The John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 3 *Journal of Computer & Information Law - Spring 2005*

Article 5

Spring 2005

"Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?", 23 J. Marshall J. Computer & Info. L. 533 (2005)

Doris E. Long
John Marshall Law School, profdelong@gmail.com

"ELECTRONIC VOTING RIGHTS AND THE DMCA: ANOTHER BLAST FROM THE DIGITAL PIRATES OR A FINAL WAKE UP CALL FOR REFORM?"

DORIS ESTELLE LONG†

I. INTRODUCTION

Electronic voting machines are the new version of pirated music. Like digital music, electronic voting was designed to make voting rights easily available to the masses. Technology, the "savior" of the 21st Century, however, has once again demonstrated how easy it is to circumvent a good idea through better "hacker" technology. As the information circulated by the students at Swarthmore College demonstrated,[1] no matter what type of digital fence is erected, someone can always find an electronic wire cutter to breach it. In reality, just as any house can be burgled no matter how sophisticated the security system, any electronic voting software can be hacked no matter how good the encryption technology protecting it. The issue is not creating a fool-proof anti-circumvention system – an impossible task – but creating the necessary digital safeguards to make circumvention difficult, to make security breaches more readily detectable, and to provide back-up systems (perhaps in paper format) to protect the integrity of the voting process even in the face of an electronic breach.

To solve the problem of providing adequately secure electronic voting systems, just as in the case of music piracy, we will need *both* technological fixes (including better record-keeping to reduce the equivalent of an electronic hanging chad) and better legal protection for those fixes.

---

† Professor of Law and Chair of the Intellectual Property, Information Technology and Privacy Group, The John Marshall Law School, Chi., Ill. This essay is based on comments made at the conference *"E-lection 2004: Is e-voting ready for prime time?"* (The John Marshall Law School, Chi., Ill., Oct. 1, 2004) and reflects legal developments up through March 2005 when it was written.

1. For a discussion of the background of the lawsuit filed by Swarthmore College students involving the posting of allegedly copyright protected information regarding the security of certain electronic voting software by Diebold Electronic Systems, Inc, *see* n. 53-69 *infra and accompanying text.*

Unfortunately, the legal regime established in the 1990's to "solve" the problem of digital piracy – the Digital Millennium Copyright Act ("DMCA")[2] – has been even less successful in protecting the integrity of the voting process. In point of fact, it has worked directly against such protection.

By the time this Essay is going to press, the results of the 2004 Presidential election are well known. Despite concerns that hackers might be able to "hijack" the election, widespread voter irregularities as a result of the use of electronic voting machines have not yet been uncovered.[3] The issues regarding e-voting which were addressed in the October conference,[4] including the issues posed by the unfortunate role of the DMCA in dealing with voting security, remain as problematic as ever. However, while reform of the verification and certification processes continues apace, much of the impetus for reform of the DMCA to address these particular issues appears stalled.[5] As of March 2005 when this essay was being finalized, reforms directed to correct the harmful effects of the DMCA upon the debate over e-voting security remain largely non-existent.[6] In addition, the same prohibitions against informal encryption research that stymied outside testing of Diebold's election software continue in place.[7]

---

2. The Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998) (codified in diverse sections of 17 U.S.C. §§101 et seq.).

3. There have, however, been numerous legal challenges to various elections in 2004 involving the use of electronic voting machines. These alone should be sufficient to encourage a rapid response to the problems raised by current security certification and verification procedures. For a brief listing of current lawsuits involving e-voting issues, *see* Electronic Frontier Foundation, *EFF: E-Voting*, http://www.eff.org/Activism/E-voting (accessed Apr. 15, 2005).

4. Conference, *"E-lection 2004: Is e-voting ready for prime time?* (The John Marshall Law School, Chi., Ill., Oct. 1, 2004) (sponsored by The John Marshall Law School Center for Information Technology and Privacy Law).

5. *See e.g.* Voter Confidence and Increased Accessibility Act of 2005, HR 550, 108th Cong., 1st Sess. (addressing the issues of verification and certification, but containing no measures to deal with the DMCA issues implicated by such procedures)(available at http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.2239:) (accessed Oct. 18, 2005).

6. This lack of activity should be contrasted with the Digital Media Consumers Rights Act of 2005, HR 1201, 109th Cong. 1st Sess. (available at http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1201) (accessed Oct. 18, 2005), which would acknowledge a fair use defense for circumvention of access protection measures, and includes as an amendment the insertion of language that would prevent the application of the anticircumvention provisions of the DMCA if the person "is acting solely in furtherance of scientific research into technological measures." *Id.* at Section 5(a). Such fair use defense could correct the present threat to encryption research and security testing posed by the DMCA. *See* nn. 83 - 85 *infra and accompanying text.*

7. *See e.g.* 17 U.S.C. §§ 1201(g)&(j); *see also* nn. 90 - 94 *infra and accompanying text.* It is not yet clear whether reforms directed to software certification will help ameliorate these issues by ultimately mandating a certification process that permits outside testing.

Perhaps more problematic, insofar as free speech is concerned, the same procedures that were initially used to keep the students at Swarthmore College from circulating internal memoranda and other documents regarding potential security problems with Diebold's electronic voting software[8] remain extant, although some courts have begun to craft their own ameliorating exceptions to some of these procedures.[9] As the speakers at the E-Voting Conference[10] so richly demonstrated, more is required to make sure that the fundamental rights to vote and to free speech are not the unintended victims of legislation designed to combat digital piracy.

II. THE UNINTENDED CONSEQUENCES OF THE DMCA

Whenever law is combined with technology, the result is bound to be a legislative solution that has unforeseen loopholes in protection and unanticipated barriers to use. The DMCA, created initially to respond to the problems of digital piracy in the early days of the internet,[11] fully qualifies as such a law.[12] It is easy to forget that the DMCA was origi-

---

If so, hopefully, Section 1201 of the Copyright Act will be specifically referenced in any such procedures to avoid the delay any potential challenge under the DMCA might cause to the institution of such much needed reforms.

