LEGAL ISSUES FACING ELECTION OFFICIALS IN AN ELECTRONIC-VOTING WORLD

Samuelson Law, Technology & Public Policy Clinic
University of California-Berkeley School of Law (Boalt Hall)
http://samuelsonclinic.org

Aaron Burstein, Esq., ACCURATE Research Fellow,
Samuelson Clinic & Berkeley Center for Law and Technology

Stephen Dang, Ph.D., Student Intern

Galen Hancock, Student Intern

Jack Lerner, Esq., Samuelson Clinic Fellow

March 15, 2007

TABLE OF CONTENTS

Part I: INTRODUCTION & OVERVIEW

Recent publicity concerning the reliability and security of various electronic voting systems has increased public scrutiny of the machines themselves as well as the election process as a whole. The election officials who are responsible for selecting, maintaining, and operating electronic voting systems face not only public inquiry but also a thicket of state and federal legal issues.

We provide in this paper a general analysis of typical legal issues that elections officials face (or should consider). This paper, however, does not take the place of fact-specific legal advice. Officials should consult their own attorneys for advice regarding specific questions they may have.

This paper analyzes legal issues that surround three broad categories of activities that elections officials undertake, or might wish to undertake:

- **Security Testing.** Most vendor contracts explicitly permit a limited range of testing, typically limited to verifying software versions and testing basic system functions. An elections official, however, might wish to perform more stringent tests of a system's security against a variety of attacks. We discuss the contract, trade secret, and copyright issues that could arise from such testing.

- **Public Disclosure and Auditing.** Whether in response to public records requests, litigation, or public education efforts, election officials must confront the issue of revealing some of the details of the voting systems used in their jurisdictions. Similarly, elections officials might need to disclose these details to assist election audits. We discuss how trade secret, copyright, and security considerations might affect elections officials' abilities to make these disclosures.

- **Assembling Systems from Separate Components.** Finally, we discuss how state election codes and contract law, as well as copyright and trade secret law, might affect elections officials who wish to combine components from different manufacturers into a single electronic voting system.

Part II: LEGAL ISSUES IN ELECTRONIC VOTING SYSTEM TESTING

Every election system should be thoroughly evaluated for security and accuracy. There is a federal-level testing regime for voting systems, but many independent experts have noted that this process is not set up to detect security flaws.[1] Moreover, many states

[1] *See, e.g.*, Avi Rubin, *The Dirty Little Secrets of Voting System Testing Labs*, HUFFINGTON POST, Dec. 16, 2005, http://www.huffingtonpost.com/avi-rubin/the-dirty-little-secrets-_b_12354.html; *Certifying Vote Equipment: Hearing Before the Subcomm. on Environment, Technology, and Standards of the H. Comm. on Science*, 108th Cong. 38-86 (statement of Michael I. Shamos, Professor, Computer Science, Carnegie Mellon University: "the system we have for testing and certifying voting equipment in this country is not

and counties undertook rapid implementation of electronic voting systems as a way to comply with the Help America Vote Act of 2002's (HAVA) mandatory accessibility requirements by the January 1, 2006 deadline, which means that they have purchased machines without the benefit of forthcoming revisions to federal testing guidelines. As a result, some states and counties have attempted to do their own functionality and security testing.[2]

A brief overview of the federal testing process will provide some explanation of why state or county elections officials might want to conduct their own security testing. HAVA empowers the U.S. Elections Assistance Commission (EAC) to "provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories."[3] These "accredited laboratories" are private-sector laboratories,[4] also known as Voting System Testing Laboratories (VSTLs).[5] Under the EAC's testing and certification program, which became effective in January 2007,[6] VSTLs will be evaluated by the National Institute of Standards and Technology (NIST) and accredited by the EAC.[7]

Prior to this testing program, the National Association of State Election Directors (NASED) handled national-level certification.[8] Under the EAC-led effort, accredited labs will test electronic voting systems for compliance with the 2002 Voting System Standards (VSS), or the 2005 Voluntary Voting System Guidelines (VVSG) once they become effective on December 31, 2007.[9] The EAC will decide whether to certify voting systems based on the VSTL's recommendation, test report, and some additional

---

only broken, but is virtually nonexistent."); Avi Rubin, *Can a Voting Machine that is Rigged for a Particular Candidate Pass Certification?*, http://avirubin.com/vote/ita.challenge.pdf (last visited July 20, 2006).

[2] *See, e.g.,* California Secretary of State, Voting Systems, http://www.ss.ca.gov/elections/elections_vs.htm (last visited July 20, 2006); Associated Press, *Elections Supervisor: Some Diebold Voting Machines Can be Hacked*, Dec. 15, 2005. Georgia, Florida, Maryland, and Texas conduct significant state-level testing, but few smaller jurisdictions do.

[3] Help America Vote Act of 2002 [hereinafter HAVA] § 231(a)(1), 42 U.S.C. § 15371(a)(1).

[4] HAVA § 231(b)(1), 42 U.S.C. § 15371(b)(1).

[5] These laboratories are accredited by the National Institute of Standards and Technology's (NIST's) National Voluntary Laboratory Accreditation Program (NVLAP). NIST, National Voluntary Laboratory Accrediation Program (NVLAP) Home Page, http://ts.nist.gov/ts/htdocs/210/214/214.htm (last visited Sept. 22, 2006). VSTLs play a role formerly occupied by independent testing authorities (ITAs), which were accredited by the National Association of State Election Directors (NASED).

[6] *See* EAC's Voting System Certification Program, http://www.eac.gov/eac_vsc2.htm (last visited Jan. 25, 2007).

[7] HAVA § 231(b)(2), 42 U.S.C. § 15371(b)(2).

[8] The EAC, however, will not review voting system qualifications made under the previous, NASED-administered system.

[9] Testing and Certification Process for Voting Systems, http://www.eac.gov/testing_certification.htm (last visited Jan. 26, 2007). The 2002 Standards are available at http://www.eac.gov/election_resources/vss.html. The 2005 Guidelines are available at http://www.eac.gov/VVSG%20Volume_I.pdf and http://www.eac.gov/VVSG%20Volume_2.pdf [hereinafter "VVSG, vol. 1" and "VVSG, vol. 2," respectively].

procedural criteria.[10] States are not required to use federally certified systems, but 39 states have adopted this requirement in their state election codes.[11]

Several groups of experts have criticized the 2002 VSS, and the 2005 Voluntary Voting System Guidelines that will replace them in December 2007, as deeply flawed on substantive and procedural grounds.[12] This criticism has been further fueled by well-documented security holes and glitches in electronic voting systems that were certified and are used by states today.[13] Both sets of guidelines rely on functional testing that is ill-suited for testing security, accessibility, and other desirable system qualities.[14] The testing process is also opaque; reports on specific systems, and even information about the reasons a given system failed, are not made public. Testing reports are considered property of the vendors.[15] Conflicts of interest potentially taint the certification process since vendors pay for their own federal testing.[16] Finally, testing labs have no obligation to publicly disclose the full results of their testing. Understandably, many election administration officials are not satisfied with this process and wish to conduct further testing.

Partly in response to the shortcomings in federal testing, some states have updated their own election system certification processes. For example, California, Missouri, and Washington have amended their election laws to impose requirements that apply specifically to electronic voting systems.[17] State election laws might also grant the secretary of state (or other official with ultimate responsibility for the election system) the authority to issue regulations pertaining to electronic voting systems. Acting under his statutory powers, in October 2005, the California Secretary of State created a new

---

[10] *See* Testing and Certification Program Manual §§ 4 and 5 (ver. 1.0), http://www.eac.gov/docs/Voting%20System%20Testing%20and%20Certification%20Program%20Manual--Final%20--120506.pdf (last visited Jan. 25, 2006) (specifying criteria and procedures for certification).
[11] VVSG, vol. 1, at 6.
[12] *See, e.g.*, Ariel Feldman, J. Alex Halderman, & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Sept. 13, 2006, http://itpolicy.princeton.edu/voting/ts-paper.pdf; NATIONAL RESEARCH COUNCIL, ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING, (2005); ACCURATE, PUBLIC COMMENT ON THE 2005 VOLUNTARY VOTING SYSTEM GUIDELINES (2005), available at http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2005_vvsg_comment.pdf; Ellen Theisen, Myth Breakers: Facts About Electronic Elections (2005), *available at* http://www.votersunite.org/MB2.pdf.
[13] Harri Hursti, "SECURITY ALERT: July 4, 2005, Critical Security Issues with Diebold Optical Scan Design", Black Box Voting, *available at* http://www.blackboxvoting.org/BBVreport.pdf. Harri Hursti, "SECURITY ALERT: May 11, 2006, Critical Security Issues with Diebold TSx", Black Box Voting, available at: http://www.blackboxvoting.org/BBVtsxstudy.pdf. Brennan Center Task Force on Voting System Security, *The Machinery of Democracy: Protecting Elections in an Electronic World* (2006), *available at* http://www.brennancenter.org/Machinery%20of%20Democracy-%20Full%208.8.06.pdf.
[14] *Id.*; EAC, Voluntary Voting System Guidelines Introduction, http://www.eac.gov/vvsg_intro.htm (last visited Jan. 26, 2007); ACCURATE, Public Comment on the 2005 Voluntary Voting System Guidelines, Sept. 30, 2005, *available at* http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf.
[15] *See* Rubin, *Dirty Little Secrets*, *supra* note 1.
[16] *See id.*
[17] *See* CAL. ELEC. CODE § 19250; Missouri Code of State Regulations, Certification statement for new or modified electronic voting systems, 15 CSR 30-10.020 (2006); Washington State Register, Electronic Voting Requirements, 2005-05 WSR 52 (2005). Note that this list is merely illustrative; other states have adopted similar requirements.

