vignette followed by a series of questions. After working through the vignettes, the interviewer asked several general, open-ended questions about privacy and security, to elicit experiences or ideas that might not have been caught in the warm-up or vignette sections of the instrument.

In August of 2011, we interviewed twenty pollworkers from our target county. We sent recruitment letters via postal mail addressed to each of the pollworkers in the four polling places we observed in the previous November and four additional polling places chosen to be close to the demographics of the original four.⁹ We wanted to interview not only pollworkers whom we had observed — i.e., from polling places where we had a good understanding of the socio-technical dynamics — but also pollworkers from polling place environments

⁵ Hall and Mulligan were part of the California Secretary of State’s Top-To-Bottom Review [6] and have experience with privacy and security issues of voting systems.

⁶ We spent 2:39 at Site 1, 2:40 at Site 2, 1:23 at Site 3 and 2:20 at Site 4 (we followed ballots afterwards from 20:00 to roughly 23:00).

⁷ Confidentiality concerns do not allow us to identify specific sites.

⁸ Our vignettes are listed in full in Appendix A.

⁹ We sent out a total of 71 recruitment letters.

we had not observed.¹⁰ We accepted subjects on a first-come first-serve basis until we reached twenty (20). We requested subjects come to a centrally located public building for the interview, and to offset transportation costs we compensated them more than we usually would have. Subjects received \$60 at the beginning of the interview and were asked to agree to and sign a statement of informed consent before starting the interview. We audio-recorded each interview and then transcribed them. We thematically coded the transcripts using ATLAS.ti qualitative analysis software. Finally, using elements of grounded theory [24] we examined lists of extracted quotes and refined a new set of codes around specific issues, which make up the interview findings below (Section 4.2). We avoided issues with inter-coder reliability by using a single team member for the first pass of coding and afterwards another team member checked each code.

4 Findings

We first describe observational findings and then findings from our analysis of the qualitative interviews.

4.1 Observations

4.1.1 Polling place leadership models

Polling place team leadership models varied widely. By “leadership model”, we mean to what extent there was a recognizable order, authority structure and coordination in tasks and actions that pollworkers used to accomplish their work. Our findings here were surprising; we expected training would tend to force polling place leadership models into a somewhat standard form.

County pollworker training outlines a polling place model in which there are two Inspectors — a Chief Poll Inspector (Chief PI) and a Deputy Poll Inspector (Deputy PI). The Chief PI is responsible for the overall operations of the polling place; in particular, the equipment, ballot box, making sure the building is open and coordinating with the Deputy PIs, who are each responsible for a particular precinct within that polling place.¹¹ The Deputy PI is responsible for the precinct ballots, the precinct roster, processing voters for that precinct and supervising the Clerks for that precinct. Larger polling places get extra Clerks. The Chief and Deputy PI are both required to attend training classes,

while it is optional for Clerks. While the staffing patterns at each site officially followed this naming convention, in practice the system of leadership was quite different at each site.

At Site 1, the Chief PI attempted to exert close control over the tasks of her staff and managed both large and small elements of the operation. This model can be described as hierarchical — she directed the work of the Deputy PI and each Clerk — with a strong element of micromanagement. Pollworkers responded to this approach in different ways. Some were amenable to this level of supervision and control, while others combined their own best judgment with the PI’s instruction.

The leadership model at Site 2 was in stark contrast to the first site. The Chief PI failed to pay close attention to the demands of his responsibilities as an inspector as well as the needs of his staff and substantially neglected his duties. His attention was diverted from activities in the polling place, leaving a vacuum of authoritative knowledge and direction. There was no clear model of leadership in this polling place. Throughout the course of our observation, another pollworker often quietly filled this leadership gap and took measures to compensate for actions the Chief PI either completed incorrectly or missed altogether. Pollworkers generally operated independently with little direction. They asked each other for advice, rather than then turning to the Chief PI for guidance.

At Site 3 the Chief PI kept close watch on the work of her staff and seemed much more familiar with elements of pollworker training, especially towards issues of security and privacy. This inspector also delegated responsibility effectively. This polling place had a hierarchical, delegated structure where everyone knew their duty and performed it, free of the micromanagement we observed at Site 1. This strategy allowed the Chief PI to focus on the core responsibilities of her position — management and oversight — while ensuring that the site followed necessary procedures. She appeared to be well respected and pollworkers followed her instructions. As a standout among the four observed sites, the Chief PI had a particularly good grasp of security issues and election procedures and was very attentive to voters and problems around her.

Site 4 had a much more decentralized leadership model, although nothing like the “anarchy” of Site 2. This polling place appeared to function as a cooperative endeavor, akin to a flat, network organization [22] where team members enjoyed similar levels of autonomy and power. In fact, it was not immediately clear during the observation period which staff

¹⁰ In all, we interviewed 12 subjects that were pollworkers from the polling places we observed and 8 from other polling places. We chose not to link subjects to specific polling places in our analysis so that they could speak freely during interviews. This limits our analysis, but we felt it both methodologically and ethically important to ensure confidentiality.

¹¹ We observed polling places with 2-3 precincts each.

members held which roles. Pollworkers displayed a positive “can-do” attitude and worked collaboratively to solve problems. This generally created a well-run site, but sometimes caused problems due to confusion or inattention to detail.

Different models of leadership seemed to have distinct implications for trust, security and the overall integrity of the polling operation at a given site. A more hierarchical approach provided a strong leadership model that placed the Chief PI as a key figure who responded to risk and uncertainty directly (Site 1) or through trusted delegation (Site 3). The worst case, (Site 2), had no leadership; the PI did not understand or value the role of leadership in polling place operations. A cooperative, progressive atmosphere (Site 4) contributed to a well-run polling place, but didn’t provide the grounding to policy and attention to detail seen at Site 1 and Site 3. We discuss the interaction between risks and leadership models in the Discussion in Section 5.