8. These procedures included, in particular, the notice and takedown procedures of Section 512(c) of the DMCA. 17 U.S.C. § 512(c). These procedures are discussed in greater detail in n. 18 *infra and accompanying text.*

9. *See e.g. Elektra Ent. Group, Inc. v. Does 1- 6,* Civ. Action. No. 04-1241 (E.D. Pa. 2004) (available at http://www.eff.org/IP/P2P/RIAA_v_ThePeople/20041012_Order_Granting_Request.pdf) (accessed Oct. 18, 2005); *see also* n. 83 *and accompanying text infra.*

10. *See supra* n. 4.

11. Although common usage continues to use initial capitals to describe "the Internet," such usage no longer seems appropriate given the internet's wide spread and long standing use. Just as "the Telephone" has become "the telephone," so too, it is time to recognize that "the Internet" has become an accepted and longstanding communication form which no longer needs to be treated with the exclamatory reverence of initial capital letters. Such special treatment, I believe, has been used in part to relieve international law of its responsibility to resolve the legal issues surrounding intellectual property on the internet. Capital letters subconsciously tell us all that the "Internet" is something new, so new that we cannot yet be expected to deal with the problems it poses. The time for such complacency, along with the initial capital letters, is long past.

12. *See e.g.* S. Rep. No. 105-190 at 8 (available at http://thomas.loc.gov/cgi-bin/cpquery/z?cp105:sr190:)(accessed Oct. 18, 2005) ("[The DMCA] will facilitate making available quickly and conveniently via the Internet the movies, music, software, and literary works that are the fruit of American creative genius. It will also encourage the continued growth of the existing off-line global marketplace for copyrighted works in digital format by setting strong international copyright standards. At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability. . . .[B]y limiting the liability of service providers, the DMCA ensures that the

nally crafted as a *compromise* between copyright owners and internet service providers to assure *both* continuing protection of copyright owners' property rights, *and* continuing growth of the internet.[13] At the time that the DMCA was enacted, courts were split on the potential direct and contributory liability of internet service providers for the transmission/posting of infringing works.[14] The DMCA, enacted in 1998, removed the uncertainty that many service providers faced regarding their liability for the posting and distribution of potentially infringing materials by third parties by providing a safe harbor for certain specified activities by service providers.[15] In the clamor that has arisen surrounding the appli-

---

efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand").

13. *See e.g.* S. Rep. No. 105-190, *id.* at 20 ("Title II [of the DMCA] preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities"); H.R. Rep. No. 105-551 at 21 (available at http://panix.com/~jesse/DMCA.html)(accessed Oct. 18, 2005)(noting that the remedies granted "ensure that it is possible for copyright owners to secure the cooperation of those with the capacity to prevent ongoing infringement"). *See also* Statement of Marybeth Peters Before the Senate Judiciary Committee, 108th Congress (Sept. 9, 2003)(available at http://www.copyright.gov/docs/registat090903.html)(accessed Oct. 18, 2005) (addressing the issue of Pornography, Technology and Process: Problems and Solutions on Peer to Peer Networks); *ALS Scan, Inc. v. RemarQCommunities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001)("The DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions in which a serve provider's systems engaged through a technological process initiated by another without the knowledge of the service provider."); *In re Verizon Internet Services*, 240 F. Supp.2d 24 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003)("Congress . . . created tradeoffs within the DMCA: service providers would receive liability protections in exchange for assisting copyright owners in identifying and dealing with infringers who misuse the service providers' systems. At the same time, copyright owners would forego pursuing service providers for the copyright infringement of their users, in exchange for assistance in identifying and acting against those infringers").

14. *Compare Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1522 (M.D. Fla. 1993)(operator of a computer bulletin board directly liable for uploading and downloading of copyrighted photographs by subscribers) *and Sega Enterprises Ltd. v. Maphia*, 857 F. Supp. 679 (N.D. Cal. 1994)(operator of computer bulletin board directly and contributorily liable for uploading and downloading of copyrighted video games by subscribers) *with Religious Technology Center v. Netcom On-Line Communication System Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995)(operator of bulletin board is not directly liable for uploading and downloading of copyrighted materials by subscribers; issue of contributory infringement left open); and *Marobie-FL, Inc. d/b/a Galactic Software v. Natl. Assn. of Fire Equip. Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997)(internet service provider not directly liable for third party user's infringing acts; issue of contributory liability left open).

15. Section 512 of the Act, referred to as the "safe harbor" provision of the statute, releases a "service provider" from liability in connection with the transmission, temporary storage, or linking of material at the direction of an end user provided the service provider meets certain specified requirements, including the removal of end user material upon the

cation of the notice and take down procedures of the Act,[16] it is easy to forget that these procedures were originally designed as part of a *bargained-for* trade-off.[17] In exchange for clearly delineated safe harbors, internet service providers were obligated to assist copyright owners in their efforts to protect their rights on the internet. One aspect of this assistance was to remove or disable access to infringing materials upon receipt of the appropriate notice of infringement from the copyright owner.[18] Failure to "take down" infringing material under the Act re-

---

receipt of an adequate notice from the copyright owner. 17 U.S.C. §512(c). The four activities for which safe harbor protection exists are: serving as a conduit for transitory communications; system caching; posting information at the direction of end users; and providing hyperlinks and other information location tools. 17 U.S.C. § 512.

The Act contains a relatively broad definition of a service provider. Under the Act any "entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as seen or received" qualifies as a service provider. 17 U.S.C. § 512(k); *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 623 (4th Cir. 2001) (the DMCA "defines a service provider broadly").

16. *See e.g.* n. 38 *and accompanying text.*

17. Admittedly, in these negotiations, not all parties' interests or viewpoints were equally represented. As Copyright Register Mary Beth Peters recognizes in her article *Copyright Enters the Public Domain*, "What has changed in the world of copyright. . .?" "The answer is what I've tried to convey with the title of this lecture. Copyright has entered a new arena – the court of public opinion. Why? Because for the first time ordinary consumers have come fact to face with copyright as something that regulates them directly, because technology allows them to be copiers and distributors on a scale and with such ease that has never before been present." Mary Beth Peters, *Copyright Enters the Public Domain*, 51 J. Copyr. Socy. 710, 705 (2004); The new appearance of consumer voices in the copyright arena may require re-consideration of some of the unintended consequences of the mechanisms established to achieve the bargained-for exchange under the DMCA. It does not, however, require wholesale abandonment of the compromise reached. To the contrary, on the whole, the granting of safe harbor status has achieved the laudable goal of assuring protection from liability to service providers for acts of third parties over which such service providers have little knowledge or control. Not even the severest critics of the DMCA, I suspect, want to adopt a system which would take us back to the old system of potential contributory liability or, even worse, the strict liability model followed in some countries. *See e.g.* China's Internet Regulations (available in English at http://www.chinaepulse.com)(accessed Apr. 15, 2005).

