Contractual Barriers to Transparency in Electronic Voting

Joseph Lorenzo Hall*
School of Information, University of California, Berkeley

Abstract

We analyze 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 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 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.[1]

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.[2] 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* and *accountability*.[3] 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 2, we talk briefly about related work. Section 3 describes the data set and how we conducted the initial analysis. In section 4, we discuss the results of the analysis and in section 5 we offer recommendations for transparency-facilitating terms and provisions. Fi-

*Contact the author at: joehall@berkeley.edu. This paper was submitted to the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07) on 22 April 2007. It was accepted on 1 June 2007 and the camera-ready version was made available on 28 June 2007. This paper will be presented at EVT'07 in Boston, Massachusetts (USA) on 6 August 2007; *See:* http://www.usenix.org/events/evt07/.

[1]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", *Anchorage Daily News*, January 24, 2006; Alaska Democratic Party, Press Release, "Alaska: Public Records From 2004 Election Will Be Released", September 20, 2006, *available at:* http://votetrustusa.org/index2.php?option=com_content&do_pdf=1&id=1801. Also see page 35 of: Collaborative Public Audit of the November 2006 General Election, The Cuyahoga County Collaborative Audit Committee and Cleveland State University Center for Election Integrity, April 18, 2007, *available at:* http://urban.csuohio.edu/cei/public_monitor/cuyahoga_2006_audit_rpt.pdf.

[2]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 University of California at Berkeley School of Law (Boalt Hall), *available at:* http://www.law.berkeley.edu/clinics/samuelson/projects_papers/Legal_Issues_Elections_Officials_FINAL.pdf.

[3]Joseph Lorenzo Hall, Transparency and Access to Source Code in E-Voting in *USENIX/ACCURATE Electronic Voting Technology Workshop* (2006), *available at:* http://josephhall.org/papers/jhall_evt06.pdf.

nally, we offer our thoughts on how to extend this work in section 6.

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.[4] 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.[5]

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.[6] 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 involved with electronic voting systems.[7]

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 downloading and submission of voting system contracts.[8]

3 Data and Methodology

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.[9] 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%) alone from California and no more than 5 from any other individual state.[10]
- The contracts are between these 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).[11]
- The three major vendors, DESI, ES&S and Sequoia, are parties to the lion's share (45 (82%)) of the contracts in our data set; these vendors are parties to 16, 17, and 12 contracts, respectively.
- These contracts cover a time period from March 2000 to July 2006. Over half (29) are from 2003

[4] Trade secrets are unique in the realm of intellectual property; they are no longer protectable once publicly disclosed (See "trade secret" definition in note 29). 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.)

[5] David Levine, "Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure", 59 Florida Law Review 135 (2006), *available at:* `http://ssrn.com/abstract=900929`.

[6] 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 4, 2007, *available at:* `http://www.cs.uiowa.edu/~jones/voting/cfp2007.pdf`.

[7] "The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost", The Brennan Center for Justice, Voting Technology Assessment Project, October 2006, 123-, *available at:* `http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf`

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

[9] 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.

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

[11] 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.

and 2004 with the remainder spread approximately equally over 2001-2002 and 2005-2006.[12]

- 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."[13]

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.[14] 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.

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.

3.2 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.[15] We read the 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".[16] 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.

4 Analysis

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 transla-

[12] Only one contract is from 2000 (see note 17). 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.

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

[14] 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 may 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.

[15] Unfortunately, some contracts were received 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 directly.

[16] 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 15, *See:* `http://accurate-voting.org/contracts/MS/MS_diebold_2005.pdf`.

tion,[17] analysis,[18] and even extend to training materials and ballots.[19] 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.[20]

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.[21]

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.[22]

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.[23]

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.[24]

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. 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.[25] 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[26] or procuring the printing of their ballots from a firm other than ES&S.[27]

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.[28]

This provision would be more troubling if unilateral on

[17] Contract between Riverside County, California and Sequoia (2000) at 8, *available at:* http://accurate-voting.org/contracts/CA/Riverside/CA_riverside_2000.pdf.

[18] Contract between Bergen County, New Jersey and Sequoia (2001) at 5, *available at:* http://accurate-voting.org/contracts/NJ/Bergen/NJ_bergen_2001.pdf.

[19] Contract between Sarasota County, Florida and ES&S (2001), at 8-9, *available at:* http://accurate-voting.org/contracts/FL/Sarasota/FL_sarasota_2001.pdf.

[20] Contract between Orange County, California and Hart (2003), at 34, *available at:* http://accurate-voting.org/contracts/CA/Orange/CA_orange_2003.pdf.