4.1.2 Observations of security and privacy-relevant issues

4.1.2.1 Open scanner door

The most significant lapse we observed in terms of security and privacy was an open, exposed container of provisional and vote by mail (VBM) ballots.

Polling place ballot boxes in this county have a main compartment for standard ballots scanned on site, as well as an auxiliary bin incorporated into the exterior of the ballot box for provisional and VBM ballots. Pollworkers and voters insert ballots into the auxiliary bin through a small slot.

According to state law, and pollworker training,¹² the door to the main bin should be closed, sealed and locked during the election and the door to the auxiliary bin should be open only if needed, and then by at least two pollworkers. The key to the auxiliary bin door should be on a bracelet around the Chief PI’s wrist.

These policies ensure chain of custody of ballots so that only valid ballots make it into the ballot box and so that fraud is unlikely to be perpetrated without detection.

At Site 2, the Chief PI left the auxiliary ballot box door open for significant periods of time. This exposed provisional and drop-off VBM ballots and the PI left the key to the door inserted into the lock.

At one point, the Chief PI became distracted and

¹² See: CA Election Code § 19322. While we cannot cite to county procedures without identifying the county, we have materials on file.

abandoned his post at the ballot box. Noticing his absence, another pollworker immediately shut and locked the door and placed the key on his wrist. Later, the Chief PI returned and took the key from the pollworker. For a second time he opened the auxiliary bin door and failed to shut it.¹³

Regardless of the reason, his actions have significant security consequences. While provisional and VBM ballots are contained in sealed envelopes, the clear and visible exposure of these documents outside their nominal chain of custody, combined with the inattention of the Chief PI while at the scanner, rendered these ballots vulnerable to tampering. These observations prompted a line of questioning on the topic in our interview guide.

4.1.2.2 Scanner left at polling place

We observed pollworkers pack up Site 4 at the end of the day. Standard operating procedure instructs the Chief PI and another pollworker to deliver a set of critical election materials to a satellite drop-off point. This allows a set of sensitive election materials — memory cards, marked ballots, etc. — to be delivered for immediate counting under a continuous chain of custody, while bulkier non-sensitive materials can be picked up from the polling place at a later time.

The optical scanner was among the items to be dropped-off, however upon arrival at the drop off location the Chief PI realized she had forgotten it at the polling site, and no one had caught this mistake.

The optical scanner contains a removable memory card that stores vote totals and is used to program the device. It contains the configuration data and ballot data that are uploaded into the central election system. Leaving it unattended for a period of time is a security risk [12]. Physical access could allow an attacker to modify vote totals on the device or install malicious software that could control future elections [9].

In this particular case, the Chief PI returned to the polling site to find the scanner undisturbed. It was unclear whether she understood the gravity of this risk.

4.1.2.3 Managing auxiliary bin overflow

We also observed problems with the security of the overflow ballot box. The auxiliary bin (Section 4.1.2.1)

¹³ As observers, we do not know why the Chief PI left the auxiliary bin door open; we were participant observers but chose in many cases not to intervene or ask questions that could immediately change behavior relevant to our study. He may have done so because the narrow mouths of the auxiliary bin on this model of polling place optical scanner are prone to clogging.

on the side of the optical scanner is used for provisional ballots and VBM ballots that are dropped off at the polls. When the auxiliary bin is full, pollworkers must use another “overflow” container for these ballots. The county provided soft-sided “overflow” ballot boxes that a pollworker could set up for this purpose. Once the box was assembled voters could cast their ballots directly into the container. This container is a soft-sided collapsible padded nylon box with a sealable zipper around the top. To control chain of custody, once the box is set up and zipped closed, a tamper-evident zipper seal¹⁴ is put into place. Ballots are cast individually through a slot on the top of the box.

The seal policy requires pollworkers to seal the overflow box with a serially numbered tamper-evident seal to ensure that attempts to open the box will be detected. When set up properly, the seal on the overflow box must be broken to gain access to ballots.

We observed issues with this process in two polling places. At Site 1, the Chief PI was having trouble securing the zipper on the overflow ballot box. She asked us to assist her and we attempted to close the zipper. One of us (Hall) broke the single fragile seal tab during this process. The PI attempted to remedy the problem by heavily taping the sealed zipper shut with the broken seal approximately in place. This was fascinating; her solution did not directly substitute for the tamper-evident function of the seal but she tried to compensate for a lack of extra seals by making forced entry into the ballot box more difficult.

At Site 4 we observed the Chief PI *periodically* empty the auxiliary bin into the overflow ballot box by opening the zipper on the overflow box and transferring handfuls of ballots into it. This is contrary to instructions that specify that the auxiliary bin should no longer be used once full and that subsequent VBM or provisional ballots should be cast one at a time through the slot in the *sealed* overflow ballot box. After each transfer was completed (ignoring or destroying the tamper seal), the Chief PI simply zipped it shut again and placed it behind the scanner, out of sight. This was clearly a misunderstanding of procedures in terms of chain of custody, observability and tamper sealing.

4.1.2.4 Smartphone usage in the polling place

At two different polling sites on election day, we observed voters using phones either to take phone calls or read and type, interacting with the device. We

¹⁴ To see an example of the type of tamper-evident zipper seal used, see: Hall, Joseph Lorenzo, “Zippered Security Seal”, <http://flic.kr/p/rVvhW>, 4 November 2006.

observed a voter in the voting booth take an extended phone call at Site 3. In one case at Site 4 a voter spent nearly 45 minutes rather loudly researching her ballot choices. This type of activity became so frequent at Site 4 that the Deputy PI asked her supervisor, “What are the rules about using cell phones in here?” The Chief PI responded, “They can’t, but for some people it’s their cheat sheet.”