18. These "notice and takedown" procedures require copyright owners to provide a written notice that includes an authorized signature (which may be an electronic one), a clear identification of the copyrighted work allegedly being infringed, a clear identification of the alleged infringing material, "reasonably sufficient" information that will allow the ISP to locate the material at issue, information, such as an email address, that will allow the ISP to contact the subject of the infringing activity, a statement of good faith on the part of the copyright holder and a statement of accuracy. 17 U.S.C. §512(c)(3). Upon receipt of such a notice the ISP must "[respond] expeditiously to remove, or disable access" to the material claimed to be infringing. *Id.* Where an ISP acts in good faith in response to a notice of infringement, it will not be liable so long as it takes reasonable steps to promptly notify the subscriber of its actions, provides the complaining party of any counter notification it receives from the complaining subscriber and replaces any removed material subject

sults in loss of safe harbor protections.[19] Safeguards are built into the system, however, so that the ISP must notify the subscriber of its actions and must replace any removed content upon proper notification of a claim of right by the subscriber.[20]

A second, and in recent years equally critical, aspect of the assistance to copyright owners was the abbreviated subpoena procedures established in Section 512(h).[21] Section 512 (h) granted copyright owners the ability to obtain a subpoena on request from a clerk of a United States District Court for disclosure by a service provider of the identity of a subscriber who has allegedly engaged in copyright infringement.[22] To obtain the subpoena, the copyright owner is only required to provide a written notice that includes the following: (1) a clear identification of the copyrighted work allegedly being infringed; (2) a clear identification of the alleged infringing material; (3) "reasonably sufficient" information that will allow the ISP to locate the material at issue; (4) a statement of good faith belief the work is being infringed; and (5) a declaration that the identity of the subscriber in question will only be used for the purpose of protecting the owner's copyright.[23] Unlike the notice and take down provisions of Section 512(c),[24] there is no requirement that subscribers whose identity is being sought be notified of the subpoena or given an opportunity to challenge its propriety prior to disclosure of their identity.[25] Moreover, such subpoenas are issued as a ministerial act of the clerk of the court, without the need for, or benefit of, judicial oversight.[26]

In light of the recent development (in legal years, certainly not in technology years) of the first Napster file trading Web site[27] and the

---

to a proper counter complaint within 10 to 14 days of receipt of the counter notice, unless the ISP receives notice from the original complaining party that it has filed a lawsuit regarding the material in question. 17 U.S.C. §512(g).

19. 17 U.S.C. § 512.

20. 17 U.S.C. § 512(g).

21. 17 U.S.C. § 512(h).

22. *Id.*

23. *Id.*

24. 17 U.S.C. § 512(c).

25. 17 U.S.C. § 512(h)(5)("Upon receipt of the issued subpoena. . . the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena. . .").

26. *Id.*

27. Napster is currently re-incarnated as a source for authorized downloads of music. *See* http://www.napster.com. However, it is most famously known as one of the original sources for software which facilitated peer to peer file trading of music files between end users. For a brief factual description of its workings and the legal consequences that resulted from such acts, *see A&M Records, Inc. v. Napster, Inc.*, 239 F3d 1004 (9th Cir. 2001); *See also* Joseph Menn, *All the Rave: The Rise and Fall of Shawn Fanning's Napster* (Crown Business 2003).

wide-spread use of peer to peer file trading on the internet,[28] it is easy to criticize the short-sightedness of Congress in not crafting clearer legislation. But Congress has never been particularly prescient in crafting legislation in this area. The ham-fisted[29] Audio Home Recording Act of 1992[30] and its equally misguided relative, the Semiconductor Chip Protection Act of 1984,[31] are obvious testaments to the problems posed when technology laps legal doctrine.[32] That does not mean that Congress should abdicate its legislative role in this area. Technology has always sped ahead of law, particularly in the area of intellectual property rights. In fact, I believe that such a result was not only anticipated by the Founders when they placed a grant clause involving intellectual property within the Constitution itself,[33] but was actually encouraged. If we have laws that encourage innovation and creativity, and those laws accomplish their stated purpose, *a fortiori* we must expect some innovation and creativity which is bound to impact the very nature of the laws that regulate them. The history of U.S. copyright law itself bears witness to the truth of this assumption as its scope of protection has been constantly expanded to include previously unanticipated new works and new meth-

28. *See e.g.* "*Copy Culture*", N. Y. Times C8 (Mar. 28, 2005); IT Innovations & Concepts, *P2P Music Statistics for December 24, 2004*, http://www.itic.ca/DIC/News/2004/12/24/P2P_Statistics_Nov_2004.en.html (accessed Apr. 15, 2005).

29. Whatever value the Audio Home Recording Act ("AHRA"), Pub. L. No. 102 – 563, 106 Stat. 4237 (codified in 17 U.S.C. §§ 1001 – 1010), might have had in connection with dealing with new technology was virtually eliminated by the courts in their interpretation of its inelegantly crafted language to exclude MP3 players. See Recording Indus. Assn. Of America v. Diamond Multimedia Systems Inc., 180 F.3d 1072 (9th Cir. 1999)(court interprets Sections 1001 and 1002 as inapplicable to computers and MP3 players which use computers to record copyrighted music, thus aking the SCMS requirements of the AHRA inapplicable to MP3 players).

30. 17 U.S.C. §§1001 – 1010.

31. 17 U.S.C. §§ 901 – 904.

32. In the case of the Audio Home Recording Act, codified in 17 U.S.C. §§ 1001 - 1010, the obvious intent of Congress to require hardware makers of equipment used as a digital audio recording device to employ a Serial Copyright Management System ("SCMS") that sends, receives, and acts upon information about the generation and copyright status of the files that the machine plays, see *id.* at § 1002(a)(2), was largely circumvented by the unanticipated development of portable flash memory devices which allowed owners to download music from their computers onto the devices. In a narrow reading of the statute which effectively eviscerated the Act, the court in *Recording Industry Assn. of America v. Diamond Multimedia Sys. Inc.*, 180 F.3d 1072 (9th Cir. 1999), held that the Diamond Rio was not covered by the statute since its files passed through a computer and such computers were expressly exempted from compliance with the Act. Such a technological loophole effectively "sunk" the Act as a method for dealing with the growing problem of digital music piracy on the internet.

