Vol. 11 No. 4, July 2006

The ethics of DeCSS posting: towards assessing the morality of the Internet posting of DVD copyright circumvention software

Kristin R. Eschenfelder, Robert Glenn Howard & Anuj C. Desai

School of Library and Information Studies, Department of Communication Arts, and Law School at the University of Wisconsin-Madison

change font

Abstract

Introduction. We investigate the conditions under which posting software known as "DeCSS" on the Internet is ethical. DeCSS circumvents the access and copy control protection measures on commercial DVDs. Through our investigation, we point to limitations in current frameworks used to assess ethical computer based civil disobedience.

Method. The paper draws on empirical findings of actual DeCSS posting to consider the limitations of current frameworks. Findings were generated from content analysis of Web sites that post DeCSS using search engine sampling with file name, language, and server location delimiters. Content analysis examined the number of Websites hosting DeCSS, the presence or absence of speech related to DeCSS and Free/Open Source software, and the arguments explaining DeCSS posting.

Analysis. Drawing on theorizing from political philosophy and the existing frameworks, the paper compares characteristics of actual DeCSS posting to the existing frameworks.

Results. The paper points out six areas that require further attention in ethical frameworks: determining motivation for posting, deciding whether some groups have more moral standing to post, assessing knowledge of the laws related to circumvention and posting, determining if protesters have taken related political actions, the legality of various formats of circumvention devices, and the physical geography of the participants.

Introduction

Recent years have seen numerous examples of the creation and Internet release of programs that allow unauthorized access to protected digital media. For example, Dimtri Sklyarov and his Russian company ElcomSoft created a program for reading for Adobe e-books; Jon Johansen and a group of European hackers created software called 'DeCSS' that permits the viewing of DVDs on unauthorized playback devices; and more recently, Johansen has broken Apple's proprietary copyright protection system (DVD-cracking... 2003, DVD Jon... 2004; Delio 2003). Intellectual property industry groups have labelled these programmers as crackers or pirates; and in some cases, these programmers have been arrested, or charged with committing a crime against intellectual property owners. User rights groups retort that the programmers are being unfairly prosecuted and that the laws these programmers have broken are unjust.

These examples are significant as they make up part of a larger conflict involving intellectual property owners, user

rights groups, pirates, computer hackers and others relating to norms and expectations for use rights for digital materials, and growing industry practices of placing copy and access control devices on digital media such as CDs and DVDs. These examples bring up questions about the circumstances under which it is ethically (if not legally) acceptable to bypass or 'circumvent' access and copy control devices placed on digital works. This paper explores the ethics of posting DeCSS (a circumvention device to bypass the access and copy controls on DVDs) on the Internet.

While the last decade has seen increasing consumer adoption of digital media such as CDs, DVDs, and e-books it has also seen the proliferation of personal computers and other hardware that facilitate making exact copies of digital content, and increased broadband access to the Internet, which facilitates easy trading of unauthorized copies of digital works.

In an effort to head off widespread copying and Internet distribution of copyrighted works, copyright owners have begun to implement technological locks known as 'digital rights management' technologies on their digital copyrighted works. These technologies contain both access locks that control access and use of materials, and copy locks that explicitly control copying of materials. However computer hobbyists have routinely 'picked' these locks by creating software-based tools to undo the protection. These software 'picks' are known as 'circumvention devices'.

Concerned that widespread distribution of circumvention devices would lead to an increase in copyright infringement, intellectual property trade groups such as the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) sought to outlaw such devices. Beginning with proposals in the United States in the early 1990s, legal prohibitions on circumvention devices were eventually written into the World Intellectual Property Organization (WIPO) Internet treaties in 1996. In the United States, Congress implemented the WIPO Internet treaties by passing the Digital Millennium Copyright Act (DMCA), which, among other things, prohibits the distribution of circumvention devices. Although many countries are not party to the WIPO Internet treaties, the European Union (EU) has issued a Directive that requires EU countries to pass laws prohibiting the distribution of circumvention devices, and many U.S. bilateral trade agreements (including those with countries such as Australia, Singapore, and Chile) require passage of similar laws.

This paper focuses on DeCSS, a circumvention device for DVDs, and the laws prohibiting its distribution. DVDs are manufactured with a digital rights management device that prevents unauthorized DVD playback devices from accessing the content on the DVD, which is called 'CSS' (short for the 'Content Scramble System'). According to Taylor's 'DVD Demystified', CSS is composed of several layers of encryption and authentication (2001). Use of CSS is licensed by the DVD Copy Control Association (DVDCCA). This regime, in effect, requires that all DVD playback device manufacturers purchase a license so their players can access the content of CSS protected DVDs (Taylor 2001). According to the DVDCCA 'CSS is a two-part system for which manufacturers of both the movie content (discs) and hardware or software (players) purchase licenses. The information on DVD discs is encrypted. The DVD players - either a computer drive or a home video player - have technology to 'decrypt' the information so it can be viewed.' (2004) Another aspect of the DRM is its 'region controls', which places region flags on both DVDs and DVD playback devices and requires a region match between the two before the content of the DVD can be accessed. The goal of the region controls is to manage the distribution and pricing of DVDs across different global regions (Taylor 2001).