The PI seemed to make a decision here that allowing this kind of use was worthy enough to bend the rules.

This county has an explicit policy that no cell phone use is allowed in the polling place. Mobile phone use is generally prohibited at polls because it can be distracting and could compromise confidentiality or aid in coercion or vote buying.¹⁵ As portable personal computational networked devices become smaller and more ubiquitous, it can be difficult for pollworkers to detect and prevent their use. In addition, phones are increasingly used not just for making calls, but also for a host of other activities, such as conducting research on the web or jotting down notes.

4.1.2.5 Photography in the polling place

While cameras are now prevalent on many mobile devices, we witnessed only a single instance of potential camera usage. At Site 4, a voter asked if they could photograph another voter. The subject of the photograph would have been a new U.S. citizen casting their first ballot. The Chief PI curiously responded, “You can take a picture of me, but you can’t take pictures in here.” The Deputy PI replied, “Is that illegal? [skeptically]... now that I think about it.”

Photography is generally not allowed in the polling place in California, out of concern for ballot privacy and voter intimidation. Certain exceptions exist for news media or other specific activities, such as press coverage of candidates casting ballots [18].

Ultimately, the photograph in this case was not allowed. Pollworkers followed the correct procedure to protect the privacy of voters. Given the lack of clarity in the PI’s response, we were uncertain as to whether pollworkers knew the rules for photography and understood the rationale. As people increasingly carry such devices and use them to document daily life, it is important that pollworkers understand the privacy risks of photography in the polling place.

4.1.2.6 Pollworker inspecting the ballot face

¹⁵ For example, Professor J. Alex Halderman recorded himself casting his vote during the November 2004 presidential election using an early camera-phone: <https://jhalderm.com/pub/misc/vote04.avi>.

In two different polling sites we observed instances where the Chief PI examined the face of a voter's ballot without first asking permission. At Site 4, the Chief PI instructed voters to feed their own ballots into the machine. However, when one ballot was not accepted, she examined the ballot, presumably looking for stray marks and overvotes. She did not ask the voter for approval. This was curious as we saw her earlier ask permission of a voter, "Can I look at it?", when the scanner would not accept the voter's ballot.

At Site 3, the Chief PI routinely inspected ballots that had been rejected by the scanner without asking voters for permission. She seemed unaware of issues of ballot privacy. This was particularly surprising because this Chief PI had otherwise exemplary security practices and showed great skill in managing the polling place.

If the scanner detects an overvote¹⁶ or other ballot error, it beeps, ejects the ballot back to the voter and displays an error message. Procedures specify that the pollworker at the scanner then informs the voter that there is a problem with the ballot and that they should check it for mistakes. Pollworkers are discouraged from looking at the ballot face to preserve ballot privacy, although they can assist at the request of the voter.

After observing these contradictory behaviors, we decided to probe ballot privacy practices in our interviews. Why would conscientious pollworkers ignore basic measures to preserve ballot privacy?

4.2 Interviews

We discuss findings from our interviews relevant to security and privacy.

4.2.1 Security perceptions

4.2.1.1 Little evidence of security awareness

Our questions, and in particular our vignettes prompted little evidence of security awareness. Pollworkers understood that rules were in place and should be followed, but they lacked understanding as to why particular security-relevant rules and procedures were in place and what risks they addressed.

Many of the pollworkers saw their jobs as simply doing what they were told; they did not know how the scanners or software worked and were not clear on how the voting process itself relied on technology. Only a few pollworkers recognized that ballot box stuffing and the malicious reprogramming of the scanners are

potential problems that can occur without proper security procedures. One pollworker went so far as to say, incorrectly, that the optical scanning machines were only to validate the count of paper ballots:

"the machine itself wouldn't do you any good because we have the voted ballots. ... you only need the machine to validate the number count." -(6)¹⁷

This interviewee assumes that the machine "just counts" and is therefore not a critical piece of the voting system, when, in fact, the totals on the memory card are directly uploaded by the county and aggregated into vote totals. Moreover, we saw no evidence of deeper security awareness, such as knowledge that voting system memory cards can hold malicious software [12].

4.2.1.2 Chain-of-custody, two-person rule

Pollworkers were acutely aware of the two-person rule — i.e., two people should always be present while handling sensitive assets. However, they tended to view this rule as more of a "check and balance" error correction operation than a potentially adversarial security control:

"two people go... so there's a balance, a check and a balance there" -(9)

The two-person rule works to maintain asset security during parts of the election process that are not as public as other election operations. Pollworkers did not make the connection that the two people involved in such a procedure need to maintain an adversarial mindset. They viewed the rule as just that — a rule in place for a reason. But that exact reason was not distinctly clear to the pollworkers until they were confronted with the question as to why that rule exists.

4.2.1.3 Seals and ballot box starting state

When it came to the discussion of the extra soft-sided "overflow" box used when the vote-by-mail and provisional auxiliary bin was full, pollworkers had few concerns about the security of handling ballots, transferring ballots from one box to another, keeping ballots in either container, and sealing the box properly.

Two issues came up with the use of the overflow box: its use for ballot storage and sealing the box.

Pollworkers mentioned utilizing the soft-sided box even before the auxiliary bin was full simply to "monitor" overflow of ballots. This is incorrect; the overflow box should only to be used when the auxiliary bin is full.

¹⁶ An "overvote" is when a voter makes more choices than permitted for a contest on the ballot. This invalidates their vote for that contest.

¹⁷ Throughout this paper quotes will reference the serial number in parentheses assigned to a subject for comparison of their statements.