33. U.S. Const. art. I, § 8, cl. 8. The presence of this clause in the Constitution becomes even more remarkable in light of the fact that the Bill of Rights had to wait for the passage of amendments to the Constitution to include critical First Amendment free speech rights.

ods of communication.[34] Given the increasingly rapid development of technology in the Digital Age, the need for Congress to revise legislation to correct oversights and mistakes becomes even more critical. This need should be directly contrasted with the purported "need" to provide special legislation to protect a particular industry. The Copyright Act has been amended more times than its sister laws – trademarks and patents.[35] Of these amendments, many have been designed to protect particular industries, such as the exemption of computer software and sound recordings from the strictures of the First Sale Doctrine codified in Section 109 of the Copyright Act.[36] Such exclusions, in my opinion, should be the exception and should only be taken when it is clear that the balance between copyright and public access is being unduly prejudiced.[37]

A. DIEBOLD AND THE SECURITY OF ELECTRONIC VOTING SOFTWARE

The unintended consequences arising from the notice, takedown, and subpoena provisions of the DMCA have been well documented.[38] The events surrounding the Diebold litigation, however, give greater urgency to the need for reform since the problems posed are related to an issue of critical Constitutional significance – the ability of citizens to exercise effectively their right to vote.[39] I do not mean to suggest that the

34. Thus, federal copyright protection in the United States has expanded from the narrow categories of protection of charts, maps and books, Copyright Act of May 31, 1790, 1 Stat. 124, to include photography; Copyright Act of 1865, 13 Stat. 540, *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53 (1884); motion pictures, Act of August 24, 1912, 37 Stat. 488; and computer software, Act of December 12, 1980, 94 Stat. 3015, *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240 (3d Cir. 1983).

35. *See e.g.* Joseph P. Liu, *Regulatory Copyright*, 83 N. C. L. Rev. 87 (2004)(noting the Copyright Act has doubled in 100 years and describing the increasing industry focus of such amendments); William M. Landes & Richard A. Posner, *The Political Economy of Intellectual Property Law* (2004) (noting the recent expansion of the Copyright Act); David Nimmer, *Codifying Copyright Comprehensibly*, 51 UCLA L. Rev. 1233, 1320 (2004)(discussing the frequency of amendments to the 1976 Copyright Act).

36. *See e.g.* 17 U.S.C. § 109 (c).

37. I do not mean to suggest that courts cannot also play a role in establishing necessary corrections as new technological developments demonstrate legal flaws in previously crafted legislation. Neither, however, should Congress abdicate its responsibility in this area.

38. *See e.g Unintended Consequences, 5 Years Under the DMCA*, http://www.eff.org/IP/DMCA/?f=unintended_consequences.html (accessed Apr.l 15, 2005); Doris Estelle Long, Written Testimony, "Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry," Submitted to the Senate Committee on Governmental Affairs (Sept. 30, 2003), *reprinted in* John Marshall Center for Intellectual Property Law News Source (Spring 2004).

39. As noted *infra*, I do not mean to suggest that the free speech issues raised in other debates over the DMCA have less "value" or importance than those raised in *Diebold*. But in the case of speech which has a direct impact on the political process, in this case voting,

free speech issues raised in other debates over the DMCA have less "value" than those raised in *Diebold*.[40] But there is less room to argue the relative merits of copyright versus speech rights when the issue impacts a core Constitutional value – political speech and the integrity of the voting process.[41]

After the 2000 Presidential election, Congress rushed to enact the Help America Vote Act ("HAVA").[42] The Act was intended to modernize the election process, moving the voting public into the purportedly precise and accurate world of computerized voting.[43] Under HAVA, the Election Assistance Commission ("EAC") was charged with establishing voluntary standards for voting machines and creating an independent testing process for the software used in such machines.[44] Unfortunately nomination of members to the EAC was delayed, and the first names for confirmation were not submitted until late fall 2003.[45] Despite the consequent delay in establishing, for example, security certification standards, e-voting machine manufacturers began to market electronic voting solutions directly to states without waiting for the planned assistance under HAVA. One company in particular, Diebold[46] an established manufacturer of automated teller machines and electronic kiosk systems, became a leading supplier to states of e-voting software and equipment.[47] By November 2003 Diebold had sold more than 33,000

---

there is less room to argue the relative merits between copyright protection and free speech rights. While other speech challenges under the DMCA have been largely directed to the speech right to use a particular expression or to use a particular format, *see e.g. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001), arguments which I believe generally seek an inappropriate accommodation of interests, in *Diebold* the core Constitutional values of political speech and the integrity of the voting process are clearly implicated and require a different accommodation.

40. Although as noted elsewhere not all of these free speech claims merit an alteration in the balance already struck by other provisions of the Copyright Act, including fair use, and the idea/expression dichotomy. *Id. See also* nn. 101- 106 *infra*.

41. *See* n. 99 *infra and accompanying text.*

42. The Help America Vote Act, Pub. L. 107-252 (Oct. 29, 2002)(codified in 42 U.S.C. §§ 15301 et seq.)

43. *Id.*

44. 42 U.S.C. § 15323. *See also* Congressman Dennis J. Kucinich, *Congressman Dennis J. Kucinich, 10th District of Ohio - Voting Rights,* http://www.house.gov/kucinich/issues/voting.htm (accessed Apr. 15, 2005).

45. Commissioners, United States Election Assistance Commission, http://www.eac.gov/hillman.asp?formatNone (accessed Oct. 18, 2005).

46. For the sake of convenience, I have used this term to refer to both "Diebold Incorporated" and "Diebold Election Systems, Incorporated" who were both parties to the Swarthmore lawsuit described more fully *infra*.