Intellectual property owners claim that the DRM combined with anti-circumvention laws prevent piracy of DVDs. As the DVD CCA notes, 'Without sufficient protections, movie studios would not have offered their copyrighted films to consumers in this high quality digital format.' (2004) But critics charge that CSS and region controls in the DRM additionally prevent many traditionally legal user rights. For example, the DRM currently used on DVDs disallows playing of DVDs manufactured in a different *region* of the world. It also prevents users from directly duplicating even a small portion of movies they lawfully purchase. Moreover, the DRM did not allow users to play DVDs on a computer running a Free/Open Source (F/OS) operating system because no licensed DVD player for F/OS computer existed.

Purportedly in response to the inability to play DVDs on F/OS computers, in the fall of 1999 a group of European hackers including Jon Johansen released DeCSS on the Internet. Many Websites made mirror copies of the program or linked to other Websites posting the program. A number of movie studios then sued many of the operators of those Websites under the anti-circumvention provisions of the Digital Millennium Copyright Act in 2000. In August 2000, the court issued its final judgment in the case (known as the *Corley* case), prohibiting the defendants from

posting DeCSS or linking to other Web sites where DeCSS could be downloaded (Universal City Studios v. Reimerdes 2000).

DeCSS became a focal point for those opposed to the DMCA's legal protection for copyright protection technologies, and DeCSS posting has been widely adopted among the digerati for the variety of reasons we outline in the next section. And while one court case exists that illuminates the legal status of DeCSS posting in the United States, the ethical status of DeCSS posting is unclear.

This paper looks closely at empirical data about DeCSS posting in order to determine the extent to which DeCSS posting is morally, if not legally, acceptable. In doing so, the paper takes the negative moral implications of digital rights management systems as given. It focuses on the question of whether characteristics of posting or authorship should affect our judgment of DeCSS posting as ethical. In doing so, the paper draws on frameworks for ethical hacking and civil disobedience (Manion & Goodrum 2000; Rawls 1999). The paper uses empirical data to point to relevant considerations that an ethical framework would need to incorporate including the following questions.

- Does the DeCSS poster need to include an explanation or rationale for why they post DeCSS?
- Does the quality or validity of the arguments used to explain DeCSS posting matter?
- Do some groups or individuals have more moral standing to post DeCSS?
- Must a DeCSS poster have exhausted all legal means of changing copyright law before posting DeCSS?

In examining characteristics of DeCSS posting, the paper draws on data from two previous studies of DeCSS posting in the United States, the European Union, the People's Republic of China, and Hong Kong (Eschenfelder & Desai 2004; Eschenfelder *et al.* 2005; Eschenfelder, *et al.* forthcoming b). These studies involved content analysis of Web sites posting the DeCSS code to determine how much DeCSS posting was going on, the nation of origin of DeCSS Web sites, arguments used by Web authors to justify their posting of DeCSS, the affiliation of Web site authors to the Free/Open Source movement, and the cultural meaning of DeCSS as its presented on the Web sites.

Ethical arguments against prohibition of circumvention devices

The arguments against the DMCA's prohibition on circumvention devices include the proposition that DRM prohibit *fair use* of legally purchased material. The American fair use doctrine permits some copying without the authorization of the copyright holder when the copying meets the criteria of fair use (Russell 2004). The original American conception of copyright is based on the view that a balance between protection and unauthorized use would promote the arts and sciences. In this sense, society has seen some unauthorized copying as desirable for cultural and innovation reasons and sought to protect that class of uses (Vaidhyanathan 2001).

In the USA, the DMCA permits circumvention of a copy lock for fair use purposes, but it prohibits circumventing an access lock. But the DMCA forbids the distribution of, or *trafficking in* both access keys and copy keys, making it difficult, if not impossible, for users to obtain a key to open the copy lock. Furthermore, access locks typically encase copy locks. This makes it impossible for a user to open a copy lock without illegally opening the access lock. Critics charge this is similar to placing a public park inside of heavily guarded public property with no public right of way (Lipinski 2003).

Critics also charge that the prohibition of circumvention devices enforces key licensing schemes developed by the owners of digital works that require playback device manufacturers to purchase licenses. Manufacturers of DVD players who desire their machines to legally play encrypted DVDs must pay a license fee to movie copyright holders (Simons 1999; Samuelson 2003). For example, Free or Open Source software advocates argued that hackers created DeCSS so that users could view legally purchased DVDs on a computer using Free or Open Source operating systems. At the time, no licensed Free or Open Source DVD players existed.

In enforcing the licensing scheme, critics charge the prohibition on circumvention devices supports corporate price fixing. DVDs contain region codes that restrict access to the work to DVD players sold in particular regions of the world by requiring a match between the region code on the DVD and the region code embedded in a DVD player. These region codes increase copyright holders' power to control pricing and release dates. Cheaper DVDs cannot be imported from elsewhere and resold in the USA, as they will not contain the correct region code to allow playback on a standard USA DVD player. Critics see DRM as part of a larger business strategy to control global flows of information and establish a regime of compulsory licensing of media players that financially benefits the copyright

interests (Samuelson 2003; Simons 1999).