Office of Voting System Technology Assessment and issued ten requirements for electronic voting systems.[18]

Although county elections officials might be required to conduct specific kinds of tests – such as logic, accuracy, and pre-election operation testing[19] – it is more often the case that state elections codes neither require nor prohibit additional testing.[20] Reasons that county elections officials might wish to conduct such tests include deciding between competing products and determining whether a given system meets local concerns, such as accessibility. The lack of guidance found in many state election codes, however, creates some uncertainty as to whether county elections officials are authorized to test electronic voting systems for these purposes.[21]

Electronic voting system vendors generally seek to more sharply define the authority of elections officials to test voting systems. The exact contractual provisions relating to testing are important, because testing that goes beyond those provisions exposes the county to potential liability under trade secret or copyright law (or both).[22] A typical vendor contract permits two types of testing, neither of which is likely to be adequate to detect system security flaws.[23] The first type, acceptance testing, is limited to testing the system to ensure that the machine's power supply and user interface are in working order. This testing must occur quickly, often within 30 days of delivery.[24] Second, typical vendor contracts allow logic and accuracy testing, which is limited to

[18] California Secretary of State, *Secretary McPherson Announces Statewide Electronic Voting System Requirements and New Office of Voting System Technology*, http://www.ss.ca.gov/elections/voting_systems/ovsta_press_release.pdf (Oct. 5, 2005). These requirements include escrow of the system's source code, volume testing, and providing a working system for testing if requested by the Secretary of State. *Id.*

[19] *See* CAL. ELEC. CODE §§ 19220 (mandating logic and accuracy testing) and 19321 (mandating pre-election operation testing).

[20] Recently, at least one county board of supervisors has demanded additional testing of electronic voting systems. According to a press release by Voter Action, the Alameda County (California) Board of Supervisors required a contract clause allowing "independent, expert security vulnerability testing" of Sequoia touch-screen voting machines as a "condition before payment" to Sequoia. Voter Action Website, http://www.voteraction.org/ (last visited Sept. 6, 2006). The signed contract, which was executed by the Alameda County Registrar of Voters, appears to lack this provision. *Id.*

[21] County elections officials might obtain this authorization at the county level. See, e.g., Leon County Supervisor of Elections, Office Information, http://www.leonfl.org/elect/?page=General%20Information/OfficeInformation.asp (last visited Jan. 28, 2007) (stating that the Supervisor of Elections has "exclusive control" over several matters relating to the conduct of elections).

[22] An elections official who conducts such tests might also be liable for breach of contract. Since this kind of claim depends heavily on the relevant state law and the language of the contract itself, we do not discuss it further.

[23] The authors examined roughly 20 contracts with elections vendors from jurisdictions in California, most of which were obtained via freedom of information requests or as part of California's Voting Modernization Board. We also interviewed election administration officials from California and Florida about their experiences in contract negotiations and with ongoing dealings with vendors.

[24] *Id.*

checking whether the software installed on a voting system appears to be of the correct version and whether the election system can tally votes correctly.[25]

A. Legal issue: Trade Secrets

Performing security testing of an electronic voting machine that was purchased under a contract containing the testing restrictions described above might subject an election official to liability for misappropriating trade secrets. A trade secret is defined as information that (1) derives independent economic value from not being generally known, (2) is not readily ascertainable, and (3) is subject to reasonable efforts to keep it secret.[26] Although trade secret owners might wish to prevent all others from learning the secret, they may also use a confidentiality or non-disclosure agreement to share without destroying trade secret protection. Information communicated orally or in writing may qualify for trade secret protection.

Trade secret law prohibits *misappropriation*, which may consist of using or disclosing a trade secret in violation of a duty to maintain secrecy (such as a non-disclosure agreement), or acquiring a trade secret through other "improper means," such as misrepresentation or espionage.[27] A trade secret owner may sue an alleged misappropriator for an injunction, damages, or both.[28]

We explore this issue through the following hypothetical.

Hypothetical #1 – Misappropriation by Disclosure That Violates a Confidential Relationship. An election official has copied the binary executable code from the voting system to a general-purpose computer owned by the jurisdiction. The county's contract with the vendor prohibits the official from providing access (outside of an election) to any component of the voting system to any person who is not employed by the elections official. Similarly, the contract prohibits the official from discussing the results of any pre-election testing with any person whom she does not employ.

Using a simple tool for reading textual phrases embedded in binary code, the elections official identifies what she suspects is a cryptographic key explicitly defined in one of the binary files. The election officials also discovers a text string that includes a warning that the binary's contents contain trade secrets and are protected by copyright.

---

[25] Contract between Diebold Election Systems, Inc. and the County of Alameda, Additional Provisions 11-12 (May 23, 2002). For a fuller description of logic and accuracy testing, see Douglas W. Jones, *Testing Voting Systems: Pre-election (Logic and Accuracy) Testing*, http://www.cs.uiowa.edu/~jones/voting/testing.shtml#landa (last visited Sept. 21, 2006).

[26] Uniform Trade Secrets Act ["UTSA"] § 1(4) (1985); *see also* CAL. CIV. CODE §§ 3426-3426.11 (enacting Uniform Trade Secrets Act with amendments). Because trade secrets are creatures of state law, the definition of "trade secret" may vary from state to state. Many states, however, have adopted the Uniform Trade Secrets Act with little or no modification, so the definition given in the main text is adequate for our general discussion. For the classical statement of the definition of a trade secret, see RESTATEMENT OF TORTS § 757, Comment b.

[27] *See* UTSA §§ 1(1)-(2).

[28] Indeed, successful trade secret plaintiffs often obtain both kinds of relief, though a court may deny one or both forms of relief in exceptional circumstances. *See* UTSA §§ 2(b), 3(a) (1985).

She consults a computer scientist and emails him relevant binary file. The computer scientist tells the official that this method of managing cryptographic keys is substandard and a serious threat to the voting system's security. Using one of the county's recently purchased electronic voting machines, the computer scientist confirms that the key defined in the binary executable code was indeed present in the machines delivered to the county, allowing anyone who knows this key to attack the system. The election official publicly describes the vulnerability, and the vendor immediately sues her for unauthorized disclosure of a trade secret and copyright infringement.

The confidentiality provisions found in a typical electronic voting system contract apply to a broad array of information, ranging from source code to technical design to poll worker manuals. In addition, some vendors label these and other documents as "confidential" or "secret" and include a contract term deeming all such documents trade secrets.

Within the context of Hypothetical #1, the elections official likely breached confidentiality by sharing the binary executable code with the computer scientist. The official might also have violated trade secret protection in the vendor's hardware and software by allowing the computer scientist access to a voting machine outside of an actual election. Thus, it would appear from the facts of the hypothetical that the vendor has a strong misappropriation claim against the elections official.

Potential Defenses.

A number of defenses might apply to the official's conduct.

- **The information is generally known or can be easily discovered.** If the binary executable code were readily available, the vendor likely would have lost trade secret protection in it, despite the statement in the electronic copy that the code was "secret."[29] Moreover, the contractual duty to maintain secrecy likely would not be enforceable in light of the general availability of the code. The law on this point, however, varies from state to state.[30] More generally, the use of "confidential" labels on widely disclosed documents, such as poll worker guides, is unlikely to create trade secret protection in those materials, since they are routinely shown to persons who have no duty to maintain secrecy.