Pollworkers adopted other ways of using the soft-sided box that included placing ballots in both the auxiliary bin and soft-sided box simultaneously from the start and taking ballots periodically out of the auxiliary bin and placing them in the soft-sided box.

When the soft-sided box is set up it needs to be properly sealed. The single seal provided is fragile and can break, leaving pollworkers trouble-shoot how to handle that situation. Responses to how this was handled include re-sealing the soft-sided box with tape, calling the main office to report it, and “keep[ing] an eye on it.” (18) Pollworkers expressed little concern for the ballots in these situations, though one mentioned, “the secondary storage is not as secure as the primary storage” (14). They believed their approach to the situation was sufficient.

One of the first topics we asked the pollworkers to talk about was a situation where a specific law was not followed at poll opening. We asked them to discuss what they would do if the Chief PI did not show everyone present at poll opening that the ballot container was indeed empty. While this is California law,¹⁸ the PI manual only states that they need to show the first voter that the scanner display screen shows a 000 total.¹⁹ While this is similar to the law, it is quite different; the aggregate displayed count being 000 is very different than a visual confirmation that the ballot box is empty.²⁰ All but one of the pollworkers stated that they were unaware of this rule or that one of the PIs deals with this. The one pollworker who recognized this concept stated that they vaguely remembered that “there [was] something that we have to come and look at.” (6) This gap in understanding surprised us since election accuracy critically relies on confirmation of the initially empty ballot box. In addition, one subject reported finding old ballots from past elections in the ballot box.²¹

4.2.1.4 *Scanner as a vulnerable computational asset*

As described above, pollworkers did not raise many security issues with voting technology during the vignette portion. However, at the end of the interview, we asked them a series of general questions about the

security and accuracy of the election. When discussing the accuracy and security of the voting system, pollworkers expressed uneasiness with the optical scanner. They raised a variety of concerns, including the possibility that the machine could be hacked, manipulated, rigged, pre-programmed, and reprogrammed. News stories of other states with more votes than registered voters or tales of elections being rigged came to mind when pollworkers faced direct questions of scanner security. Regardless of whether pollworkers considered themselves electronically savvy, the concern for the way the optical scanner functioned throughout the voting process largely stemmed from a misunderstanding of its functionality, who programmed it, and its precise role in the voting process. One noted, “I’m an electronic technician, and I’m not sure I trust the technology.” (10) Some pollworkers did comment that “messing with the voting machines,” “screwing around with the data collection,” (1) and even tampering with the machines was something that they felt could be easily done.

4.2.1.5 *Equating security with safety and physical security*

Several pollworkers, when asked generally about their concerns for the security of an election, connected the idea of security to physical security or safety specifically. Two main concerns were mentioned: one, the physical security of the polling place, and two, the security of the optical scanner unit and ballots themselves when being transported to and from the polling sites. A few pollworkers mentioned that there might be incidents where “somebody came in with guns” (18) or there “weren’t enough people inside working the poll” (16) or not all the doors to the polling place except the front door were locked. To them, these were the type of issues that determine election security. Other pollworkers who expressed physical security concerns discussed stories they had heard about car accidents involving ballots or other pollworkers losing ballots en-route to the main polling center. To these pollworkers, the only security issues they saw were ones involving situations where either accidents happened or physical harm was intended, and not issues of election manipulation or voting technology security.

4.2.1.6 *Chain-of-command issues*

A number of pollworkers mentioned issues involving chain of command. Two issues arose when pollworkers discussed their coworkers or bosses at the polling site: one, that the chain of command did not always work because friction existed between co-Clerks and between Clerks and their bosses; and, two, that the chain of

¹⁸ See: CA Election Code § 14215.

¹⁹ This may be confusion with CA Election Code § 19360, which requires pollworkers to check that the voting system counter is 000.

²⁰ In fact, researchers have demonstrated in the past that flaws in certain models of optical scanner software allow “pre-stuffing” the electronic ballot box such that negative votes for one candidate can cancel out positive votes for another candidate, resulting in a 000 total on the display [15].

²¹ During our observations, the Chief PI at Site 1 said she had also found ballots left from the previous election in the ballot box.

command funneled security and privacy issues involving technology upwards to more senior pollworkers.

Several Clerks expressed frustration with other Clerks that they were forced to work with on polling day that they thought of as incompetent or simply annoying. Other pollworkers in the Clerk position found that their superiors were often overbearing; these Clerks had been in their positions for many years and having someone above them tell them what to do was condescending. One pollworker strongly felt so, and said the following when her superior attempted to give her instructions,

“duh. I know how to run my table. I know how to do my bag. I know how to do this, so why you telling’ me this?” -(5)

PIs in turn, found Clerks who did not consistently listen and follow instruction frustrating. One inspector in the most recent election stated,

“Let’s get that straight. You’re a Clerk. I’m a lieutenant. You work for me. You do what I say. You don’t like to do what I say, then you can go...” -(7)

When it came to deferring issues of security and privacy to superiors, Clerks were quick to relinquish ownership of solving problems; Clerks saw their jobs involving specific tasks from the PI, and that was all that they would do. Issues that arose when errors occurred such as the auxiliary box being full, the scanner jamming, or voters becoming upset (among other issues), were almost always sent to the Chief or Deputy PI to fix. “That’s one for the chief” (13) or “I would contact the boss and she seemed to have the final word” (10) or “I would probably ask the chief inspector...” (19) were phrases mentioned by Clerks during interviews. The sentiment that the Clerks were not in control, but the inspector or deputy chiefs had that responsibility, was brought up especially when discussing technology failures or technological security or privacy concerns: “...it’s their responsibility [the inspector]; they’re supposed to know what to do...” (15) or

“I would defer to the inspector. I mean, I’ve had questions for the inspector and I may disagree, but it’s not my decision.” -(18)