Critics also express concern that the anti-circumvention provisions essentially criminalize reverse engineering and in doing so may limit consumers' ability to further develop and use F/OS software to develop playback devices for consumer media (Stallman 2002; Raymond 1998; Samuelson 2002; Samuelson 2003; Simons, 1999; Touretzky 2001). Prohibition of the circumvention of DRM leaves the consumer unable to legally crack access locks in order to find out how the software they have purchased functions. Opponents see the *right to tinker* as both an inherent right of the legal purchaser of software and as an important component of software innovation and education (Felten 2003; Samuelson 2002).

Some fear the prohibition of circumvention devices will stifle innovation and research in software development and F/OS software by chilling professional and scientific communications about DRM related software such as encryption and watermarking (Grove 2003; Lessig 2002; Lessig 2004; Simons 1999; Stallman 2002; Tien 2000). Many computer scientists argue that computer code is a form of speech and, as such, should not be regulated by the government (Touretzky 2001). Because circumvention devices for digital materials consist of software code, these opponents see the wholesale prohibition on their distribution as a problematic restriction on speech.

DRM facilitate stronger control over access and use of works than previously possible with paper materials (Lipinski 2003). Critics charge that DRM technologies, in combination with restrictive licensing practices, can be used to prevent traditional first sale uses by determining how often a user may access a work, or how much of the work they may access (Camp 2003; Foroughi, Albin & Gillard 2002). First sale rights permit the owner of a copy of a work to display, lend, or resell that physical copy. Some suggest that copyright interests seek to change consumers' expectations about what types of rights come with purchase of a copyrighted work – moving consumers to a pay-per-use distribution model where purchase of a work no longer includes unlimited use (Samuelson 2003).

Ethical evaluation frameworks

The literature contains numerous depictions of on-line activism, e-protest, e-civil disobedience, or 'hacktivism' (Denning 1999; Lievrouw 2003; Manion & Goodrum 2000; McAdam *et al.* 2001; Vegh 2003). Past authors have defined online activism as the use of computers to organize and manage protest activity (McAughey & Ayers 2003), and hacktivism as the use of computer code to generate effects similar to physical protest or civil disobedience. Some argue that hacktivism, which we will refer to in this paper as e-civil disobedience, differers from computer-based malfeasance such as cracking or cyber-terrorism in terms of the following types of considerations (Manion & Goodrum 2000):

- whether or not the action causes damage to property – or the degree of that damage (i.e., avoiding damage to critical infrastructure or severe economic damage);
- whether the action entails violence;
- whether the actions have a profit motive;
- whether actors are willing to accept responsibility for outcomes of actions; and
- whether actors have an ethical motivation, such as seeking change to stop oppression, inequality, or injustice.

In assessing e-civil disobedience, one can also draw on political philosophy literature related to civil disobedience. Martin Luther King Jr. described civil disobedience as the open, willing, and loving breaking of an unjust law – where protesters do not seek to overturn whole legal system or bring down civil society (King Jr. 1969). Rawls defines civil disobedience more narrowly as 'public, non-violent, conscientious yet political act contrary to law usually done with the aim of bringing about a change in the law or policies of the government' (Rawls 1999: 320). Rawl's definition of civil disobedience requires that protesters break laws, but not necessarily those laws that they seek to change.

Rawls's framework has several additional requirements that go beyond the criteria outlined above, and that become important in our discussion of DeCSS posting. First, he claims that those engaged in civil disobedience must knowingly violate the law. Second, they must justify their acts in terms of political principles rather than religious or moral principles or self-interest. Further, Rawls argues that civil disobedience is really only justifiable in certain circumstances: for instance where actors have experienced 'substantial' injustice, when normal appeals for change to political institutions have been unsuccessful, and when the disobedience itself does not lead to a larger breakdown in respect for law and civil society.

Consideration of the relevant characteristics of legitimate DeCSS posting requires that we compare the characteristics of the real-life DeCSS posting to the e-civil disobedience and justified civil disobedience frameworks outlined above. In the next section, we describe the characteristics of DeCSS posting that we observed from past studies.

What we know about DeCSS posting

Brief overview of methods

The data in this section are drawn from two separate studies involving automated collection of DeCSS posting pages stemming from search engine searches, and content analysis of the contents of the resulting Web pages. Here we provide a brief description of our methodology and its limitations, but interested readers can find more detailed information about both in the publications cited below.

Data for each of the studies were generated from search engine based samples in which the authors used names of DeCSS files as queries in the Altavista and Google search engines. The queries produced hundreds of results which we cleaned to remove repeats, consolidate related pages, and remove pages that did not actually post the DVD software. After producing a final set of functional DeCSS posting Websites, we performed content analysis on the unit of analysis for each study - the Website content related to DeCSS, its related court cases, and its related political issues (e.g., copyright law, reverse engineering, free speech).

The first study's sampling frame was drawn from an English language only query on the AltaVista search engine in January 2001 and then again in March 2003 using the terms "DeCSS" and "DECSS". After cleaning, the sample included twenty-eight Websites from the first date and twenty-three from the second. Content analysis examined each Website to determine changes in the number of DeCSS posting pages over time, the amount of text related to DeCSS on the Websites, and whether or not the authors referred to Free/Open Source software on the Websites (Eschenfelder & Desai 2004; Eschenfelder *et al.* 2005). In addition, two of the authors analyzed the arguments used on the Websites in terms of codes developed through a review of the literature, grounded analysis of a subset of the data, and extensive pretesting including numerous rounds of code book revisions. All arguments coded had intercoder reliability scores above 85%, indicating acceptable levels of reliability (Krippendorf 2004).