- **Other law supersedes the contract.** If the law requires the county to disclose certain information, it probably can't be covered by the confidentiality provision.[31] A provision providing that every file created

[29] Although vendors ordinarily take care to protect against inadvertent disclosure, it has happened. *See Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).
[30] *See* James Pooley, TRADE SECRETS § 3.04[3] (citing cases from Maine, New Jersey, Pennsylvania, and Washington).
[31] Persons dealing with government agents are held to have notice of statutory limitations on their authority, which limits the contracts that they can agree to. *E.g.*, Wilber Nat'l Bank v. United States, 294 U.S. 120, 123-24 (1935); *see also* CAL. CIV. CODE § 1667.

by the elections system is confidential information belonging to the vendor, for example, probably will not be enforceable, because state elections codes typically require that some of those documents be made public.[32] (Many contracts explicitly provide that conflicting state law supersedes the terms of the contract.[33]) But not all potentially applicable laws will supersede contracts. Most public records laws, for instance, would not supersede a confidentiality provision, because these laws ordinarily have exemptions for trade secrets and other commercial information.[34]

- **Public Policy Defenses.** The First Amendment might provide a defense to trade secret misappropriation in Hypothetical #1. As one scholar has noted, the First Amendment traditionally has protected disclosures of secret information when the disclosure relates to "'matters of substantial concern,'" such as public safety and public health.[35] Security vulnerabilities in a voting system are undoubtedly of great public concern. This defense, however, might be limited by the fact that a government official, rather than a private person, is disclosing the trade secret. Although the U.S Supreme Court has recognized a right of "government speech,"[36] the scope of that right is relatively underdeveloped in general and untested in the context of trade secret misappropriation. A full analysis of this issue is beyond the scope of this paper.[37]

Avoiding Trouble

The likely success of a misappropriation claim in Hypothetical #1 suggests two steps that elections officials might take to avoid liability:

- **Bring experts in-house.** One potential way to conduct testing without violating a confidentiality provision is to give the tester some kind of

[32] *See, e.g.*, CAL. ELEC. CODE § 17303-04 (providing for records of election to be retained by elections official and available for public inspection).
[33] Kern County Contract at 24 (contract does not bar disclosure required by court, but owner of confidential information must have opportunity to oppose disclosure) (on file with authors).
[34] CAL. GOV. CODE § 6254.15 (exempting "corporate financial records" and "corporate proprietary information including trade secrets"); Fla. Stat. § 119.071(f) (2005) (exempting software that is a trade secret).
[35] Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment* 14-15 (draft as of Aug. 9, 2006) (quoting American Law Institute, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1993)), *at* http://www.ischool.berkeley.edu/~pam/papers/TS%201st%20A%204th%20dr.pdf. *See also* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261 (1998).
[36] *See generally* Johanns v. Livestock Mktg. Ass'n, 544 U.S. 550 (2005).
[37] Statutes protecting "whistleblowers" against misappropriation liability are also worth considering but are probably unlikely to provide a defense for the government official. A provision in California's trade secret law protects "persons employed by public entities [who] report improper government activity" from liability for trade secret misappropriation. CAL. CIV. CODE § 3426.11. It is unclear whether this statute covers the disclosure in Hypothetical #1.

official status within the county government. If the tester is actually a county employee or serves in some official capacity, it may be possible to assert that he may access confidential information in the same way as technicians and other staff. Depending on how the contract is written, even outside contractors may be covered on the theory that the testing they perform is a part of the county's elections work.[38] Whether this defense is viable will depend on state law—mere "use" of a trade secret can constitute misappropriation[39]—and the details of the relationship between the tester and the vendor. An important limitation on this strategy is that it does not offer any clear defense to public disclosure of a vulnerability. Whether a county would want to disclose the vulnerability will depend on the particular situation, but the fact that the vulnerability was discovered by a county employee or official would do little, if anything, to alleviate potential liability for unauthorized trade secret disclosure.

- **Limit confidentiality provisions in vendor contracts.** A provision that allowed the elections official to consult with a computer security expert, subject to the appropriate non-disclosure agreement, might have avoided trouble. A provision that required the elections official to notify the vendor, and obtain its approval, before consulting an expert might make this provision more palatable to the vendor.

Given the breadth of confidentiality obligations found in a typical vendor contract, we anticipate that election officials will primarily be concerned with claims based on those contracts. Nevertheless, it is also worth keeping in mind that a contractual duty of secrecy is not necessary for misappropriation; acquiring a trade secret from a person who is known to have used "improper means" to acquire the secret is also misappropriation. This form of liability might arise, for example, from learning about a voting system vulnerability from a vendor's employee who is known to be under a non-disclosure agreement. For the most part, however, situations giving rise to this kind of misappropriation liability bear little relevance to the security testing context.

B. Legal Issue: Copyright

In response to some election administration officials' attempts to conduct security testing of voting systems that they purchased, vendors have claimed that such testing would infringe their copyrights.[40]

---

[38] A recent copyright case, *StorageTek v. Custom Hardware Eng'g & Consulting*, 421 F.3d 1307 (Fed. Cir. 2005), reached an analogous result. The case dealt with a consulting firm that did maintenance work on computer backup systems without the vendor's permission.

[39] UTSA § 1(2).

[40] *See, e.g.,* Zachary Goldfarb, *As Elections Near, Officials Challenge Balloting Security*, THE WASHINGTON POST, Jan. 22, 2006; Letter From Michael E. Lindroos, Diebold Election Systems, Inc. to Ion Sancho (Jan. 31, 2006), *available at* http://www.bbvdocs.org/diebold/threat-letter.pdf (alleging "potential violations of our licensing agreements and intellectual property rights"); *cf. Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004) (vendor alleged copyright in e-mails and other documents about workings of electronic voting system).

Copyright: The Scope of Protection, and What Constitutes Infringement.

Practically every form of original expression – including books, plays, and song lyrics, as well as computer programs in source code and binary forms – that can be "fixed in a tangible medium" is protectable under copyright law.[41] Media that qualify as "tangible" range from paper to a computer's random-access memory (RAM),[42] which can be easily overwritten and is effectively erased when the computer is turned off.

Copyright law grants the author (or whoever holds the copyright) a number of exclusive rights, including the right to reproduce – i.e., to copy – the work. In 1998, Congress enacted the Digital Millennium Copyright Act (DMCA), which protects "a technological measure that effectively controls access to" a copyrighted work.[43] The DMCA not only prohibits circumvention of an access control, but also trafficking in a circumvention device.[44] In other words, while traditional copyright law protects the content of a digital work, the DMCA protects the "locks" on digital works, such as an encryption scheme, and prohibits sending around unauthorized "keys" that defeat these locks.[45]

Both branches of copyright law have implications for security testing by elections officials. We provide another hypothetical as a vehicle for discussing potential violations of copyright law, as well as potential defenses.

Hypothetical #2: A county recently purchased an electronic voting system. Concerned about a rumored vulnerability that allows an attacker to manipulate ballot data on its way to a central vote tabulator, the county election official performs the security testing herself. During the testing, she enters a cryptographic key that allows her to access a ballot data processing program that resides in the voting machine. The county's contract with the vendor contains a license for the voting machines' software, which states that the county may use the software only for specified purposes – acceptance

---

[41] 17 U.S.C. § 102(a).

[42] *See* MAI Sys. Corp. v. Peak Computer, 991 F.2d 511 (9th Cir. 1993). *But see also* U.S. Copyright Office, DMCA SECTION 104 REPORT 111, 122 (2001) (noting that "many uses of works that entail RAM copying are expressly or impliedly licensed. In addition, exemptions, such as fair use, that apply to copying in other contexts apply in this context as well.").

[43] 17 U.S.C. § 1201(a)(1)(A) (prohibiting circumvention of a "technological measure that effectively controls access to a work protected under this title"); § 1201(a)(2) (prohibiting trafficking in circumvention devices).

[44] *Id.*

[45] *See, e.g.*, Timothy Wu, *Copyright's Communications Policy*, 103 MICH. L. REV. 278, 351 (2004). There is some debate about what measures qualify as "technological measures" and what qualifies as a circumvention tool. Both the DMCA itself and the First Amendment impose some limits. For example, one well-publicized case was based on the allegation that an academic paper discussing vulnerabilities in a digital music protection scheme. The United States, writing as a friend of the court, took the position that the DMCA proscribes neither the research that led to this paper, nor the publication of the paper itself. *See* Brief of the United States in Support of the Motion to Dismiss, Felten v. RIAA (Nov. 8, 2001), CV-01-2669 (GEB) (N.D. Cal.), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011108_doj_reply_brief.html.

testing, operational testing, and actual voting – and may not make unauthorized copies of the software. The contract also prohibits copying the technical manuals for the voting machines. The official attempts the attack described in the rumors and confirms that it is successful. She publicly discloses this result.

After learning of the elections official's test, and subsequent disclosure of the vulnerability, the vendor sues the official for (1) making unauthorized copies of the voting system software and (2) circumventing the technological measure that controls access to the system's ballot image manipulation software.

Copyright Violation: Unauthorized Reproduction

As stated above, several courts have found that copying a computer program from a hard disk into RAM – a step that is necessary to use the program – involves making a "copy" within the meaning of the Copyright Act. Thus, when the elections official used a voting machine to test for a vulnerability in the ballot image manipulation software, she made copies of the system's software. Since the vendor holds the exclusive right to reproduce its software,[46] and it did not authorize this use, it has made a plausible claim of copyright infringement.

There are, however, three powerful defenses that the elections administrator could assert.