4.2.1.7 Ad-hoc development of security and privacy protocols

Pollworkers mentioned creating ad-hoc protocols for security or privacy purposes, or to maintain a smooth-running polling site. The most oft-cited ad-hoc protocol was how to handle a broken seal on one of the boxes or

bags. The official protocol when this occurs involves calling election headquarters and having new seals delivered. Few pollworkers mentioned this and instead discussed strategies such as putting “some temporary thing with tape over the zipper” (12) or “tap[ing] it shut to make sure that’s not jeopardized being open” (8) to remedy the situation. Other ad-hoc protocols included creating a routine system for cleaning out the provisional and vote-by-mail ballot box into the overflow box every two hours to combat overflow, creating custom color-coded guides or charts for Clerks and voters, creating flow-charts that better explained Clerk duties, and bringing in food for the other pollworkers (this helped to build rapport and keep workers at the polling place).²²

4.2.2 Privacy perceptions

4.2.2.1 Intuition and privacy

Compared to security issues, pollworkers had a more intuitive grasp of privacy concerns. As discussed below, they mentioned ballot secrecy or the importance of voter privacy at the polls often. One pollworker mentioned that if the press came in to take pictures:

“Some people, when they see their picture in the paper like that, I guess, probably most people would object to it.” -(3)

She used the possible response voters to help guide her response. In another case, the pollworker put herself in the shoes of a voter when thinking about privacy:

“Actually, I guess if I’m filling out [my] ballot and there’s somebody behind me taking a picture, I’d feel a little uncomfortable...” -(20)

Pollworkers also used privacy experiences in other settings to draw analogies to the polling place. One subject reflected on her other work to help understand rules about polling sites. According to the pollworker:

“I mean, I work at another thing where it’s a federal facility, and we don’t allow photographs inside because it’s a federal facility...” -(15)

In a second example, the interviewee likened rules at the polls to those at a casino:

“Okay, say if somebody’s there and don’t want somebody know they’re there... or somebody’s gamblin’ and you got a camera and lookin’ at somebody’s [cards] and you can talk on the cell phone... and you can tell the other person what the

²² At Site 4 a stray bit of lasagna literally gummed up the scanner when the “ender card” was fed through to close the polls.

moves are. You can cheat like that too.” -(5)

Here, she tied the prohibition of cameras at casinos to protection of personal privacy, freedom from bias, and to security concerns at the polls.

4.2.2.2 *Inconsistent behavior when examining ballot faces*

When discussing how they handle ballots rejected by the scanner, more than half of interviewees specifically discussed whether they examined the ballot face to identify errors. Three interviewees said that they looked at the ballot face, but did not mention that they asked permission to do so. One said,

“If it is rejecting it I look through the ballot myself and say, ‘Hey, look you did this, you voted twice for this...’” -(2)

In another case, the interviewee seemed dismissive of privacy issues, presenting himself as a trustworthy, neutral facilitator:

“I haven’t had anybody complain. Of course you’re looking at their ballot. ... We’re not supposed to be. I don’t care how anyone votes.” -(18)

A couple of interviewees said that they looked at the ballot face, but only after asking the voter for permission. One pollworker mentioned the importance of privacy, but balanced it against practical concerns:

“Most people say ‘Can you help me find it?’ You’d say this is your private information, ... If you want us to help we will... ‘who cares?’ It’s a vote.” -(11)

In a second case, the pollworker discussed how she needed to step in to compensate for the limitations of the equipment:

“We’re instructed that the voters don’t want us to look at ballots, but if I don’t look at the ballot they don’t have an idea of what they did wrong.” -(12)

In contrast, six interviewees specifically said that they do not look at the face of voter ballots. One pollworker described these actions in terms of process:

“We try not to look at the ballot. If the error does come up we just immediately mark it destroyed. Say you’ll need to fill this out again.” -(4)

In another example, the interviewees offered a more personal perspective.

“I would have a hard time looking at their ballot because ... I respect the privacy of people’s ballots.” -(17)

4.2.2.3 *Secret ballot*

The importance of the secret ballot seemed well understood. Interviewees specifically mentioned the importance of voter privacy at the polls and/or the necessity of the secret ballot. While some pollworkers simply referred to rules that enforced privacy issues, such as “no photography” or discussed why a voter may not want to share her ballot choices, others offered a more detailed analysis.

Three people specifically talked about bias and electioneering when discussing the secret ballot. In the context of discussing photography at the polls, each of these individuals made the connection between taking pictures and other activities that may unfairly influence or intimidate voters. According to one person:

“It’s just like we had people coming in with t-shirts advertising various candidates and we asked the person to button the jacket ... because it was a form of electioneering.” -(6)

The other two pollworkers similarly mentioned the problem of wearing clothing that advertises a specific candidate.

4.2.2.4 *Privacy and smartphones*

Pollworkers had a mixed understanding of whether voters could use smartphones in the polling place to research candidates and propositions. Half of our interviewees specifically stated that voters may not use phones in any way in the polling place. In a typical response, one pollworker immediately tied the use of a smartphone to the more general rule about mobile phones,

“Well, I’m pretty sure cell phones aren’t allowed. You tell them the cell phones aren’t allowed.” -(3)

Nearly as many interviewees were unaware that smart phone activity must be restricted in the polling place. Some linked the use of phones to paper notes that voters might take into the polls. According to one pollworker,

“I don’t see any reason that you can’t have notes on your Smartphone any different than if you bring a piece of paper or a ballot already filled out.” -(13)

Another expressed that his only concern was about voter flow management:

“I’ve never seen anyone surf the web. If someone were to do that, I don’t know that that’s a problem ... as long as they’re not holding up the line...” -(6)

Three pollworkers specifically mentioned that cell

phones were not allowed at the polls, but that they would permit certain activities, like surfing the web or reviewing notes. According to one,

“As long as the person is not making a phone call or texting somebody and getting advice that way, I’m not sure that using the smart phone to check things out is a horrible thing.” -(12)

A second person said that web surfing would be acceptable:

“That’s okay as far as I’m concerned or if they have the little web site that’s hosted by some special interest group.” -(17)

The third pollworker discussed the complexity and nuance that newer devices create. He said,

“Well, it says on the sign as you come in ‘Please turn off your cell phone’, which is a Smartphone. Right? However, you can’t turn off a PDA right? Or an iPad per se and that’s not a cell phone per se and people do need research.” -(11)

This pollworker ultimately determined that this was an acceptable activity.