47. *See e.g.*, Top Stories, http://www.diebold.com/dieboldes/top_stories.htm (accessed Oct. 18, 2005) (detailing sales by Diebold to state and local entities during relevant period).

machines to various state and local entities.[48]

In March 2003, a hacker broke into a Diebold computer and leaked about 15,000 internal company memoranda regarding Diebold's e-software.[49] These memoranda included discussions of bugs in Diebold's software and warnings that its computer networks were poorly protected against hackers.[50] The Diebold memoranda began circulating over the internet, and were posted by numerous groups, including a group of college students at Pennsylvania's Swarthmore College who posted an archive consisting of approximately 13,000 Diebold emails containing the memoranda in question.[51] Relying on the DMCA, Diebold sent notices to Web sites that hosted the archived emails demanding that the infringing materials be taken down.[52] In its notices, Diebold specifically alleged that the email archives contained copyrighted, proprietary material belonging to Diebold.[53] In response to the notices, Swarthmore ordered the students to remove the documents from the university Web site.[54]

In response to the takedown notices from Diebold, the Online Policy Group, and two Swarthmore College students who maintained a Web site that had hosted the archived emails at issue, filed a declaratory judgment action against Diebold, seeking, *inter alia*, injunctive relief for copyright misuse, and damages for misrepresentation of copyright claims under the DCMA.[55] They further sought a declaration that the publication of the Diebold emails was lawful.[56] Diebold eventually agreed that it would not send any more notices to ISPs involved in publishing the

48. John Schwartz, *File Sharing Pits Copyright Against Free Speech*, N. Y. Times (November 3, 2003) (available at http://www.nytimes.com/2003/11/01/business/media)(accessed April 15, 2005)

49. *Id.*; *see also* Kim Zetter, *Students fight E-Vote Firm*, http://www.wired.com/news/business/ 0,1367,60927,00.html (accessed Apr. 15, 2005).

50. The presence of some of these flaws was later confirmed in July 2003 when an independent study of a hacked copy of the software was conducted by a team of experts from Johns Hopkins and Rice Universities. The study found flaws which, if exploited, would allow someone to vote repeatedly or to change the votes of others. A later review of the software by the State of Maryland agreed that the software flaws did exist but found that other practices would keep the vulnerabilities in the code from being exploited. *See* Schwartz, *supra* n.8.

51. *Id.*

52. *Id.*

53. *See generally* Complaint, *On Line Policy Group v. Diebold, Inc.*, ¶40 (available at http://www.eff.org/legal/ISP_liability/OPG_v_Diebold/complaint.php)(accessed Apr. 15, 2005)(hereinafter "Diebold Complaint"). *See also Online Policy Group v. Diebold, Inc.*, Order Granting in Part and Denying in Part Cross-Motions for Summary Judgment (Sept. 30, 2004)(available at http://eff.org/diebold/legal/ISP_liability/OPG_v_Diebold/20040930_Diebold_SJ_order.pdf)(accessed Apr. 15, 2005) (hereinafter "Diebold Summary Judgment").

54. *Id.*

55. *See generally* Diebold Complaint, ¶¶ 66 -81.

56. *See generally* Diebold Complaint, ¶¶ 82 – 89.

emails at issue.[57] As a result of this agreement, the court ultimately found that plaintiffs' claims for injunctive and declaratory relief were moot. Nevertheless, the court found that claims regarding Diebold's *past* use of the DMCA to prevent publication of the emails remained actionable.[58]

B. When the DMCA is Abused

The use by Diebold of procedures designed to protect music from digital pirates to prohibit the dissemination of information regarding e-voting security underscores the problems that current DMCA procedures pose to the free circulation of speech and information. The DMCA was *never* created to stifle either speech or public debate.[59] Yet the use by Diebold of notice and take down procedures *as currently crafted* achieved such a result. In fact, the court in *Diebold* expressly found that Deibold's actions had suppressed content whose use *did not* qualify as copyright infringement.[60] Use of the DMCA notices to seek removal of this material was clearly outside the scope of DMCA procedures.[61]

Relying on the fair use doctrine, the court found that Diebold's actions had resulted in the actual suppression of content over which Diebold had no claim for copyright infringement.[62] The court's decision was based in part on a narrow factual finding that Diebold had failed to identify which of the 13,000 archived emails contained copyrighted content.[63] The heart of the decision, however, was based firmly on a finding that the critical public interests involved supported the plaintiffs' fair use of the materials.[64] In emphasizing the importance of the public interests at issue, the court stated: "The email archive was posted or hyperlinked to for the purpose of informing the public about the problems associated with Diebold's electronic voting machines. It is hard to imagine a subject the discussion of which *could be more in the public interest*."[65]

Eschewing any attempt to blame the plaintiffs for any harm caused by the unauthorized publication of the email archive, the court recog-

57. *See On Line Policy Group v. Diebold, Inc.*, Plaintiff's Post Hearing Letter and Supplemental Ng Declaration (Nov. 24, 2003), Transcript of Law & Motion Hearing pp. 3:24–4:3 (Feb. 9, 2004), available at http://eff.org/diebold/legal/ISP_liability/OPG_v_Diebold/hearing)(accessed Apr. 15, 2005).

58. Diebold Summary Judgment 10.

59. *See* nn. 101-106 *infra and accompanying text.*

60. Diebold Summary Judgment at 12–13.

61. Diebold Summary Judgment at 13.

62. Diebold Summary Judgment at 12-13.

63. Diebold Summary Judgment at n.14.

64. Diebold Summary Judgment at 11.

65. Diebold Summary Judgment at 11 (emphasis added).

nized: "At most, Plaintiffs' activity might have reduced Diebold's profits because it helped inform potential customers of problems with machines. However, copyright law is not designed to prevent such an outcome."[66] The court emphasized the transformative nature of Plaintiffs' use, describing such transformation *on a functional basis*: "[The plaintiffs] used the email archive to support criticism that is in the public interest, not to develop electronic voting technology."[67] Ultimately, the court found that Diebold "knowingly materially misrepresented that Plaintiffs' infringed Diebold's copyright interest, at least with respect to portions of the email archive clearly subject to the fair use exception."[68] It harshly criticized Diebold's actions, stating:

> No reasonable copyright holder could have believed that the portions of the email archive discussing possible technical problems with Diebold's voting machines were protected by copyright, and there is no genuine issue of fact that Diebold knew – and indeed that it specifically intended –that its letters to OPG and Swarthmore would result in prevention of publication of that content. . . . The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA's safe harbor provisions – which were designed to protect ISPs, not copyright holders – as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.[69]

The court's ultimate determination that Diebold's knowing misrepresentation violated Section 512(f) of the DMCA arguably demonstrates that the built-in protections against abuse work. Under the provisions of the DMCA, as currently crafted, Diebold's acts were a clear abuse of the process *and were found to be such* in a properly conducted legal challenge which granted the Swarthmore students a right of relief for Diebold's abuse under Section 512(f).[70] Granting monetary relief against those who "knowingly, materially misrepresent" that material or activity is infringing, however, smacks strongly of closing the barn door after the proverbial horse has escaped. Although the owner of the horse may appreciate compensation for the harm caused by having to track her horse down, when that horse represents something as fundamental as speech related to political activity, money is hardly a sufficient or timely remedy.