Infringement Defense #1: Copying Not Within the Scope of the Exclusive Rights, and Therefore Not Infringing

The first line of defense to the allegation of copyright infringement in Hypothetical #2 is that the election official's actions fell under a copyright limitation that protects users of computer software. Specifically, the Copyright Act expressly limits the rights of a computer program copyright holder to limit reproduction of that program; it is not an infringement for the owner of a copy of a computer program to "make a new copy . . . [that is] created as an essential step in the operation of the program . . . ."[47]

The use described in Hypothetical #2 appears to fit this limitation rather well. The election official performed the security test in her capacity as an official of the county, which owns the copy of the voting system software.[48] In addition, the reproduction that she made was essential step in the use of the program. The election official was using the program for the purpose for which it was written; the official did not modify the program or create derivative works. Moreover, she used them on the

[46] 17 U.S.C. § 106(1).
[47] 17 U.S.C. § 117(a)(1).
[48] It may be the case that the county does not hold title to the copy of the voting system software, but rather holds a license to use the copy. Since the license gives the county the right to possess the copy, however, this fine distinction is unlikely to make § 117 inapplicable. *See* Krause v. Titleserv, Inc., 402 F.3d 119, 122-25 (1st Cir. 2005) (concluding that rightful possession of a copy of a computer program for an indefinite period and without material restrictions constitutes ownership for the purposes of 17 U.S.C. § 117).

machine with which the program was sold. Finally, although it appears that no court has decided whether operating a program specifically for security testing constitutes an "essential step" in the use of the program, courts have found that copying a program in order to fix bugs or update data are "essential steps."[49] Testing whether the software contained an exploitable security vulnerability is also likely to be viewed as an "essential" step in the program's operation, although it appears that no court has ruled on this specific question.

Conclusion: Statutorily Protected Reproduction. The election official described in Hypothetical #2 has a strong argument that her use of the voting system software was non-infringing under a provision of the Copyright Act that truncates the exclusive rights in a computer program roughly at the line of customary use by the owner of a copy.

Infringement Defense #2: Fair Use

Fair use doctrine presents the elections official with perhaps the strongest defense to a claim of copyright infringement.[50] The fair use statute is notably flexible (or frustratingly vague); its preamble mentions certain purposes for which unauthorized copying (or other kinds of potential infringement) might not be infringement and then directs courts to consider four (or more) factors in deciding whether a use is fair. Below, we present these factors and discuss how they might apply to the infringement claim in Hypothetical #2.

- **Effect on market for or value of the work.** The Supreme Court has referred to the impact of use on the market of the copyrighted work as "the single most important element of fair use."[51] The Court has clarified that copyright law protects rightsholders from harm done by copies that *substitute* for the original; but harm that flows from criticism is not "cognizable."[52]

  In the case of security testing authorized by a county election official, copying during testing is required to determine the adequacy of the security measures. The results aid the election official's decision on whether to purchase the electronic voting system. While the results of security testing may harm sales, the testing results do not provide an alternative or substitute for the original work. For example, criticism of a voting system that involves some copying of the system's software might have the effect of reducing demand for that system. In order to make this factor weigh in its favor, the voting system vendor

[49] See id. at 125-26. *See also* Aymes v. Bonelli, 47 F.3d 23 (2d Cir. 1995).
[50] 17 U.S.C. § 107. As discussed in the main text, the statutory definition of fair use is quite vague and has been extensively interpreted by the federal courts.
[51] Harper & Row v. Nation Enters., 471 U.S. 539, 566 (1985).
[52] *See* Cambell v. Acuff-Rose Music, Inc., 510 U.S. 569, 591-92 (1994) ("We do not, of course, suggest that a parody may not harm the market at all, but when a lethal parody, like a scathing theater review, kills demand for the original, it does not produce a harm cognizable under the Copyright Act.").

would have to show that the election official's test harmed the vendor's position in the market for some form of copyrightable derivative works, perhaps security testing reports. Hypothesizing such harm would be inadequate; the vendor would have to show that it had entered, or at least had plans to enter, that derivative works market.[53] For these reasons, security testing probably would not be found to appropriate the market for electronic voting systems and likely would not weigh against fair use.

- **Purpose and character of the use.**[54] The preamble of the fair use statute provides an illustrative list of potentially noninfringing uses – such as criticism, comment, news reporting, and scholarship – but this list is neither exhaustive, nor does it grant automatic protection to copying undertaken for these purposes.[55] Instead, several additional factors inform the purpose of use. For example, copying for commercial purposes tends to weigh against fair use, though such copying is not necessarily infringing.[56] Copying for educational purposes weighs in favor of fair use, though at least some nexus between the copier and the educator appears to be necessary.[57] Lower courts have also found that making copies of a work in order to extract facts—which are not protectable by copyright—is a type of use that weighs in favor of fair use.[58] More generally, courts recognize that fair use requires striking a balance between "the interests of authors and inventors in the control and exploitation of their writings and discoveries on the one hand, and society's competing interest in the free flow of ideas, information, and commerce on the other hand."[59]

  Although courts have yet to determine the "purpose and character" of copying to conduct the kind of security testing presented in Hypothetical #2, good faith testing in order to facilitate more informed discussion of electronic voting systems seems unlikely to be characterized as a commercial use. A court would likely hold that security testing is non-commercial in nature, and that such testing implicates a high degree of public interest. In turn, disseminating

[53] *See id.* at 590.
[54] 17 U.S.C. § 107(1).
[55] 17 U.S.C. § 107. *See also Acuff-Rose*, 510 U.S. at 578 (explaining that the preamble is "illustrative and not limitative"); L.A. Times v. Free Republic, 54 U.S.P.Q.2d 1453 (C.D. Cal. 2000) (rejecting fair use defense despite a news reporting use).
[56] *Compare* Harper & Row v. Nation Enterprises, 471 U.S. 539, 566 (1985) *with* Harper & Row *with Acuff-Rose*.
[57] *See* Princeton Univ. Press v. Michigan Doc. Svcs., 99 F.3d 1381, 1383 (6th Cir. 1996); Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522, 1529-35 (S.D.N.Y. 1991).
[58] *See* Sony Computer Entertainment Am., Inc. v. Bleem, LLC, 214 F.3d 1022, 1026-28 (9th Cir. 2000) (approving of defendant's copying screen shots of plaintiff's video games for the purpose of comparative advertising); Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1527-28 (9th Cir. 1992) (analyzing copying an entire software program in order to gain access to the program's unprotectable "functional" elements).
[59] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

security testing results would also elicit a high degree of public interest and thus raise strong First Amendment arguments in favor of fair use.

- **Nature of the copyrighted work.** Courts consider a broad array of a work's characteristics under this factor. Two considerations might be especially important in the context of Hypothetical #2, and security testing more generally. First, computer software is not considered a fictional work and thus tends to receive thinner copyright protection.[60] Second, the vendor in our hypothetical did not publish its source code or make executable versions of its software widely available. While the first consideration clearly weighs in favor of fair use, the fact that the code was unpublished presents a more subtle issue. Although the Supreme Court has held that the "fact that a work is unpublished is a critical element of its 'nature,'" the work in question in that case was destined for publication; and the breach of confidentiality in handling that manuscript arguably harmed both the copyright holder's creative control and financial interests.[61]

  In Hypothetical #2, the purpose of not publishing source code is twofold: to prevent competitors from using the code and to prevent vulnerabilities from being discovered. The testing in Hypothetical #2 is unlikely to lead competitors to use it: it seems unlikely that competitors would want to use such code, and in any event the elections official did not publish the code. Although it is true that the elections official probably would not have confirmed the security vulnerability without running an unauthorized copy on the county's election machine, there is a countervailing public interest in obtaining better information about electronic voting system security. Thus, this factor is unlikely to weigh heavily for or against fair use.

- **Amount and substantiality of the work used.** The less of a work that is copied, or the less substantial is the portion that is copied, the more likely it is that that use is fair. As the Supreme Court has put it, a finding that "no more was taken than was necessary" weighs in favor of fair use.[62] However, it would be difficult, if not impossible, to conduct the kind of security testing described in Hypothetical #2 without making at least temporary copies of entire software programs. Thus, this factor is unlikely to weigh against a finding of fair use.

Conclusion: Fair Use. Under each of the four factors used to assess the fair use defense, security testing presents a strong case for the defense. Specifically, a finding of fair use likely turns on the purpose of the testing. Election officials, academics, and watchdog agencies that seek to improve the security of voting systems can make the strongest case for fair use defense because such testing does not attempt to appropriate

[60] NIMMER ON COPYRIGHTS § 13.04.
[61] *Harper & Row* 471 U.S. at 564.
[62] *Acuff-Rose*, 510 U.S. at 587 (internal quotation and citation omitted).

the commercial value of the copied work. The purpose of this testing is instead to evaluate or criticize the original work. As a result, elections officials should be able to assert a strong fair use defense to copyright infringement claims relating to security testing.