[21] Orange County 2003 contract, note 20, at 34.

[22] See Levine, note 5.

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

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

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

[26] Bloomington County 2003 contract, note 23, at 3-4.

[27] Contract between Sacramento County and ES&S (2004) at 4, 8-9, *available at:* http://accurate-voting.org/contracts/CA/Sacramento/CA_sacramento_2004.pdf.

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

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.[29] 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.[30] For example, in DESI's 2001 contract with Alaska:

> It is expressly understood between the parties that [...] unit pricing constitute proprietary information the nature of which is a trade secret, and that disclosure of this information may place [DESI] at a competitive disadvantage.[31]

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.[32]

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.

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.[33]

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 [...]."[34]

These types of restrictions can prohibit types of analyses that require the voting system to be examined in a specific environment such as a lab or problematic polling place. If the vendor objects and does not give

[29] 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 § I(4), *available at:* http://www.law.upenn.edu/bll/ulc/fnact99/1980s/utsa85.htm.

[30] 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).

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

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

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

[34] Solano County 2003 contract, note 33, at 7. Also Bergen County contract, note 18, at 5, Contract between Pulaski County, Indiana and Microvote (2003), at 5, *available at:* http://accurate-voting.org/contracts/IN/Pulaski/IN_pulaski_2003.pdf. Contract between Miami County, Indiana and Microvote (2003), at 5, *available at:* http://accurate-voting.org/contracts/IN/Miami/IN_miami_2003.pdf. Contract between Dubois County, Indiana and Microvote (2003), at 5, *available at:* http://accurate-voting.org/contracts/IN/Dubois/IN_dubois_2003.pdf. Orange County 2003 contract, note 20, at 26. Contract between Yolo County, California and Hart (2006), at 8, *available at:* http://accurate-voting.org/contracts/CA/Yolo/CA_yolo_la_2006.pdf.

its written authorization, provisions like these can effectively hold up location-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.[35]

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 Product, Customer shall provide [DESI] with the source code for the modifications and/or enhancements.[36]

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.[37]

Finally, some contracts feel the need to clarify that voters or "individuals participating in an election"[38] 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."[39]

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 need to be recognized going forward, such as security evaluation, post-election auditing and election contests and litigation.

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"[40] to "as soon as possible"[41] to "as soon as public disclosure request is made"[42] to "promptly"[43] to "as much prior notice as reasonably practicable"[44] to no less than 10, 15 or 20 business days.[45] It is unclear why there is so much variation in these time periods.[46] 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.[47]

[35] Contract between Michigan and Diebold (2004), at 202, *available at:* http://accurate-voting.org/contracts/MI/MI_diebold_2004.pdf.

[36] Alaska 2001 contract, note 31, at 22.

[37] Note: as mentioned in Section 4.5 local jurisdictions are not typically given access to source code.

[38] Solano County 2003 contract, note 33 at 7.

[39] Orange County 2003 contract, note 20, at 17.

[40] Contract between Utah and DESI (2006), at 24-25, *available at:* http://accurate-voting.org/contracts/UT/UT_diebold_2006.pdf.

[41] Riverside County 2000 contract, note 17, at 8; Palm Beach County 2001 contract, note 25, at 12.

[42] Snohomish County 2002 contract, note 32, at 10-11.

[43] Contract between Georgia and DESI (2002), at 15, *available at:* http://accurate-voting.org/contracts/GA/GA_diebold_2002.pdf.

[44] Contract between Ohio and DESI (2004), at 14, *available at:* http://accurate-voting.org/contracts/OH/OH_diebold_2004.pdf; Contract between Cuyahoga County, Ohio and DESI (2005), at 7, *available at:* http://accurate-voting.org/contracts/OH/Cuyahoga/OH_cuyahoga_2005.pdf.

[45] Contract between Santa Clara County and Sequoia (2003), at 16, *available at:* http://accurate-voting.org/contracts/CA/Santa_Clara/CA_santaclara_2003.pdf; Contract between Alameda County, California and Sequoia (2006), at 23, *available at:* http://accurate-voting.org/contracts/CA/Alameda/CA_alameda_2006.pdf; San Bernardino 2003 contract, note 28, at 11.

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

[47] Contract between Bexar County, Texas and ES&S

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.[48] 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.[49]

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].[50]

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 4.1. This will tend to facilitate oversight through public records requests by ensuring that the customer will be shielded from any harm related to disseminating information about their voting system.