4.2.2.5 Privacy and photography

The majority of pollworkers knew that photography is forbidden in the polling place, in accordance with California Secretary of State policy [18]. Many of the interviewees said that photos are not allowed. A slightly smaller number specifically mentioned privacy concerns in their response. When asked why photography might be restricted, one person said,

“I would think privacy issues, that people don’t want to be photographed at the polls...” -(1)

Four subjects provided a more rules-oriented response without specifically discussing a rationale. Said one interviewee,

“I think the rule is no cameras are allowed in the polling area. I think there’s a rule in that and I would enforce that.” -(2)

Two people among the 16 who knew the rules said that they would make certain exceptions. According to one,

“You’re not supposed to have anybody take pictures and that’s the guideline, [but] if it’s a friend taking a picture we don’t get too uptight about it.” -(11)

Four pollworkers seemed either unaware of the rule or they misunderstood how to apply it. One person understood that photography could be a violation of privacy, but thought that this only applied in the voting

booth. Another said photographs were okay as long as the ballot is not photographed. One said he was not sure what to do if a person wanted to take a picture. One woman said she had, “never heard that that’s a problem.” (9)

5 Discussion

Our two-pronged observation/interview methodology allowed us to observe actual risks situated in a particular election environment and then to interview pollworkers about those specific risks to better understand their level of risk awareness and their understanding of policies and procedures. Our observations gave us insight into issues that arise on election day and how leadership models may contribute to these risks. By interviewing pollworkers from both observed and unobserved polling places, we grounded the interview responses in known polling place instances but also collected data on these issues from a wider sample.

5.1 Awareness of Privacy & Security Risks

We find that awareness of security-related policies and procedures and comprehension of security risks is low compared with privacy risks. Pollworkers did not recognize the sensitivity of certain assets in the polling place — e.g., auxiliary bin ballots, the optical scanner — and did not have a good grasp on security protocols such as chain of custody and tamper seals. With the exception of instances where we observed PIs examining ballots without consent, pollworkers did have a better understanding of privacy issues. One explanation for this asymmetry could be that election security is more of a distributed value, rarely challenged in the field, whereas ballot privacy is more of an individual and personal value that pollworkers encounter more frequently. Poll workers do not often encounter election adversaries, but certainly will hear about privacy complaints from voters if voters feel there is a concern or real issue with the secrecy of their ballot. We hope as people gain a working understanding of the principles behind digital security measures — e.g., watch for people messing with exposed plugs — that this knowledge begins to trickle down into the pollworker force. We do think there is value in specifically covering a “crash course” in cybersecurity during pollworker training.

The role of photos and smartphones in the polling place was particularly interesting, given their dubious status as both reference aides and points of vulnerability. We saw evidence that voters use smartphones — which are invariably equipped with cameras — as reference tools.

This is tolerated by pollworkers despite their awareness of privacy issues with photography and risks to vote buying and coercion involved with voter communication while inside the voting booth. We have come far since earlier days of US elections where vote-buying and intimidation was par for the course [17], so perhaps this is a case of the opposite problem from what we outline above in terms of privacy vs. security: whereas people find cybersecurity to be so new that it is unfamiliar, forms of undue influence on the ballot may instead be so *old* to be unfamiliar. This tension between devices as aides vs. adversaries will grow in the future: this year, some California counties will specifically sanction the use of smartphones as “cheat sheets” [1]. These counties will design their voter guides as mobile applications where voters can save their choices within the application and take their mobile device to the voting booth for reference. This poses a significant tension between managing risks involving these devices and providing state-of-the-art, usable voter reference tools. These counties may need to remove “No Cell Phones” signage from their polling place and replace them with a more complicated sign that better expresses election official policy: “Smartphones are allowed for voter reference tools only, not for talking, photography or otherwise communicating with other people.”

Finally, we saw some evidence of ad-hoc development of security and privacy protocols. In many cases, this was a positive contribution to security in the polling place; such as carefully taping closed an accidentally broken security seal to frustrate casual attempts at forced entry. While this didn’t substitute for tamper-evident seals — as tape can be removed with time and effort and re-applied — it forces a potential ballot-box stuffer to spend precious time gaining entry. However, ad-hoc protocols could also be problematic, such as periodically emptying the auxiliary bin when it should rarely be opened. This bulk transfer of sensitive material forced pollworkers to ignore the overflow box’s security seal; feeding transferred ballots one-at-a-time through the provided slot would have been time-consuming and difficult. Studying ad-hoc policy and procedure development in elections would be a fruitful direction for future research efforts.

5.2 The Role of Leadership

Our sample was small and designed to discover extremes in polling place environments. Even with a small sample of four polling places in our observations, we found quite divergent polling place management styles that we tentatively suggest relate to different perspectives on risk management and trust. The polling places we observed displayed almost archetypical

diversity in leadership models: a micromanaged hierarchy (Site 1), a delegated hierarchy (Site 3), a “flat” cooperative (Site 4) and a power vacuum/anarchy (Site 2). Of course, with a larger baseline of polling places from a more systematic sample, we would likely see additional leadership models and begin to untangle the relationship between leadership models and polling place security and privacy.