The second study employed the Google search engine's application programmer interface to restrict the sample to Websites hosted in pre-2004 expansion European Union nations, Hong Kong, Macau, and the People's Republic of China. This analysis involved eighty-seven unique Websites from eighteen nations. Resulting Websites, including Websites in ten different languages, were translated to English by native or experienced speakers of each language prior to further analysis. The content analysis for the second study included the nation of origin of each Website, the amount of text related to DeCSS on the Website, whether or not the Website referred to Free/Open Source software, and whether or not the Website made references to laws or legislation related to DeCSS. (Eschenfelder *et al.* 2005).

It is important to keep in mind that search engine based samples do not represent random samples, rather they represent popular pages likely to be included in search engine indexes, which do not include all Websites. They would not include very new Websites, less popular Websites, or sites that block search engine robots. Further, our content analysis relied on clues present on Websites to infer Website author intention and motivation. Interviews or other data collection methodologies would provide more illuminating data in this area. Despite these limitations, the data do provide a useful backdrop to assess current ethical frameworks.

Range and variation in DeCSS posting

Past research shows that DeCSS posting has slowly declined since the *Corley* trial, but as of spring 2004, it was still widely available. This research also shows that DeCSS posting varies by nation. Of the nations included in past research, DeCSS posting is more prevalent in the U.S., the Netherlands, Germany, France, and the UK. No active DeCSS posting was observed in the People's Republic of China.

Past research shows that Websites varied in the degree to which they included text about DeCSS that explained the DeCSS posters motivations or rationale. We observed three types of DeCSS posting.

Type 1. File names only. These Websites contained no arguments or justifications. They merely offered a label/link

to download the DeCSS code. The label was some form of DeCSS (e.g., decss.exe or css-auth.tar.gz). For example in the following image, while the site contains a good deal of extra information, none of it is about DeCSS (Note we have blocked all information that identifies Websites in our images.)