Infringement Defense #3: Copyright Misuse

Several federal courts of appeal have recognized copyright misuse as a defense to infringement.[63] Copyright misuse occurs when a copyright holder asserts its rights in a manner "contrary to the public interest" in copyright.[64] This "public interest," according to the courts that have recognized the misuse defense, is that the grant of limited, exclusive rights will achieve the constitutionally specified purpose of encouraging the creation of new works. Copyright misuse is a potentially broad defense; a finding of misuse bars a copyright holder from enforcing its copyright against *any* infringing activity that occurred during the period of misuse. Thus, an alleged infringer need not have been directly subject to misuse to employ this defense.[65]

Courts recognize at least two triggers for asserting copyright misuse. First, the copyright's exclusive rights constitute a "limited monopoly" that is an "exception to the general public policy against restraints of trade."[66] Unsurprisingly, courts have allowed the misuse defense in cases in which a copyright holder has asserted its rights in a potentially anticompetitive manner.[67] Second, copyright misuse and other defenses and limitations have grounding in the First Amendment:

> The spirit of the First Amendment applies to the copyright laws at least to the extent that the courts should not tolerate any attempted interference with the public's right to be informed regarding matters of general interest when anyone seeks to use the copyright statute which was designed to protect interests of quite a different nature.[68]

Copyright misuse might be available as a defense under the facts of Hypothetical #2. Testing of electronic voting machines implicates competition in several ways. Performing security testing, or reviewing the results of such tests, before purchasing or leasing a machine would provide a powerful means for jurisdictions to compare one element of different machines' performances. Even if it is impossible to test machines before purchase, the results of these tests could affect the next round of purchases within that jurisdiction, or could influence the decisions of other jurisdictions. The availability

---

[63] The copyright misuse doctrine was created by analogy to the more established defense of patent misuse.
[64] Video Pipeline, Inc. v. Buena Vista Home Entm't, 342 F.3d 191, 204-05 (3d Cir. 2003).
[65] Lasercomb Am., Inc. v. Reynolds, 911 F. 2d 970, 979 (4th Cir. 1990).
[66] *Lasercomb*, 911 F.2d at 977-78.
[67] The "typical misuse case" involves "an anti-competitive licensing agreement." *Video Pipeline*, 342 F.3d at 205. Prevailing on a copyright misuse defense, however, does not require proof that the copyright holder has violated the antitrust laws. *Practice Mgmt. Info. Corp. v. Am. Med. Ass'n*, 121 F.3d 516, 520 (9th Cir. 1997).
[68] *Video Pipeline*, 342 F.3d at 205 (quoting Rosemont Enters., Inc. v. Random House, Inc., 366 F.2d 303, 311 (Lumbard, J., concurring)).

of independent test results could, in the long run, spur competition among vendors to improve security beyond what is required under federal guidelines. Thus, although election officials do not produce competing products and are unlikely to start doing so, these officials constitute an overwhelming majority of the purchasers of (and dollars spent on) electronic voting systems. Restricting elections officials' ability to obtain full information about the security of the available systems, in turn, limits vendors' incentives to respond to demands for improved security.

Election officials might also be able to use the copyright misuse defense through an appeal to the broader concern with preserving public debate. Courts have recognized that criticism of a work is a kind of creative activity that copyright law seeks to encourage and protect; asserting a copyright in a manner that suppresses criticism therefore might constitute misuse.[69] As discussed in the fair use analysis above, security testing of electronic voting systems is a kind of criticism; the objective of such testing is to discover and describe vulnerabilities in order to encourage the development of more secure machines. It would be difficult, if not impossible, to perform security testing without copying an electronic voting system's software, which raises the possibility that enforcement of copyright would suppress this critical activity.

Moreover, the only legitimate sources of electronic voting systems' software are the vendors themselves. Election officials and others, of course, would be free to criticize electronic voting systems without performing security testing; but the quality of this criticism would likely be inferior to analysis that is informed by the kind of testing that we have discussed here. Ensuring that electronic voting systems provide verifiable, secure, and accurate elections is of obvious importance; public debate on this issue is impoverished if key participants — election officials — are limited by concern of committing copyright infringement. As a court that was presented with a copyright misuse defense relating to the alleged infringement of internal e-mails obtained from Diebold Election Systems, Inc. ("DESI") noted, "[i]t is hard to imagine a subject the discussion of which could be more in the public interest" than electronic voting system problems.[70]

Conclusion: Copyright Misuse. The use of copyright misuse doctrine as a defense to a copyright infringement claim involving electronic voting systems warrants some caution. It is a relatively new defense, which the U.S. Supreme Court has yet to

---

[69] For a clear statement of a court's concern with preserving critical expression as well as the drawing of a clear relationship of competitive activity and critical expression through the promotion of creative production, see *Video Pipeline*:

> A copyright holder's attempt to restrict expression that is critical of it (or of its copyrighted good, or the industry in which it operates, etc.) may, in context, subvert — as do anti-competitive restrictions — a [sic] copyright's policy goal to encourage the creation and dissemination to the public of creative activity.

342 F.3d at 205-06.

[70] Online Pol'y Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004). This court, however, did not decide the copyright misuse question, because the plaintiffs eventually withdrew that claim. *Id.* at 1199 n.4.

recognize as a defense to infringement.[71] Moreover, cases in which litigants successfully asserted copyright misuse have generally prevailed on a finding that the copyright holder behaved anticompetitively.[72] Thus, the scope of the public debate rationale for the copyright misuse defense, and the conditions under which it might apply to elections officials, are particularly uncertain.

Copyright Violation: Circumvention of a Technological Measure.

The argument for applying the DMCA to our hypothetical elections official's actions is as follows: By using a cryptographic key, she obtained access to the voting system's ballot data processing software. Although the voting machine would perform this operation during normal use, it does not rely on the machine's operator to do so. Thus, under normal operation, the elections official would not have access to the ballot image software at all. Moreover, the vendor might argue, the voting system software license does not extend to security testing, further supporting the argument that the elections official was not authorized to access the ballot image software.

Before making this argument, however, the vendor would have to establish that the DMCA applies to the ballot data processing software in the first place. The DMCA requires that a technological protection measure, such as encryption, "effectively controls" access to the copyrighted work. Unless this program is encrypted (or otherwise protected) to all other means of access to the software, there might not be an effective measure controlling access to the data processing software. On the other hand, if the cryptographic key that the official entered does serve to decrypt the software itself, then the DMCA would likely apply.[73] Even so, the vendor would still have to show some connection between the election official's access to the ballot data processing software and copyright infringement in order to make a claim under the DMCA.[74] As explained above, the election official has a few strong arguments to prove that she did not infringe the vendor's copyright at all.

---

[71] *Video Pipeline*, 342 F.3d at 204 (stating that the Supreme Court has not "affirmatively recognized the copyright misuse doctrine"). *See also* Brief for the United States as Amicus Curiae, Practice Mgmt. Info. Corp. v. Am. Med. Ass'n (Aug. 1998) (noting "the limited development and relatively rare invocation of the copyright misuse defense in the courts of appeals"), *available at* http://www.usdoj.gov/atr/cases/f2000/2076.htm.

[72] *See, e.g.*, *Lasercomb*, *PMIC*. *Cf. Video Pipeline* (giving broad exposition to the public debate rationale but holding that this rationale did not support application of the doctrine in this case). In a case that is currently pending in the Northern District of California, English professor Carol Schloss is claiming copyright misuse on the ground that "the Estate [of author James Joyce] is using threats of copyright infringement to restrain Schloss's free speech and artistic expression in order to illegally extend the scope of Defendants' copyright." Complaint, Schloss v. Sweeney ¶ 127 (N.D. Cal. C 06 3718, June 12, 2006), *available at* http://cyberlaw.stanford.edu/Complaint%20Endorsed%20Filed%206-12-06.pdf. Given the early stage of this litigation, it is impossible to say whether this case will bring additional guidance to the copyright misuse doctrine.

[73] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546-48 (6th Cir. 2004).

[74] Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203-04 (Fed. Cir. 2004).

Still, to anticipate other cases in which there is more obviously an effective access control in place, as well as a stronger claim of copyright infringement, we discuss applicable defenses to the alleged DMCA violation.

Defense: Security testing exemption. The DMCA provides an exemption for "security testing," which it defines as "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network."[75] In addition, the security testing exemption to the DMCA applies only if the act of testing "does not constitute infringement" under the other parts of the Copyright Act.[76]

It is likely that our hypothetical election official's actions qualify as security testing.[77] Also, as the official responsible for running elections in her county, which owns the voting machine, the elections official in Hypothetical #2 is probably authorized.[78] Moreover, though the jurisdiction does not own the copyrights to the software that the voting system uses, the elections official is probably an "operator" of the software, and therefore empowered by the security testing exemption to authorize testing.[79] Thus, the DMCA's security testing exemption probably applies to the facts of the hypothetical.

But this exemption might not find such easy application in other situations. For instance, if the election official had performed her testing before the county purchased the voting machines, it is unclear whether she would have met the authorization requirement.[80] Or, an academic researcher or activist group might want to test the cryptographic soundness of code that has been leaked to the Internet.[81] In such cases, a court may apply the security testing exemption to these testers because they share the intent of improving effectiveness of electronic voting systems prior to implementation.[82] Their testing is also unlikely to facilitate infringement of the voting system's software.[83]

---

[75] 17 U.S.C. § 1201(j)(1).

[76] Because the discussion of fair use given above applies equally to this element of § 1201(j), we do not give a separate analysis of infringement in this section.

[77] *See* H.R. 105-796, at 67 (Oct. 8, 1998) (stating that the purpose of the exemption is to allow testing of the effectiveness of a security measure before it is implemented).