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 give 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.[51]

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.[52] Of course, this would have to be done carefully but the idea is a promising one.[53]

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."[54] 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.[55]

(2002), at 19, *available at:* http://accurate-voting.org/contracts/TX/Bexar/TX_bexar_2002.pdf; Contract between Will County, Illinois and ES&S (2003), at 9-10, *available at:* http://accurate-voting.org/contracts/IL/Will/IL_will_2003.pdf.

[48] "Contractor agrees that the contract will be a public document [...]" Utah contract 2006, note 40, 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, note 45, at 23.

[49] Yolo County 2006 contract, note 34, at 25.

[50] Palm Beach County 2001 contract, note 25, at 12. Similar language exists in other Florida contracts, see: Sarasota County 2001 contract, note 19, at 9; Contract between Pasco County, Florida and ES&S (2001), at 9-10, *available at:* http://accurate-voting.org/contracts/FL/Pasco/FL_pasco_2001.pdf.

[51] Ohio contract, note 44, at 9-10.

[52] Doug Jones, "Connecting Work on Threat Analysis to the Real World", presented at VSRW'06, a workshop on Threat Analysis for Voting System Categories, June 8, 2006, George Washington University, *available at:* http://www.cs.uiowa.edu/~jones/voting/VSRW06.pdf.

[53] 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.

[54] Utah contract 2006, note 40, at 11.

[55] Sarasota County 2001 contract, note 19, at 4.

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.[56]

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.[57]

Considering the increasing importance of source code analysis in conducting pre- and post-election oversight and auditing of voting systems,[58] having these provisions explicitly stipulated 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.[59]

In other smaller jurisdictions we see either complete absence of these kinds of provisions or explicit prohibition of access during an audit.[60] It is unfortunate that smaller jurisdictions don't seem able to negotiate access to source code as needed.[61]

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.[62]

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.

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.[63] 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.[64]

Unfortunately, the term "benchmark test" is not defined in these contracts and could be construed to cover any

[56] Utah contract 2006, note 40, at 11.

[57] Michigan 2004 DESI contract, note 35, pg. 34.

[58] See Hall note 3. 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. Two recent studies include: David Wagner, David Jefferson and Matt Bishop, California Voting Systems Technology Assessment Advisory Board, "Security Analysis of the Diebold AccuBasic Interpreter" ("VSTAAB Report"), February 14, 2006, *available at:* `http://www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf` (confirming the "Hursti I" attack); Alec Yasinsac, David Wagner, Matt Bishop, Ted Baker, Breno de Medeiros, Gary Tyson, Michael Shamos and Mike Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware" ("SAIT Report"), February 23, 2007, *available at:* `http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf`.

[59] Alameda County 2006 contract, note 45, at 28.

[60] "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 2003 contract, note 28, at 4-5.

[61] Smaller jurisdictions may not see a need for such access or may feel that requesting such access might cause them other difficulties. See the discussion in Aaron Burstein and Joseph Lorenzo Hall, "Troubleshooting Voting System Source Code Disclosure Laws", (2006), *in preparation; on file with author*.

[62] Alameda County 2006 contract, note 45, at 42.

[63] "CUSTOMER is prohibited from publishing the results of benchmark test runs on the Oracle Software." Bexar County 2002 contract, note 47, at 7.

[64] Also see Orange County 2003 contract, note 20, at 28.

kind of stress- or performance-testing, comparative or not.[65]

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.[66] For example, from the DESI contract with Alaska in 2001:

> [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].[67]

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.

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.

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 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.[68]

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 doesn't 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.[69]

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

[65] 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.

[66] Kim Zetter, "Did E-Vote Firm Patch Election?", *Wired News*, October 13, 2003, *available at:* `http://www.wired.com/politics/law/news/2003/10/60563`.

[67] Alaska 2001 contract, note 31, at 7. Similar provisions exist in: Contract between Kern County, California and DESI (2002), at 23, *available at:* `http://accurate-voting.org/contracts/CA/Kern/CA_kern_2002.pdf` ("90 days" to install); Solano County 2003 contract, note 33 at 8 ("20 days" to install).

[68] Restrictions such as these played a large role in recently preventing an audit team in Cuyahoga County from diagnosing a possible database corruption event. See: Collaborative Public Audit, note 1, at 35.

[69] Contract between Mendocino County, California and DESI (2003), at 6, *available at:* `http://accurate-voting.org/contracts/CA/Mendocino/CA_mendocino_2003.pdf`.

preoccupied with potential damage claims so as to prohibit all but the most trivial types of disclosure.

6 Future Work

There are a number of dimensions along which this work could be extended. In the Fall, we will 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 longitudinal hypotheses.

Acknowledgments

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 author 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.