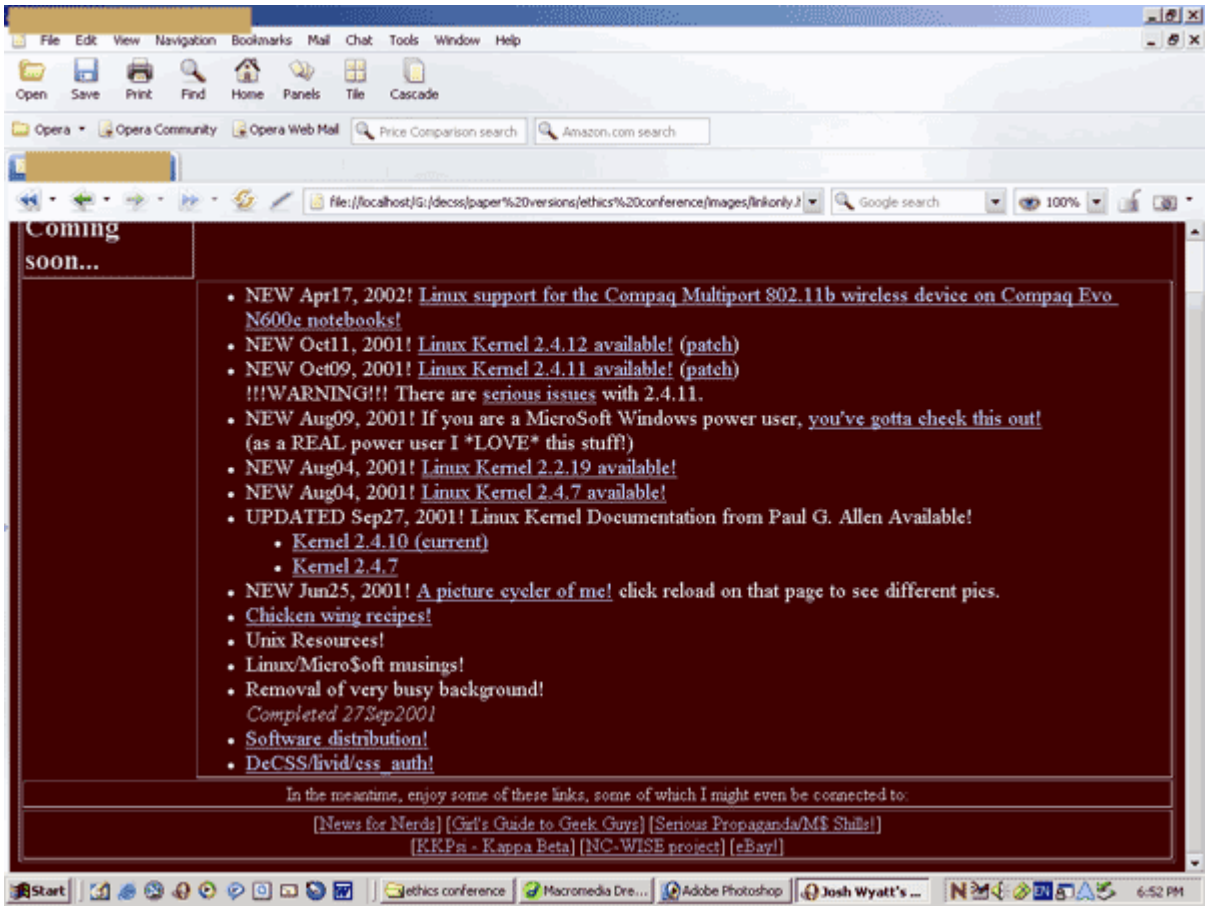

Figure 1: Example of Type 1 file names only DeCSS posting Website

As shown in the next image, Figure 2, other Type 1 sites consisted of software archives that contained no text beyond the label for the DeCSS file and information about the file system structure.

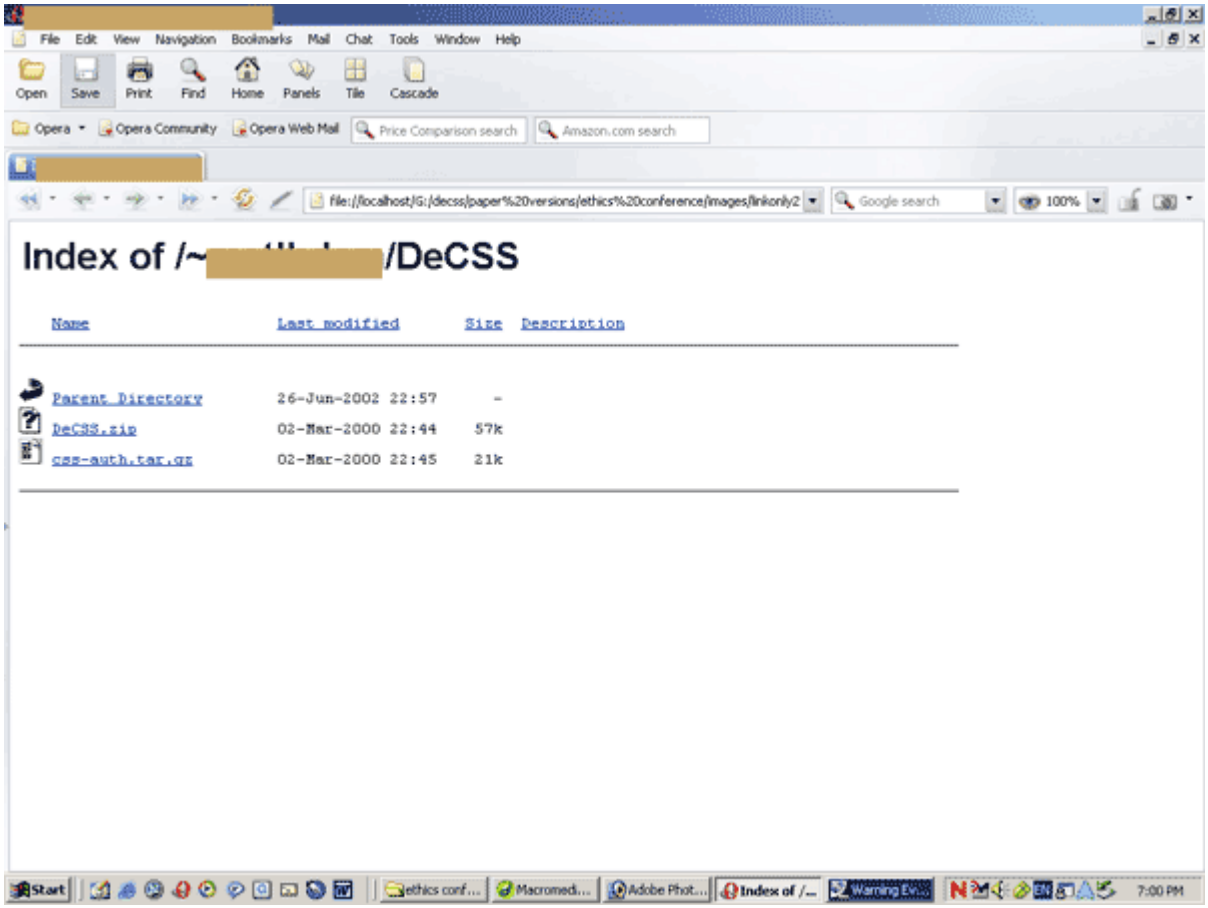

Figure 2: Another example of Type 1 File names only DeCSS posting Website

Type 2. Annotated links. These Websites contained no arguments or justifications, but the label or link included some brief explanation such as "decss.exe download the famous DeCSS code".

Type 3. Ambiguous. These Websites contained a fragmented or ambiguous argument or explanation that frequently required substantial inference. For example, one site asked visitors to 'Help 2600 in their fight against the powers that be' Other sites simply carried the following graphic admonishing viewers to "submit to the MPAA".