In our sample, the interaction of these various management styles, and underlying trust models, correlate to polling site attention to security and privacy threats and to procedures designed to mitigate them. We observed the most significant security lapse in the “anarchy” of Site 2, where the PI substantially neglected his duties. Site 1 and Site 3 displayed good understandings of election integrity issues and specific county policies. Site 4 had a productive and positive working atmosphere, but displayed serious ignorance of privacy and security risks. It is difficult from our data to say whether or not this correlation was due directly to leadership models, but it seemed to play a meaningful role. This is another superb direction for future work.

Different models of leadership have distinct implications for trust, security and the overall integrity of the polling operation at a given site. A Chief PI may adopt a particular leadership style for many different reasons, and we believe that there is a critical relationship between the PI’s choice of organizational strategy and his or her perspective on how to convey a sense of trustworthiness and integrity among the principal actors in a polling location. A more hierarchical approach can sometimes provide a strong leadership model that places the PI as a key figure who responds to all risks and uncertainties directly (Site 1) or through trusted delegation of subordinates (Site 3). Of these two hierarchical styles, the first involves micromanagement and information gatekeeping that can undermine trust between team members in favor of centralized decision-making. In comparison, the distributed leadership model of Site 3 spreads the responsibility of dealing with risks and uncertainties evenly among delegates, resulting in a shared sense of ownership and empowerment to solve problems (at the expense of tightly-controlled, centralized management of risk). Finally, the supportive and trustworthy atmosphere of Site 4 unfortunately overlaid substantial misunderstanding of privacy and security values as well as associated county procedure.

There may not be a single ‘best’ style of leadership for *all* locations — but clearly some are more vulnerable to risks to security and integrity than others.

5.3 Recommendations

A few recommendations emerge from this work.

We propose that training materials be oriented around the risks they are designed to address. This will promote pollworkers' general knowledge of risks to election integrity as well as the specific policies their roles support in order to mitigate risks on election day. Privacy, rather than computer security, seems to be a more natural and intuitive value from which to approach these issues for pollworkers. Pollworkers in our sample appear unaccustomed to thinking about *information* privacy and security, thus we tentatively recommend that Counties consider positioning election specific policies and procedures in a context that conveys some basic understanding of generalized threats to these values.

The selection and execution of a specific leadership model or management style within a polling place seemed to play a key role in alleviating problems of security and privacy, at least in our limited and non-representative sample. In our investigation, a delegated hierarchical model like that of Site 3 seemed to best promote good security and privacy practices.²³ The cooperative model of Site 4 was remarkable in the level of trust and cooperation it displayed. This model could be especially powerful if some of the tendency to ignore and normalize risks was eliminated.

Acknowledgments

This work was possible only because of the generous and tireless dedication of the election staff and volunteers of the unnamed county we studied.

We are grateful to Sean Peisert, Bonnie Glaser and anonymous referees for discussion and comments on earlier drafts.

The National Science Foundation supported this work under A Center for Correct, Usable, Reliable, Auditible and Transparent Elections (ACCURATE), Grant Number CNS-0524745. Any opinions, findings, conclusions and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] *Press Release: Marin, Santa Cruz and Shasta Counties Teaming Up to Go Green*. 2012; URL: <http://www.atwoodz.com/marin-santa-cruz-and-shasta->

²³ Of course, we don't want to give the impression that this research rigorously compared all possible leadership models, but that in our limited investigation this seemed to be a particularly effective model.

[counties-teaming-up-to-go-green/](http://www.atwoodz.com/marin-santa-cruz-and-shasta-counties-teaming-up-to-go-green/).

[2] Alvarez, R.M. and T.E. Hall, *Controlling democracy: the principal-agent problems in election administration*. Policy Studies Journal, 2006. **34**(4): p. 491-510.

[3] Atkeson, L.R. and K.L. Saunders, *The effect of election administration on voter confidence: a local matter?* PS: Political Science & Politics, 2007. **40**(4): p. 655-660.

[4] Balzarotti, D., G. Banks, M. Cova, V. Felmetzger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna, *An experience in testing the security of real-world electronic voting systems*. IEEE Transactions on Software Engineering, 2010. **36**(4): p. 453-473.

[5] Brace, K., W., *Nation Sees Drop in Use of Electronic Voting Equipment for 2008 Election — A First*, 2008, Election Data Services. URL: http://www.edssurvey.com/images/File/NR_VoteEquip_Nov-2008wAppendix2.pdf.

[6] California Secretary of State, *Top-To-Bottom Review*, 2007, California Secretary of State. URL: http://www.sos.ca.gov/elections/elections_vsr.htm.

[7] California Secretary of State, *Voting Systems Used by Counties*, 2012, California Secretary of State. URL: <http://www.sos.ca.gov/voting-systems/oversight/vsys-by-county.htm>.

[8] Claassen, R.L., D.B. Magleby, J.Q. Monson, and K.D. Patterson, *At Your Service*. American Politics Research, 2008. **36**(4): p. 612-634.

[9] Davtyan, S., S. Kentros, A. Kiayias, L. Michel, N. Nicolaou, A. Russell, A. See, N. Shashidhar, and A.A. Shvartsman. *Taking total control of voting systems: Firmware manipulations on an optical scan voting terminal*. in *Proceedings of the 2009 ACM symposium on Applied Computing 2009*.

[10] Glaser, B.E., K. Mac Donald, I. Hui, and B.E. Cain. *Explaining Voting System Performance: Do Technology, Training, and Poll Worker Characteristics Matter?* in *Annual Meeting of the American Political Science Association*. 2007.