---

66. *Id.*

67. *Id.*

68. Diebold Summary Judgment at 12.

69. Diebold Summary Judgment at 13.

70. Section 512(f) provides a cause of action for the "knowing material misrepresentations" regarding either the infringing nature of the material at issue, or the mistaken removal of the material. 17 U.S.C. § 512(f). Remedies under the statute, however, are limited to "damages, including costs and attorneys' fees." *Id.*

C. What Diebold Didn't Tell Us

While *Diebold* is the paradigmatic case for problems with the notice and take down provisions of the DMCA when critical speech issues are involved,[71] *Diebold* didn't touch on two additional critical barriers that the DMCA poses to a full and frank examination of the security issues surrounding electronic voting machines. One of the cornerstones of the DMCA was its new legal protection for technological access barriers designed to prevent unauthorized reproduction of protected works. Briefly, Section 1201 prohibits the circumvention of technological measures that effectively control access to a copyright protected work[72] as well as, and perhaps more importantly, the trafficking in any "technology, product, service, device, component, or part thereof" that "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a protected work."[73] Originally used for its intended purposes of prohibiting the circumvention of copy protection codes on CDs and DVDs,[74] these same provisions could be used to prevent the private testing of electronic voting machines or, perhaps even more importantly, the dissemination of such test results without the permission of the owner of the voting technology at issue.

Because electronic voting machines use technology to protect their record keeping, problems can only be discovered by outsiders if such "technological protection measures" are circumvented. If the software is copyright protectable, which is likely,[75] and the security measures protecting such software are found to qualify as an "effective technological measure" under the Act, which is also highly likely,[76] then any circum-

71. Not all speech, however, is created equal. *See e.g. Chaplinksky v. New Hampshire*, 315 U.S. 568 (1942); *Brandenburg v. Ohio*, 395 U.S. 444 (1964). *See also* nn. 101–107 *infra and accompanying text.*

72. 17 U.S.C. §1201(a)(1)(A).

73. 17 U.S.C. § 1201(6). The device must also have "only limited commercially significant purpose or use other than to circumvent protection afforded by a[n effective] technological measure. . . ." *Id.* at §1201(b)(1)(B).

74. *See e.g. Universal City Studios, Inc. v Corley*, 273 F.3d 429 (2d Cir. 2001); *Paramount Pictures Corp. v. 321 Studios*, 69 U.S.P.Q. 2d 2023 (S.D.N.Y. 2004).

75. *See e.g. Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3rd Cir. 1983), cert dismissed*, 464 U.S. 1033 (1984); *Lexmark Intl. Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Ky. 2003)(court found that code which controlled toner cartridges had sufficient originality to qualify as a copyright protected work that could fall within the scope of protection of the DMCA), *vacated and remanded*, 387 F.3d 522 (6th Cir 2004)(court found district court had failed to apply the appropriate originality standard and suggested that access codes may lack originality based on their utility function).

76. The "effectiveness" standard for qualifying technology has been set at such a low threshold that the test is virtually non-existent. *See generally Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp.2d 294 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

vention must be authorized by the copyright owner.[77] In other words, under the DMCA, Diebold has the exclusive right to authorize such circumvention.[78] It is a rare provider indeed who would be willing to expose its product to such rigorous and uncontrolled testing, absent legal compulsion to do so.

Had the information that the students at Swarthmore College disclosed regarding potential security flaws in the software been uncovered by one of the students, and not an employee of Diebold who was presumably authorized to circumvent protection measures and make such tests in the course of employment, then the result of Diebold's challenge under the anti-circumvention provisions of the DMCA would have been extremely different. Although the DMCA has exemptions for both encryption research and security testing, those exemptions are so narrowly crafted that they do not readily fit the activities of third parties.[79] To qualify for an exemption under the encryption research provisions, the research in question must be limited to activities "conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."[80] The individual must have obtained the encrypted copy "lawfully" (tough to do for most e-voting software, which is not generally available "off the shelf")[81] and must have "made a good faith effort to obtain authorization before the circumvention (no unknown circumvention, please).[82] The individual must generally be a professional in the area (no amateur researchers need apply)[83] and the only person to whom their results are mandated to be dis-

77. Despite the potential loophole that fair use can be used to defend against charges of unauthorized circumvention under Section 1201(a), which protects measures to secure authors their rights under copyright, such a fair use defense is not available where the protection measure is also used to prevent access or to defend against a charge of trafficking in circumvention devices. *See e.g. Universal City Studios, Inc. v. Corley,* 273 F.3d 429 (2d Cir. 2001); *US v. Elcom Ltd.*, 203 F. Supp 2d 1111(ND Cal. 2002). Thus, despite the *Diebold* court's proper determination that use of copyrighted works to assist in information dissemination regarding the security of Diebold's voting software qualified as a fair use, such defense is unavailing to those who seek to test the security of the software where the technological measures at issue are *a fortiori* designed to protect access.

78. This does not mean that legislation cannot mandate such outside testing.

79. See 17 U.S.C. §§ 1201(g) & (j).

80. 17 U.S.C. § 1201(g)(1)(A).

81. 17 U.S.C. §1201(g)(2).