Figure 3: Example of image from Type 3 ambiguous Website

Type 4. Elaborated arguments. These Websites included arguments that included both a claim and an overt justification of that claim. They required little interpretation by the reader. (e.g., 'Help 2600 fight against the powers that be because those powers are stealing our fair use rights to DVDs that we have legally purchased!') Not all Type 4 arguments were equally elaborated however. Some arguments (e.g., 'Corporations are Bad' 'Copyright Law is Bad') are still fairly ambiguous, while others (e.g., 'Viewer of Choice') were less so.

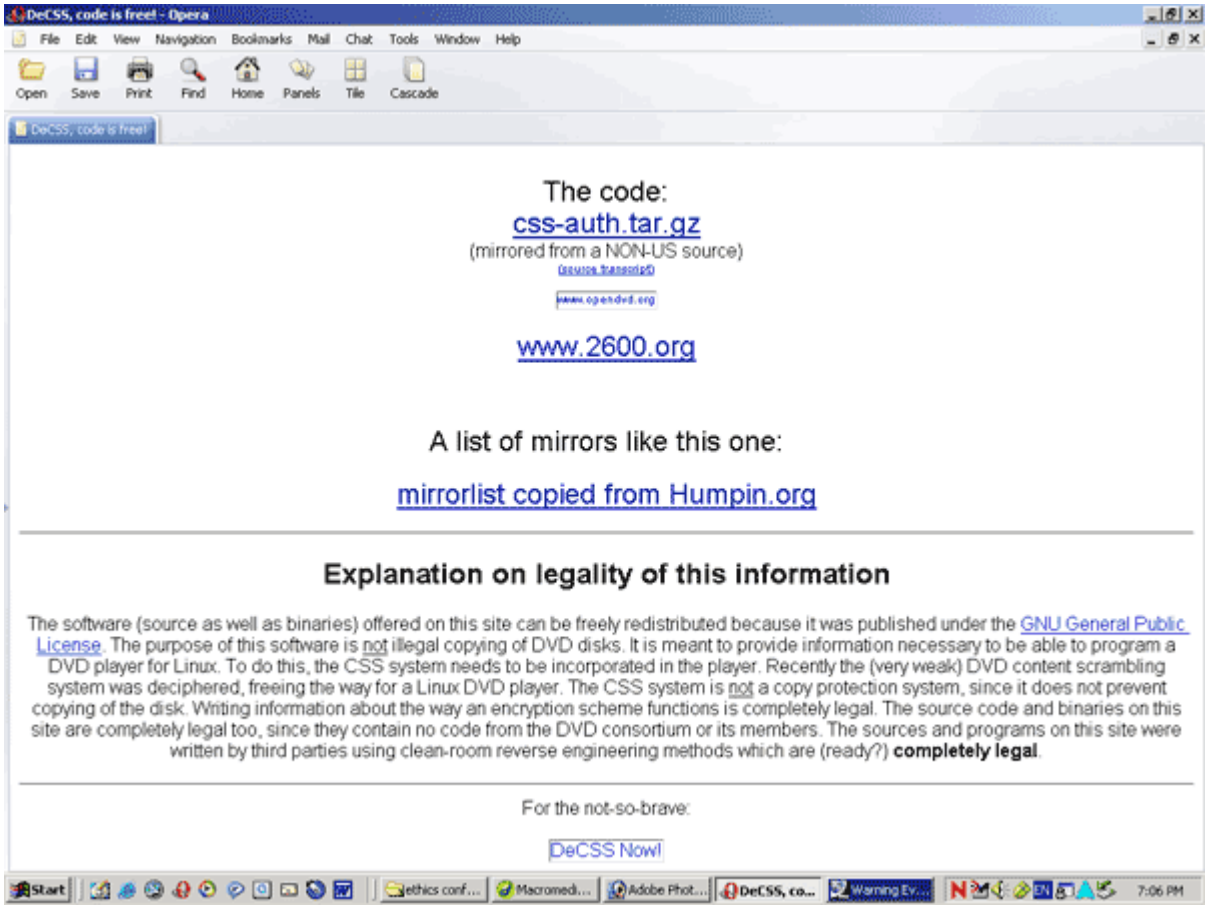

Figure 4: Example of Type 4 Website

One important finding was that most Website authors did not include sufficient text to explain why they posted DeCSS. Most sites fell into the Type 1 or Type 2 categories, with many sites containing only file names and most sites containing less than 200 words related to DeCSS.

File type

DeCSS posting also varied in terms of the type of file posted. In most cases, Websites included an executable format of the DeCSS code. In numerous cases however, Website authors included DeCSS in a format which would have required some manipulation before use. For example, Website authors posted prime numbers that one could use to re-engineer the code, screen snapshots of code, graphical images with embedded code. For example, Figure 5 below is an image of Jack Valenti, former head of the MPAA with a version of the DeCSS code embedded into the image.

Figure 5: Jack Valenti image with embedded DeCSS

Arguments used

Our content analysis of the Type 3 and Type 4 sites identified the motivations or rationale used by those DeCSS posters: we analyzed these using a set of 'arguments' developed from the literature and pretesting. The most popular argument was 'Viewer of choice' in which the poster claims that consumers lawfully purchasing DVDs have the right to play the DVD on a machine running the operating system of their choice (e.g., a F/OS operating system such as Linux, FreeBSD, etc.), or that corporations or copyright interests are attempting to restrict such rights.