[78] It is possible that the vendor would argue that the county does not own the software: the county has a license to use a copy of it and does not own the copyright. This reading of § 1201(j), however, is in obvious conflict with the overall structure of that section, and we do not consider it further. A related question is whether an elections official may authorize security testing of an electronic voting system that the jurisdiction leases, rather than owns. Section 1201(j) permits a computer system "operator" to authorize testing, a description that is likely to apply to the elections official.

[79] *See* 17 U.S.C. § 1201(j)(1) (authorizing an "owner or operator" of a "computer, computer system or computer network" to authorize security testing).

[80] Unfortunately, there is no case law interpreting this requirement.

[81] *See Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004). A helpful archive of court filings in this case is available at http://www.eff.org/legal/ISP_liability/OPG_v_Diebold.

[82] See 17 U.S.C. § 1201(j)(3) (providing that using security testing "solely to promote the security of the owner or operator" of the computer system and "in a manner that does not facilitate infringement"

[83] *See id.*

Conclusion: Circumvention of a technological measure. The use of cryptography in this system does not necessarily mean that the DMCA applies. Assuming that the DMCA does apply, the security testing exemption to the DMCA's anti-circumvention provision might apply to the hypothetical elections official described above, but this exemption is virtually untested in court. It is even less clear that this exemption would apply to a security tester who is not employed by or affiliated with an elections official. Finally, the requirement that security testing not involve infringement greatly complicates the use of this defense, since it might require the elections official (or other party) to prove that his or her testing was a fair use of the software or otherwise did not infringe a copyright.

Part III: LEGAL ISSUES IN PUBLIC DISCLOSURE AND AUDITING

Election administration officials have many reasons for disclosing information about electronic voting systems: they are frequently approached by members of the public who seek access to information about elections; they may desire public input or expert guidance to ensure that their voting systems are accurate and secure; and they may endeavor to assure the public of the same. Conducting a sound audit of an electronic voting system might also require disclosure of some voting system details. Disclosure in these situations is governed by the intersection of state public records laws, trade secrets, and copyright law.

Nearly every state has a statute that requires government agencies to make "public records" available for public inspection.[84] Public records statutes generally have three features: (1) a definition of "public records"; (2) the definition of government agencies' duty to public records available; and (3) the enumeration of exceptions to the definition of a public record, or the duty to disclose a public record. The typical definition of a public record is very broad – including essentially all documents, in any form, created in the course of official government business – and public records statutes generally require that the government provide these records to any person who requests them.

Although certain records relating to electronic voting, such as vendor contracts (with the possible exception of price terms), contain no trade secrets and fall squarely within the typical definition of a public record, other kinds of voting system-related information might qualify for an exception to the duty to disclose. Some of the most important exceptions for elections officials to consider are for trade secrets or confidential information[85] and for security-related information.[86] In addition, copyright law might constrain election officials' ability to fulfill public records requests.

---

[84] The popular titles of these laws vary from state to state – e.g., sunshine laws – but we refer to them generically as public records laws or public records statutes. For examples of such statutes, see CAL. GOV'T CODE §§ 6250-6254.18; FLA. STAT. § 119; N.Y. PUB. OFF. LAW §§ 84-90.

[85] *See, e.g.*, ALA. STAT. § 40.25.120(4) (creating public records disclosure exception for "records required to be kept confidential by a federal law or regulation or by state law"); CAL. GOV. CODE § 6254.15 (creating exception for "corporate proprietary information including trade secrets"). Even if a state's public records statute does not contain an explicit exemption for trade secrets, it is possible that disclosure of a trade secret without the owner's consent would violate the Takings Clause of the Fifth Amendment. *See* Ruckelshaus v. Monsanto, 467 U.S. 986 (1984) (applying the Takings Clause to trade secret disclosure by

To see how these exceptions might work in practice, consider the following hypothetical:

Hypothetical #3.[87] After a particularly close election in State X, a citizen files a proper request with the Secretary of State for access to the central ballot database created by the X's electronic voting system. The Secretary denies the request on two grounds. First, he cites the voting system vendor's objection that the database is encoded in a "proprietary" format that has not been publicly disclosed. Second, the Secretary states that the database might contain information that would facilitate attacks against the voting system, and that public disclosure of the database format itself might aid such attacks.

A. Legal Issue: Trade Secrets/Confidentiality Exception

The trade secret issue in Hypothetical #3 lies in the fact that the database format is secret, and the vendor has not authorized disclosure. Recall that a trade secret is information that (1) derives independent economic value from not being generally known, (2) is not readily ascertainable, and (3) is subject to reasonable efforts to keep it secret. Although the application of this definition will depend on the details of a specific case, it is worth remembering that a file format must satisfy all three elements of this definition in order to be protected as a trade secret.

However, even if a vendor's database file format lacks trade secret protection, or if releasing a copy of the file would not constitute disclosure of the secret, election officials must determine whether the file format is *confidential* and, if so, whether that state's public records statute permits disclosure. As stated above, many public records statutes protect confidential information from disclosure. What qualifies as confidential is, in turn, partially specified by contract – a contract cannot create trade secret protection for information that is not secret or does not gain independent economic value from being secret[88] – and may include software design.[89] Although a contract might provide that the

---

the U.S. Environmental Protection Agency); Philip Morris, Inc. v. Reilly, 312 F.3d 24 (1st Cir. 2002) (applying the Takings Clause to a Massachusetts statute's trade secret disclosure provision).

[86] *See, e.g.*, ALASKA STAT. § 40.25.120(10) (creating a limited exception for "records or information pertaining to a plan, program, or procedures for establishing, maintaining, or restoring security in the state, or to a detailed description or evaluation of systems, facilities, or infrastructure in the state"); MINN. STAT. § 13.37.

[87] This hypothetical closely parallels a request made by the Alaska Democratic Party in late 2005. The Party eventually sued for access to the state's "central tabulator data file," which contains final vote tallies from Alaska's 2004 general election. Alaska Democratic Party Press Release, Apr. 18, 2006 (in Lexis news database). *See also* Don Hunter, *Suit Asks for Vote Records*, ANCHORAGE DAILY NEWS B1, Apr. 19, 2006; Lisa Demer, *State Rebuffs Raw Vote Demand*, ANCHORAGE DAILY NEWS, Jan. 24, 2006, *available at* http://www.adn.com/news/alaska/story/7386582p-7298824c.html. The State recently agreed to release the database. Alaska Democratic Party, Press Release, Sept. 20, 2006, http://www.alaskademocrats.org/ht/display/ReleaseDetails/i/871710/pid/283063.

[88] *See* Bondpro Corp. v. Siemens Power Generation Corp., 2006 U.S. App. LEXIS 23183, *18-*19 (7th Cir. Sept. 12, 2006) (emphasizing this definitional point).

definition of confidential information only extends as far as the relevant public records statute will permit,[90] sorting through this vague language might prevent an election official from making a timely response to a public records request.

Election officials could clarify the status of voting system information that is likely to be of public interest by requesting specific carve-outs in contracts with vendors.[91] For example, they could seek contract language that specifically allows them to release ballot files in their native format. Additionally, election officials should investigate whether they must provide, or may provide, copies documents that have had secret or confidential information redacted.

B. Legal Issue: Security Information Exception

The second issue raised by Hypothetical #3 is whether disclosure of the central ballot database falls under State X's security information exception. It is difficult to generalize about security information provisions because they vary widely from state to state. The exception in California, for example, is limited to records that accompany a criminal investigation or that contain "critical infrastructure information" held by the California Office of Homeland Security.[92] Minnesota, in contrast, classifies as "nonpublic" (and thus exempt from the public records law) all "security information," which includes "government data the disclosure of which would be likely to substantially jeopardize the security of information . . . against . . . tampering, improper use, . . . [or] illegal disclosure . . . ."[93]

Thus, election officials must become familiar with the scope of their state's security information exception to ensure that they do not withhold information that does not qualify for this exception. Additional issues that elections officials may need to explore on a case-by-case basis include:

- Whether the presence of security information in documents that are responsive to a public records request merit a flat denial of the request, or whether the sensitive information could be redacted.

---

[89] *See, e.g.*, Agreement Between the County of San Mateo and Hart Intercivic, Inc., (draft as of Aug. 15, 2006), *available at* http://www.co.sanmateo.ca.us/bos.dir/BosAgendas/agendas2006/Agenda20060815/20060815_a_11.pdf ["Hart-San Mateo Contract"] (defining as "Confidential Information" "designs of . . . Hart Proprietary Software").

[90] *See* Hart-San Mateo Contract, *supra* note 91, ("COUNTY, to the extent permitted by the California Public Records Act, and Government Code sections 6250 et seq., agrees to maintain the confidentiality of all Hart Confidential Information and Sybase, Inc. confidential information. . . .").

[91] Elections officials could also use contracts to prevent the chance that some materials that vendors commonly mark as "confidential," such as technical manuals and poll worker training materials, may not be withheld from public records responses on the ground that these materials fall under a public records statute's confidentiality exemption.

[92] CAL. GOV'T CODE §§ 6254(f), (bb).

[93] MINN. STAT. § 13.37.