82. *Id.*

83. One of the key factors in determining whether a person qualifies for exemption is "whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced in the field of encryption technology." 17 U.S.C. § 1201(g)(3). Thus, the deck is heavily stacked in favor of professionals. Interested amateurs are not absolutely precluded, but the presumptions are heavily stacked against their acts qualifying for exemption.

closed is the copyright owner.[84] In fact, there is virtually no recognition of any right to further dissemination absent the copyright owner's permission.[85] In a worst case scenario, under the DMCA Diebold might even have been able to enjoin links to information regarding the security of its software.[86]

The DMCA also contains an exception for "security testing."[87] Such testing, however, is limited to "good faith testing, investigating or correcting a security flaw or vulnerability" of a "computer, computer system, or network."[88] This language seems to exclude testing of individual software per se. More problematic, such testing is strictly limited to testing authorized by the owner or operator of such equipment,[89] which would appear to exclude any outside amateur testers. The same problematic limitations on dissemination under the encryption research testing apply to security testing, making this exemption even less applicable to amateur and other outside testers than the encryption research exception.[90]

The expedited subpoena provisions of Section 512(h) described above also could prove a powerful tool against those who seek to test the security of e-voting software, or disclose the results of any such testing. As noted above, in addition to serving a notice for take down of the allegedly infringing information, Diebold could also have sought the names of the students who posted the material under Section 512(h), purportedly for purposes of bringing individual actions against them for copyright infringement. Unlike the notice and takedown provisions which required

84. One of the factors to be considered under Section 1201(g) is whether the person conducting the research provides the copyright owner "with notice of the findings and documentation of the research, and the time when such notice is provided." 17 U.S.C. §1201(g)(3)(C). Section 1201(g) also considers whether the information was disseminated, and if so, if it was disseminated in a manner "reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates . . . a violation of applicable law . . . including a . . .breach of security." 17 USC §1201(g)(3)(A). While the statute does not preclude public dissemination of research, it leans heavily in favor of controlled dissemination, exercised largely by the copyright owner. None of these factors favor an amateur e-voting tester.

85. *Id.*

86. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001)(linking prohibited as a form of trafficking under Section 1201).

87. 17 U.S.C. §1201(j).

88. *Id.*

89. *Id.*

90. Similar to the encryption research exception under Section 512(g), one of the factors to be considered in determining whether a person qualifies for the exemption under Section 1201(j)(3)(A) is whether the information is "used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system or computer network." 17 U.S.C. § 1201(j)(3)(A).

the university to give the students notice of the demand,[91] no such notification is required under Section 512(h).[92] The students would have no right to notice or to even challenge the subpoena *prior to disclosure* unless their service provider elected to provide such notice.[93] Few subscribers follow such path.[94] The few that have done so, however, have generally been successful in restricting what appears to be a pattern of overreaching.[95] Fortunately, this is one area where courts are beginning to take action to correct the problem. Thus, for example in *Elektra Entertainment Group, Inc. v. Does 1- 6*,[96] involving subpoenas sought under Rule 45 of the Federal Rules of Civil Procedure, the court required the ISP to notify subscribers whose identities were sought for the purpose of allowing the subscribers to file a motion to quash or vacate the subpoena against them.[97] The notice, however, went farther than merely requiring notice of the subpoena. In the notice, the court established a twenty-one day response period, provided information regarding potential jurisdictional challenges that could be raised against the subpoena and even provided a "resource list" for guidance on finding an attorney to represent any subscriber, including the contact information for organizations such as the American Civil Liberties Union of Pennsylvania and the Electronic Frontier Foundation, who were identified as "friends of the court" ready to "help you consider your legal options."[98]

III. REFORM IS NEEDED NOW TO PROTECT CORE POLITICAL VALUES

Diebold's use of the DMCA to prevent the publication of information regarding security concerns with its voting software puts the Copyright Act on a direct collision course with the First Amendment. Political

91. *See* 17 USC §512(g)(2)(requiring service provider to "[take] reasonable steps promptly to notify the subscriber that it has removed or disabled access" to the material subject to a proper notice pursuant to Section 512(c)).

92. 17 U.S.C. §512(h)(5)(requiring the service provider to "expeditiously disclose" the information required under the subpoena with no corresponding obligation to notify the end user of the subpoena before or after such disclosure).

93. *Id.*

94. Seth Schiesel, *Your Own Affair, More (VCR) or Less (MP3),* N. Y. Times (Oct. 2, 2003)(stating that with the exception of SBC every major internet provider has complied with the RIAA's subpoena requests)(available at http://scrawford.blogware.com/blog/_archives/2003/10/5/ 3902.html)(accesssed Oct. 18, 2005).

95. *See e.g. RIAA v. Verizon Internet Serv., Inc.*, 352 F.3d 69 (D.C. Cir. 2003); *Elektra Entertainment Group, Inc. v. Does 1 -6*, Civ. Action No. 04-124 (ED Pa.2004)(available at. http://www.eff.org/IP/P2P/RIAA_v_ThePeople/20041012_Order_Granting_Request.pdf (accessed Oct. 18, 2005).

96. Civ. Action. No. 04-1241 (E.D. Pa. 2004) (available at http://www.eff.org/ IP/P2P/ RIAA_v_ThePeople/20041012_Order_Granting_Request.pdf (accessed Oct. 18, 2005).

97. *Id.*

98. *Id.* (Court –Directed Notice Regarding Issuance of Subpoena).

speech lies at the heart of Constitutional First Amendment rights.[99] Nothing seems more "political" than information about the reliability of voting machines, and, ultimately, the fairness of the election process. Yet the DMCA contains no exceptions for such critical fair uses. *Worse, it contains insufficient remedies to curb potential abuses.*[100]

Contrary to popular press, copyright and free speech are *not* natural enemies. The primary goal of copyright law is to encourage the creation and distribution of new works.[101] These works in turn expand the marketplace of ideas the free speech clause of the Constitution was designed to protect.[102] As the Supreme Court in *Eldred* properly recognized, copyright serves as "the engine of free expression," whose "limited monopolies are compatible with free speech principles."[103] Even in *Diebold*, the court acknowledged that potential conflicts between copyright protection and free speech are "ameliorated in part" by the idea/expression dichotomy,[104] the originality requirement which excludes facts from copyright protection,[105] and the fair use doctrine.[106]

Yet copyright is often perceived as the enemy of speech.[107] Indeed, much of the legal activity surrounding the DMCA involves challenges to its impact on the First Amendment.[108] Such challenges have proven largely unsuccessful to date.[109] Nevertheless, as the *Diebold* case dem-

99. *See e.g.* Alexander Meiklejohn, *The First Amendment is an Absolute*, 1961 Sup. Ct. Rev. 245, 255 (1961); Cass R. Sunstein, *Democracy and the Problem of Free Speech* (Free Press 1995); Geoffrey Stone, *Perilous Times: Free Speech n Wartime From The Sedition Act of 1798 to the War on Terrorism* (WW Norton & Company 2004).