The second most popular argument was 'Scare tactics' in which DeCSS posters justify posting by arguing that copyright interests are trying to intimidate people by using or misusing the law including cease and desist orders

and bringing lawsuits. In the third argument, 'Piracy occurs without DeCSS', the posters argue that DeCSS does not promote or cause piracy, that most piracy occurs without DeCSS, or that CSS is an access control system, not a copy control system and, therefore, that DeCSS is not a copyright piracy tool.

In the 'Current copyright law is bad' argument, posters explain that the ideals of copyright law have been warped to fit corporate goals. Current copyright law is unjust or will have negative effects. In the 'Corporations are bad' argument, posters make the claim that corporations and copyright interests are bad for some undefined reason, for example that corporations are violating some undefined right of consumers. In the 'Current copyright Law is bad' and 'Corporations are bad' arguments, DeCSS posters did not state what aspects of copyright or corporate behaviour they found undesirable. Other popular codes such as 'Scare tactics'; 'Abuse of legal system', 'Piracy occurs without DeCSS', 'Reverse engineering', and 'Free speech' made more specific claims.

In the 'Reverse Engineering' argument, the author argues that reverse engineering is legal and therefore the hacking of CSS or region codes by using DeCSS on legally purchased materials should not be prohibited. In the 'Free speech' argument, the DeCSS posters claimed that the prohibition on posting DeCSS challenges free speech rights.

References to law

Past studies also show that the majority of sites made no reference to laws related to DeCSS. In the English language site study, five sites from each sample referred to law. A few referred to specific laws or court cases (e.g., 'DMCA', 'Corley', the 'NY lawsuit').

Additional sites made less specific references to law. For example, one author referred to 'moronic Patent/Copyright law.' Others referred to court cases without identifying the case by name (e.g., 'recent legal actions').

Additionally, some sites did not mention either specific laws or general areas of law, but referred readers to other Websites that contained significant legal content, suggesting that the Website authors were aware of the legal implications of DeCSS.

In the European Union and China study, a similarly small number of sites referred to the EU Copyright Directive or to specific national level laws.

Data also show that DeCSS posters in one nation sometimes referred to laws in other nations that did not apply to them, but arguably served as influences guiding the change of laws in their home nations. For example, numerous EU posters commented on the US DMCA. In some cases, DeCSS posting was not clearly illegal in the poster's home nation.

Further, sometimes DeCSS posters referred not to national laws, but to larger global copyright harmonization frameworks such as the WIPO treaties or the EU Copyright Directive. Finally, as noted in the previous section, authors employed the 'copyright law is bad' argument without any explanation of what aspects of copyright law (home nation, other nation, international) the author found unjust.

Piracy context

The data from the two studies show that DeCSS posters from China and the EU presented DeCSS in different contexts on their Websites. In the People's Republic of China, DeCSS posters present DeCSS as an audio-visual or cracking tool.

In contrast, in the E.U. and the U.S., DeCSS was either presented in no context (Type 1 or 2) or in a political context, surrounded by text referring to one of the arguments outlined above. We did not find any examples of USA or E.U. sites presenting DeCSS in an explicit piracy context, and we found several that specifically disavowed any piracy uses for DeCSS.

Free or open software affiliation

Data from both studies suggest some affiliation between DeCSS posting and Free or Open Source software identification or use. Many, but not all, DeCSS posters referred to free/open software or the associated community.

Moreover, the strength of those references varied. In the English-language study, less than twenty percent of Websites did not refer to Free or Open Source software. In the EU-China study, Chinese sites made few references to such software, but many EU sites did.

Under what circumstances are the posting of circumvention devices morally permissible?

In this section, we draw on the empirical data to point to relevant considerations that an ethical framework would need to incorporate. As outlined earlier, Manion and Goodrum distinguished between computer based malfeasance and legitimate e-civil disobedience in terms of five characteristics: damage done to persons or property, use of violence, existence of a profit motive, the willingness to accept responsibility for outcomes of actions, and ethical motivation (Manion & Goodrum 2000).

The political philosophy theorizing further emphasizes that in order for protest to qualify as civil disobedience, participants must knowingly violate the law, and they must justify their acts in terms of political principles rather than religious or moral principles or self-interest. Rawls also argues that civil disobedience is only justified in circumstances of substantial injustice, when normal appeals for change to political institutions have been unsuccessful, and when the disobedience itself does not lead to a larger breakdown in respect for law and civil society.

Several areas of these frameworks seem unproblematic in relation to the DeCSS posting we observed. We found no evidence that DeCSS posters damage physical property; and, if they only make fair use of DVDs they own, they do no harm to intellectual property. One could argue however that by perpetuating the availability of circumvention devices, DeCSS posters allow others to copy DVDs they do not own. We found no evidence that DeCSS posting leads to violence against persons. We did not find any Websites selling DeCSS. Finally, by posting DeCSS on public Websites with static intellectual property addresses, the authors are making themselves traceable. In fact, many DeCSS posters included contact information on their Websites. This suggests that the Website authors are willing to be held responsible for their actions.