- The basis for concluding that documents contain security information. This point is not always obvious; whereas passwords and encryption keys would likely put information at risk, details about the format of a database file probably present little, if any, security risk. Independent computer security experts can provide valuable guidance in assessing these risks.

C. Legal Issue: Copyright

A plausible interpretation of the vendor's assertion, in Hypothetical #3, of a "proprietary" interest the database file is that it is claiming a copyright interest in the file format, its contents, or both. At least one vendor, DESI, has taken the position that copyright constrains how elections officials may respond to public records requests.[94] In a letter to the Ohio Board of Elections, DESI warned that documents that are not subject to trade secret protection "can be viewed in the presence of a public official but not copied or distributed. Copying, distributing the material or allowing notes to be taken from the material may violate" federal copyright law.[95] It is therefore worth considering whether copyright protection might prevent an elections official from producing materials – such as the database mentioned in Hypothetical #3 – that otherwise would be produced in response to a public records request.

Several copyright doctrines limit the copyright interests that elections officials need to consider in disclosing the kinds of files described in Hypothetical #3. Copyright can cover only creative expression of an idea or factual information, not ideas or facts themselves.[96] Due to this "idea-expression dichotomy," copyright does not protect the facts contained in a database – the ballot records, in Hypothetical #3 – and the information in the database could be reproduced in another format and distributed.[97] In addition, the format of the database file probably reflects the requirements of higher-level processing software; although the processing software might be protected by copyright, this protection does not extend to a work whose function and design are dictated by the need to be compatible with the software.[98]

The native format of the database, moreover, might be significant for analysis conducted by the party making the request. For example, a forensic analysis of the file might depend on having access to the original format in order to determine whether or how information might have been altered or lost. These considerations also suggest application of the merger doctrine. Under this doctrine, an expression of an idea that can be expressed in one or a very few ways cannot be copyrighted.[99] This prevents the copyright from effectively inhibiting spread of the idea. In a database used in an electronic voting system, any creativity involved in designing a database layout may be driven by the needs of the application, or may be the most efficient way of organizing

[94] Letter from DESI to Ohio State Boards of Elections, "Diebold's Position on Releasable Materials for Open Records Requests," Jan. 13, 2006 (on file with authors).
[95] *Id.*
[96] NIMMER ON COPYRIGHT § 16.01.
[97] *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991).
[98] *See* Computer Assocs. Int'l v. Altai, 982 F.2d 683, 702-10 (2d Cir. 1992).
[99] NIMMER ON COPYRIGHT § 13.03[B][3].

uncopyrightable data. This may make it difficult for a vendor to claim copyright protection in a file format.

Finally, fair use, described in detail above, is an important defense here as well.[100] As stated above, copyright protection in file formats is thin or non-existent. Moreover, the potential harm to the market value of this work would likely be slight; there is generally no market for voting systems' database files (or the accompanying database management software) that is separate the market for voting systems. Thus, the likelihood that disclosure of a database file in a proprietary format would lead to substitution by infringers appears to be exceedingly small.

In conclusion, determining whether the trade secret, security information, or copyright exceptions apply to public records requests for voting system information requires close attention to the technical details of the information and the relevant administrative interpretations of the public records statute. In addition, intellectual property claims in information that is subject to disclosure warrant close analysis. Elections officials should also consider whether they have a duty to release redacted information. Finally, elections officials can avoid some of these conflicts by specifying in contracts with vendors that the jurisdiction may release information that is likely to be responsive to public records requests.

Part IV: ISSUES IN BUILDING SYSTEMS OF INTEROPERABLE COMPONENTS

Finally, we examine the set of legal issues that arise from assembling "mixed" voting systems, that is, using different vendors' components in a single electronic voting system, or, perhaps, using a subset of the components from a single vendor's voting system. Mixed systems are appealing for several reasons: they might permit an official to use existing equipment in new ways; they might enable voting features only available by combining components from multiple vendors; and they might help to promote competition within the marketplace.

Numerous legal considerations, however, might constrain the kinds of mixed systems that election officials may assemble. First, we discuss how many states' requirements to use federally certified voting system can hamper the use of mixed systems. In Section B, we briefly discuss the contract law, trade secret, and copyright issues surrounding mixed systems that election officials would face, even if they resolve the certification issues discussed in Part IV.A.

A. Federal Certification and State Elections Codes

Approximately 40 states require the use of federally certified voting systems.[101] This requirement places a significant constraint on the approval of mixed systems at the

[100] See the discussion in Part II.B for a thorough discussion of the fair use defense.
[101] U.S. Election Assistance Comm'n, *Frequently Asked Questions* (last revised Jan. 19, 2007), http://www.eac.gov/docs/Revised%20Certification%20QA%20v2%20(%20BH%20rev%20)%202%20(%20GH%20edits%20).pdf.

state level. Federal certification requires the testing of a full voting *system*; test labs do not evaluate, and the EAC does not certify, individual components.[102] Consequently, a mixed system—even if it is assembled from components of certified systems—cannot be regarded as a federally certified system, unless that particular system has been certified.

For example, suppose that Manufacturer A obtains certification for a voting system consisting of a ballot marking device, an optical scanner, and election management software. Manufacturer B obtains certification for a voting system consisting of an optical scanner and election management software. A county might wish to assemble a voting system composed of A's ballot marking device and B's optical scanner and software. Given these facts, however, the county's proposed mixed system will not have federal certification, since that particular combination of components was not submitted to a test lab and certified by the EAC. If this county is in a state that requires election authorities to use federally certified systems, it will not be able to use the mixed system without violating the state's legal requirements.[103]

It is possible, in theory, to certify a mixed system, even one that consists of components from different vendors; but this has not happened so far at the federal level. Testing such a system would require each vendor to give permission for its equipment to be tested as part of that system; the fact that a vendor submitted components as part of another system would not allow testing to proceed. Similarly, certification of a voting system does not imply that a subset of components in that system are certified as a voting system, even if the subset constitutes a voting system.

Some states that require jurisdictions to use federally certified systems as a general rule may be willing to make exceptions. For example, voting system requirements issued by the California Secretary of State provide that "[m]ultiple independently tested and certified voting systems may be used together to meet federal and state requirements so long as their interface is limited to exchange of aggregated vote totals and/or ballot layout."[104] Apparently acting under this exception, California in May 2006 certified a system containing the ES&S AutoMARK device (a ballot marking device) and related software, the Diebold AV-OS optical scanner, and Diebold's Global

---

[102] *See generally* U.S. Election Assitance Comm'n, Testing and Certification Program Manual (referring throughout to voting system certification). *See also* VVSG, vol. 1, at A-19 (defining "voting system" to mean the "total combination of mechanical, electromechanical or electronic equipment" required to define ballots, cast and count votes, display results, produce audit trails; and documentation and practices used to develop the system and identify its components).

[103] States may make exceptions to their own laws or regulations regarding mandatory use of federally certified voting systems. For example, former California Secretary of State Bruce McPherson certified a system consisting of the ES&S AutoMARK (a ballot marking device), the Diebold AV-OS optical scanner, and Diebold Global Election Management System (GEMS). This certification was authorized under the Secretary of State's regulations, which allow "[m]ultiple independently tested and certified voting systems may be used together to meet federal and state requirements so long as their interface is limited to exchange of aggregated vote totals and/or ballot layout." See item 7 of: California Secretary of State, *Voting System Fact Sheet*, http://sos.ca.gov/elections/voting_systems/vs_factsheet.pdf (last visited Jan. 28, 2007)..

[104] *Id.* California certified additional mixed systems for the November 2006 election. *Id.*

Election Management System (GEMS), and Diebold Global Election Management System (GEMS).[105] Four counties used this mixed system in 2006 elections.[106]

B. Contracts, Trade Secrets, and Copyright

Setting aside the issue of federal certification, election officials face other legal hurdles in assembling and testing mixed systems. Vendors have demonstrated hostility to attempts to certify mixed systems. In Volusia County, Florida, for example, elections officials planned in July 2005 to combine the AutoMARK ballot-marking device produced by Election Systems and Software (ES&S) with an optical scanner produced by competitor DESI.[107] Florida regulations required Volusia County to seek state certification for the hybrid ES&S-Diebold system. After learning that Volusia County had proposed to use a DESI machine in the state's possession as part of the mixed system certification, DESI notified the state Division of Elections that the DESI equipment was on loan and "cannot be used with any third party vendor's certification proceeding" without DESI's permission. Moreover, the letter warned, DESI would "take the necessary steps to protect its proprietary interests" if any vendors sought certification for a hybrid system containing a DESI component.[108] Ultimately, Florida did not certify the AutoMARK device for use in the state.[109]

More generally, vendor contracts contain provisions that could be construed either to prohibit mixed systems outright, or to obtain the purchaser's agreement not to seek certification of mixed systems, irrespective of the defensibility of doing so under trade secret or copyright law. As discussed in the context of security testing in Part II, vendor contracts typically contain broad prohibitions on how jurisdictions may use electronic voting systems after purchase. Terms that apply to the mixed system context include

---

[105] Letter from Bruce McDannold, California Office of Voting Systems Technology Assessment, to Billie Alvarez, Elections Division Manager (Santa Barbara County), May, 11, 2006, available at http://www.cs.berkeley.edu/~daw/tmp/automarkcert.pdf.