100. The only remedies available for abuse of the process under the DMCA are monetary damages. Surely, where speech is being suppressed, after the fact monetary awards for misrepresentation under Section 512(f) is too little, too late, particularly when such core Constitutional values are at stake.

101. *See e.g.* U.S. Const. Art.I, § 8, cl. 8 (giving Congress the power to enact copyright laws to "promote the progress of science and the useful arts").

102. *See e.g. Abrams v. U.S.*, 250 US 616 (1919)(Holmes, dissent).

103. *Eldred v. Ashcroft*, 537 US 186 (2003).

104. *See e.g.* 17 U.S.C. § 102(b)(excluding ideas from copyright protection); *Baker v. Selden*, 101 US 99 (1879).

105. *See e.g. Feist Publications, Inc. v. Rural Tel. Serv. Co. Inc.*, 499 U.S. 340 (1991).

106. *See e.g.* 17 U.S.C. § 107; *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994); *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539 (1985).

107. Mary Beth Peters, *Copyright Enters the Public Domain*, 51 J Copyr. Socy. 705 (2004).

108. *See e.g. U.S. v. Elcom Ltd.*, 203 F. Supp. 2d 1111(N.D. Cal. 2002); *Universal City Studios, Inc. v Corley*, 273 F.3d 429 (2d Cir. 2001); *In re Verizon Internet Services Inc., Subpoena Enforcement Matter*, Civ. Action No. 03-MS-0040 (D.C. Cir. 2003) (available http://www.dcd.uscourts.gov/03-ms-0040.pdf)(accessed Oct. 18, 2005) (denying motion to quash subpoena based in part on the claim that the expedited subpoena provisions of Section 512(h) qualify as an unconstitutional prior restraint on speech).

109. In all of the cases cited in n. 108 *supra*, the First Amendment defenses raised were ultimately unsuccessful.

onstrates, poorly designed legal "fixes" to technological problems create false conflicts that detract from the real issues at stake. Quite simply, lawmakers are never as prescient as we hope. Like most of us, they failed to appreciate that anti-circumvention provisions would ever be used to stifle public debate over accuracy of voting systems. They failed to include critical exceptions to permit speech-related activities to guarantee secure and accurate electronic voting and they failed to provide sufficiently strong remedies to guarantee that abuses of the process, such as those by Diebold, would not only be discovered but punished severely enough to serve as a deterrent to others who would seek to abuse the DMCA. These oversights must be corrected so that copyright can once again be brought into its proper relationship as a supporter and promoter of First Amendment values.

At a minimum, the right to obtain injunctive relief for misrepresentations must be included among the remedies available under Section 512(f) so that abuses can be properly stopped without waiting for public opinion. While such opinion has been notably fast to date in cases involving perceived abuses of the DMCA,[110] public opinion can as easily be manipulated in the opposite direction.[111] Moreover, a legal system that simply establishes public opinion as the sole determinant for liability is no legal system at all, but an abdication of the rule of law whose unintended consequences I think we all would rather avoid.

Second, the subpoena provisions of the DMCA must be modified to *require* notice to the subscriber before his/her identity is disclosed. While twenty-one days may be too long to allow infringing materials to remain on the web given its rapid dissemination rate,[112] clearly a reasonable time must be given to allow subscribers to defend critical privacy interests in the face of potential over reaching by copyright owners.

---

110. *See e.g.* Lawrence Lessig, *Jail Time in the Digital Age*, N. Y. Times (July 30, 2001)(discussing Dimitry Skylarov prosecution and threat of prosecution of Princeton University Professor for disclosing encryption research both allegedly in violation of the DMCA); Amy Harmon, *Adobe Opposes Prosecution in Hacking Case*, N. Y. Times (July 24, 2001)(Adobe opposes prosecution of Skylarov in response to public outcry); John Schwartz, *2 Copyright Cases Decided in Favor of Entertainment Industry*, N. Y. Times (Nov. 29, 2001); John Schwartz, *Diebold Decides Not to Sue Over Internet Postings*, N. Y. Times (Nov. 26, 2003)(Diebold drops complaint in face of publicity).

111. Frank Rich, *The Great Indecency Hoax*, N. Y. Times (Nov. 28, 2004)(public complaints support indecency fines. Study indicates threatened fine of $1.2 million based on 159 public complaints which were actually written by 23 individuals. Of these 23 all but 2 were identical to a form letter posted by the Parents Television Council).

112. This was the period of time granted by the court in *Elektra Entertainment Group, Inc. v. Does 1- 6*, Civ Action. No. 04-1241 (E.D. Pa. 2004)(available at http://www.eff.org/IP/P2P/RIAA_v_ThePeople/20041012_Order_Granting_Request.pdf (accessed Oct. 18, 2005). *See* discussion *supra* n. 85.

Third, the encryption and security testing exceptions must be expanded to allow for legitimate testing, including by amateurs, of encryption and security devices. The scope of such exceptions could still remain based on a legitimate expectation that such testing be directed toward facilitating encryption research, with requirements that any such research be disseminated first to the owner of the technology. If the goal is to empower protection technologies, there is no legitimate reasons why such information should not be disclosed to the copyright owner in the first instance. Concerns that the copyright owner will take steps to suppress further dissemination of "harmful" information can be dealt with through appropriately crafted statutory factors that emphasize the public interest in such dissemination. Where critical first amendment concerns are impacted, such as in the *Diebold* case, public dissemination should be favored.

IV. CONCLUSION

The DMCA was not created and should not be used to stifle public discussion of critical issues relating to the security of the voting process. But for a few public-minded students, Diebold's abuse of the DMCA might have gone unchallenged. Reform of the DMCA is long past due. The Act must be strengthened to continue to allow copyright owners to bring legitimate claims to stop the rampant digital piracy that threatens the economic bargain contained in the Constitution[113] and mirrored in the DMCA. At the same time, reforms must be made to remedy the potential for abuse. Only when such reforms are achieved can the Copyright Act re-take its position as a supporter of First Amendment values.

113. *See* U.S. Const. art. I, § 8, cl. 8 (granting Congress the power to enact copyright laws which would grant to authors *exclusive* rights to their works for limited periods of time).