[11] Glaser, B.E., K. Mac Donald, I. Hui, and B.E. Cain, *The Front Lines of Democracy: Who Staffs Polling Places and Does it Matter?*, 2007, University of California, Berkeley, Election Administration Research Center.

[12] Halderman, J.A., E. Rescorla, H. Shacham, and D. Wagner, *You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting*

Systems. USENIX/ACCURATE Electronic Voting Technology Workshop, 2008.

[13] Hall, T., J.Q. Monson, and K.D. Patterson, *Poll workers and the vitality of democracy: An early assessment*. PS: Political Science & Politics, 2007. **40**(4): p. 647-654.

[14] Hall, T.E., J. Quin Monson, and K.D. Patterson, *The Human Dimension of Elections*. Political Research Quarterly, 2009. **62**(3): p. 507-522.

[15] Hursti, H., *Critical Security Issues with Diebold Optical Scan Design*, 2005, Black Box Voting. URL: <http://www.blackboxvoting.org/BBVreport.pdf>.

[16] Jenkins, N., M. Bloor, J. Fischer, L. Berney, and J. Neale, *Putting it in context: the use of vignettes in qualitative interviewing*. Qualitative Research, 2010. **10**(2): p. 175-198.

[17] Jones, D.W. and B. Simons, *Broken Ballots: Will Your Vote Count?* 2012, Stanford, CA: Center for the Study of Language and Information.

[18] Lean, J., *CCROV Memorandum #10301, November General: Cameras At Polling Places*, 2010, California Secretary of State. URL: <http://www.sos.ca.gov/elections/ccrov/pdf/2010/october/10301jl.pdf>.

[19] MacDonald, K. and B. Glaser, *The Why, How, what and when of Precinct Board: Reactions from the*

Front Lines a Survey of California Poll Workers in the Primary Election of 2006, 2006, University of California, Berkeley, Election Administration Research Center.

[20] McDaniel, P., M. Blaze, G. Vigna, et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, 2007, Ohio Secretary of State. URL: <http://www.patrickmcdaniel.org/pubs/everest.pdf>.

[21] Pastor, R.A., *Improving the US Electoral System: Lessons from Canada and Mexico*. Election Law Journal, 2004. **3**(3): p. 584-593.

[22] Saxenian, A., *Regional Advantage: Culture and Competition in Silicon Valley and Route 128*. 1996: Harvard University Press.

[23] Selker, T., *Election auditing is an end-to-end procedure*. Science, 2005. **308**(5730): p. 1873-1874.

[24] Urquhart, C., H. Lehmann, and M.D. Myers, *Putting The 'Theory' Back Into Grounded Theory: guidelines for grounded theory studies in information systems*. Information Systems Journal, 2010. **20**(4): p. 357-381.

Appendix A: Vignettes

(Read: “For the next part of the interview, we will describe a number of scenarios one might encounter while working in a polling place. We will tell you a short story and then ask you a question or two about each one. The purpose of these scenarios is not to test your specific knowledge of polling place rules. Instead, we are trying to learn about how you approach problems and what tools and knowledge you apply to resolve them. Afterward, we will finish with a few more general questions to get additional insight into your responses.)

Set-up: For these scenarios, imagine that you are serving as a pollworker in [redacted] County on Election Day.

Scenario 1: You arrive to open the polls. After setting things up and 5 minutes before polls open, the head pollworker (Poll Inspector) decides to close and seal the ballot box on the optical scanner, contrary to rules you remember that say the first voter should confirm that the ballot box is empty before voting begins.

- What issues, if any, are raised in this situation?
 - (or ask: how much of an issue is this and what would you do?)
- What might a pollworker do to address these issues?
 - (or ask: what could you do to address this issue or situation?)
- What is the ideal outcome of this situation?
- What is the worst possible outcome?
- On a scale of 1 to 5, how concerned are you about this situation, with 1 being not concerned at all and 5 being very concerned?

(For each scenario, repeat the list of questions above)

Scenario 2: A voter arrives and provides her name at the check-in table. She is not listed on the voting roster. You determine that she needs to fill out a provisional ballot and hand her the appropriate materials. The voter says, “This provisional ballot is a lot of extra work, and I bet they won’t even count my vote.”

Scenario 3: Another voter walks into the polling place. Without speaking, the voter takes out a driver’s license and hands it to you, pointing to his name.

Scenario 4: A first time voter wants to commemorate the event by having a friend take a photograph of her as she fills out her ballot.

Scenario 5: A voter is consulting a smartphone while filling out his ballot. He appears to be researching candidates to inform his vote.

Scenario 6: The pollworker staffing the ballot scanner has stepped away to assist a colleague. A voter completes her ballot and stands next to the scanner for several minutes, unsure what to do next.

Scenario 7: Once the ballot has been fed into the machine, it displays an error that the voter has over-voted — that is, voted too many times in one contest — and the scanner rejects the ballot.

Scenario 8: Throughout the day, provisional and VBM ballots are added though a slot into the “auxiliary bin” of the optical scanner unit. Over time, a stack of ballots gets clogged in the neck of the bin, making it difficult to put additional ballots in the slot. (Explain what the auxiliary bin exactly is; usually this needs explaining)

Scenario 9: Eventually, the auxiliary bin is completely filled with provisional and VBM ballots. The overflow ballot box is needed. In [redacted] County, this box is blue, soft-sided cube with a zippered top. While setting up the box, a colleague breaks a numbered seal on the box zipper. (Explain what the zipper seal is; usually this needs explaining)

Scenario 10: After closing the polls, the poll inspector takes the ballots to election headquarters. Upon arriving, he realizes that he left the top of the optical scanner back at the polling place. (The top of the scanner is the computerized part that voters feed ballots into, separate from the large ballot-box receptacle underneath it.)