[106] Marin, San Luis Obispo, and Santa Barbara counties used this mixed system in the 2006 primary and general elections. California Office of the Secretary of State, County Voting Systems for the June 6, 2006, Primary Election (June 1, 2006), http://sos.ca.gov/elections/voting_systems/gp06_systemsinuse_a.pdf; County Voting Systems for the November 7, 2006 General Election (Nov. 6, 2006), http://sos.ca.gov/elections/voting_systems/systemsinuse_110606.pdf. Siskiyou County used this system in the 2006 general election only. *Id.*

[107] To take another example, it is questionable whether Florida even permits certification of mixed systems: "Where initiated by a county Supervisor of Elections or the Department of State, modifications to previously certified systems which are designed to remedy system anomalies, which do not introduce new functions and do not introduce additional hardware components into the system configuration, may be certified under the Florida Voting Systems Standard, . . ." Certification of electronic or electromechanical voting systems, 1S-5.001 F.A.C., *available at* http://fac.dos.state.fl.us/faconline/chapter01.pdf.

[108] Letter from Ian S. Piper, Diebold Election Systems, Inc., to Paul Craft, Division of Elections, Florida Department of State (July 11, 2005) (on file with authors).

[109] Kevin P. Connolly, *Dragging Feet, County Buys No-Paper Voting Screens: The Quest for an Alternative with Paper Ballots Won't End, Some Vow*, ORLANDO SENTINEL, Feb. 24, 2006.

prohibitions against the "adaptation" and "reverse engineering" of any part of the system.[110]

Although the structure of Florida's law might, in this case, have alerted DESI to the use of a DESI component in a hybrid system certification, vendor contracts might pose obstacles to assembling hybrid systems from components that a jurisdiction has already purchased. A typical list of prohibitions in vendor contracts forbids the adaptation, modification, and reverse engineering of hardware and software without the vendor's consent. Moreover, these contracts usually assert that the vendor has a proprietary interest in nearly all aspects of the use and design of its voting system. A vendor might further argue that its contract with the county effected a waiver of potential defenses under both trade secret and copyright law.

Because the potential trade secret claims and defenses are essentially identical to the testing context, we do not offer a separate analysis here. Two variations of copyright infringement liability warrant brief discussion.

- **Infringement Claims.** As discussed in Part II, the unauthorized use of computer software can give rise to a claim of copyright infringement. Compared to the testing context, it is less clear that typical vendor contracts prohibit jurisdictions from using voting system components that they have purchased in mixed systems. Thus, a vendor might not be able to make out a plausible claim that a mixed system constitutes copyright infringement. In addition, the defenses of fair use and copyright misuse would be available to the election official. The application of these defenses closely tracks the testing analysis in Part II.

- **Violation of the DMCA's anticircumvention provisions.** Election officials should also consider whether the Digital Millennium Copyright Act's (DMCA) prohibition on defeating the technical protection measures – i.e., the "locks" – on digital works would apply to assembling a mixed-component voting system. As discussed in Part II, any claim that the DMCA applies in such should be closely examined; the mere presence of cryptographic measures does not necessarily bring the DMCA into play. Still, circumvention might be necessary, for example, to determine how one vendor's protected ballot database and vote tabulation software can be

[110] *See, e.g.*, Hart-San Mateo Contract ¶ 49(B):

> COUNTY agrees that this Agreement and the sale of Hart Hardware and license of Hart Proprietary Software to COUNTY does not grant to or vest in COUNTY any right, title or interest in such proprietary property. COUNTY shall not, under any circumstances, without HART's prior written consent, cause or permit the adaptation, conversion, reverse engineering, disassembly or de-compilation of any Hart Proprietary Software, Firmware or Hart Hardware. All ideas, concepts, know-how, data processing techniques, documentation, diagrams, schematics, firmware, equipment architecture, software, improvements, bug fixes, upgrades and trade secrets developed by HART personnel (alone or jointly with COUNTY) in connection with Hart Confidential Information, Hart Hardware, Firmware and Hart Proprietary Software will be the exclusive property of HART.

used with another vendor's voting machines.

This kind of voting system examination might be protected under DMCA's reverse engineering exemption. Like the security testing exemption discussed in Part II, the reverse engineering defense applies to a relatively narrow range of conduct. To qualify, a reverse engineer must (1) obtain a legal copy of a technically protected program; (2) circumvent that program for the sole purpose of, and to the extent necessary to achieve interoperability with "an independently created computer program"; (3) not use information previously available to the reverse engineer; and (4) not commit traditional copyright infringement.[111]

At first glance, it appears relatively easy for an election official to qualify for the reverse engineering exception: First, the election official could purchase the target voting systems and obtain a license to its software. Second, the source code for the voting systems is typically unavailable. And third, the primary purpose of an election official's reverse engineering would be the identification of elements necessary to achieve interoperability. The fourth part of the exception – the absence of traditional copyright infringement – might be more difficult to establish, as an elections official might have to use a voting system's software in an unauthorized manner to achieve interoperability. The fair use argument given above applies here as well. Moreover, reverse engineering by elections officials is unlikely to allow others access to the vendor's software. Finally, much of the data that voting system software processes is not subject to copyright protection.[112]

A potentially more troublesome issue is that election jurisdictions agree not to engage in reverse engineering in their contracts with vendors. Although one federal court has held that a contractual clause that prohibited reverse engineering impermissibly conflicted with copyright law,[113] a number of other courts have enforced similar clauses.[114] Contracts for electronic voting systems are typically negotiated before purchase and are subject to public comment, two factors that would further support their enforceability. If an anti-reverse-engineering clause is enforced against an election jurisdiction, it probably will not be able to use the reverse engineering exception to avoid circumvention liability.

Part V: CONCLUSION

[111] 17 U.S.C. § 1201(f)(1).
[112] This contrasts favorably with the facts in *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005), in which the court held that a reverse-engineered game server did not qualify for the reverse engineering exception because this server allowed individuals to use infringing copies of the game.
[113] Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255 (5th Cir. 1988).
[114] *Davidson*, 433 F.3d at 630; Bowers v. Bay State Technologies, 302 F.3d 1332 (Fed. Cir. 2002).

A recurring theme in this memo is the importance of contract terms in influencing numerous activities that elections officials must take to perform their duties. Security testing, public records disclosure, and assembling mixed systems are all influenced by contractual limitations on what jurisdictions may do with the machines they purchase, the software they license, and the technical information they receive from vendors. On the other hand, contracts present an opportunity for elections officials to clarify their abilities to address public concern about electronic voting. We summarize here the principal types of contract clauses that deserve attention:

- **The designation of "proprietary" information.** Different kinds of information receive quite different forms of legal protection. Crafting contracts that are more specific about what information is protected by copyright, trade secrecy, neither, or both would lend clarity to elections officials' duties in all areas that we have discussed.

- **Contracting for carve-outs.** In many cases, contracts assign rights to vendors "to the extent permitted" by applicable laws. Although these clauses may bring a certain efficiency to contracting, they do not offer much help to election officials who wish to perform testing or respond to public records requests. As the capabilities of electronic voting systems, and the features of them that the public seeks to know more about, become more familiar, specifying in advance elections officials' right to accommodate likely areas of public concern should become practical.

- **Limiting anti-reverse engineering clauses.** Reverse engineering would likely play an important role in both testing and building systems of interoperable components. The reverse engineering exception to the DMCA is rather narrow and might be waived by the broad anti-reverse engineering clauses that appear in typical vendor contracts. If a state allows mixing components from different vendors, election officials should seek to avoid blanket reverse engineering clauses, or at least create exceptions that would allow elections officials to build the systems that are permitted by state law. Finally, since a jurisdiction might want to know whether they can use a vendor's component as part of a mixed system before it buys that component, it might be necessary to negotiate reverse engineering exceptions to agreements governing equipment that is on loan from vendors.

- **Obtaining contractual rights to conduct testing.** Developments over the past few years have provided a more concrete idea of the kinds of security vulnerabilities in electronic voting systems. At the same time, the federal guidelines that many states incorporate, at least indirectly, into their certification requirements might not be stringent enough to test for these or other vulnerabilities. At minimum, jurisdictions could seek contractual permission to determine whether the machines they have purchased, or are considering purchasing, are vulnerable to known attacks. Although such a limited provision

might not allow for discovery of new vulnerabilities, it would at least allow jurisdictions to determine whether they are at risk, to develop measures (such as improved chain-of-custody requirements) that might mitigate those risks, and to work more effectively with vendors to address security vulnerabilities.

A related contracting point is to specify the relationship between the election jurisdiction and the person who will perform the security testing. A jurisdiction might want to hire an academic researcher or a computer security consulting company to conduct testing; a contract should provide for the range of likely possibilities. If necessary, the contract could contain a provision for notifying the vendor of the selection of a security tester and ensuring that appropriate non-disclosure agreements are in place.