Six areas of the ethical framework were more problematic. First, in many cases it was difficult to determine the motivation of many DeCSS posters. Further, some groups may have more moral standing to post DeCSS because of harm they experience or expect to experience. Third, the Websites provided little knowledge of DeCSS posters' knowledge of laws related to DeCSS. Moreover, Websites provided no information about the degree to which DeCSS posters have taken other actions to try to change anti-circumvention laws. Fifth, questions remain about the legality of various formats of the DeCSS code. Finally, given the transnational nature of much DeCSS posting, the relation of physical geography, legality, and the definition of 'civil disobedience' becomes problematic.

Motivation for posting DeCSS

The empirical results from the studies raise the question of whether Website authors need to explain why they post DeCSS in order for their actions to be ethical. But the lack of arguments on Type 1 or Type 2 Websites made it difficult to assess the motives of DeCSS posters. One might dismiss all the Type 1 and 2 Websites as unethical, but theorizing from the communication and rhetoric fields suggests that even unannotated links could be considered as arguments because when they are viewed by a certain audience familiar with the socio-political context of DeCSS, they evoke arguments related to DeCSS (Habermas 1974; McGee 1990; Zulick 1997). This argument, however, assumes that the Website builder imagines his or her audience as one that is familiar with the discourse related to DeCSS.

For example, assume that DeCSS poster Tom is part of a professional circle of Free or Open Source software programmers. He had read extensively about the implications of the DMCA, the *Corley* case, and anti-circumvention in general. He maintains a Website which he expects fellow programmers to visit in order to gain more information about him. He posts DeCSS on this Website with no accompanying explanation or justification. Other developers who visit the site and who are also familiar with the larger conversation about DeCSS in the Free or Open Source software community may see that Tom posts DeCSS and perceive that Tom is 'in the know' politically, and that Tom is concerned about the effect of circumvention prohibition on free and open software development. Other people who visit the site, who are not of that community, may know nothing about the larger

conversation about DeCSS in the community and may not understand why Tom posts DeCSS.

In essence, the posting of DeCSS functions much as does the wearing of a pink ribbon at a public ceremony. While the ribbon makes no elaborated argument on its own, it refers to a heavily elaborated argument already current in public discourse: that more effort should be placed into researching the deadly disease of breast cancer.

But even Type 3 or 4 Websites were sometimes problematic if they did not contain a very well elaborated justification. Type 3 Websites had little elaboration and required substantial interpretation. But some Type 4 arguments, like 'copyright law is bad' and 'corporations are bad', were often expressed such it was unclear what aspects of copyright law or corporate behaviour justified DeCSS posting. Further, in several cases claims made by DeCSS posters, references to related laws were incorrect.

From this perspective, some arguments seemed 'better' in the sense that they were more elaborated; they stated clear and reasonable reasons for posting DeCSS. We are not saying that these arguments are good in some absolute sense (though they may be), but they do permit a reader to see what the DeCSS poster is arguing on both sides of the (stated or implied) "because" clause.

A group's moral standing

Another issue raised by the data is whether any particular group has more moral standing to post DeCSS. That is, can some people, because of their group affiliation, morally post DeCSS while others cannot? One might argue that Free or Open Source software users have more standing to morally post DeCSS because they stand to lose more. Many argue that hackers created DeCSS to facilitate viewing of legally purchased DVDs on computers using the Linux operating system (Bing 2003). Some such users fear that DRM and anti-circumvention laws could inhibit further development of Free or Open Source software, which relies on reverse engineering techniques that have traditionally been viewed as legal (Samuelson 2002, 2003; Simons 1999). One can argue that DeCSS is an early move by copyright interests to exclude Free or Open Source compliant systems from future entertainment media innovations.

This suggests that Free or Open Source software users have more to lose than other groups. Free or Open Source software users could have more of a moral standing to post DeCSS as they arguably suffer the clearest and greatest injustice if DRM and anti-circumvention laws do prevent future Free or Open Source software development. But what of the moral standing of non-Free or Open Source software-affiliated DeCSS posters? Many may object to the anti-circumvention laws for reasons unrelated to open source. For example, one may object to the erosion of fair use and first sale user rights institutionalized by the law and the technology and not experience serious negative effects. It is unclear to what extent one must directly experience injustice before DeCSS posting becomes justified. It is also unclear to what extent one can one post DeCSS preemptively, i.e., to protest injustice that is reasonably expected as an outcome of the law.

DeCSS poster's knowledge of the law

Our data suggest that the civil disobedience requirement that protesters knowingly violate the law may be problematic for DeCSS posting. In most cases, DeCSS posters did not make it clear whether their posting was inspired by the law; further, it was not clear whether they knew anything of the law. The popularity of arguments such as 'Corporations are bad' and 'Scare tactics' suggests that some DeCSS posters could be protesting corporate behaviour or the methods of legal prosecution rather than the law itself. Further, while the argument 'Copyright law is dad' suggests that at least some posters were aware of the connection between DeCSS and copyright law, the code excluded those arguments that pointed to specific areas of copyright law (e.g., fair use concerns, anti-circumvention provisions). Thus use of the 'Copyright law is bad' code indicates only a general reference to law and does not indicate that the poster is aware of the anti-circumvention provisions.

This raises the question of whether the protest would qualify as e-civil disobedience if the DeCSS poster is unaware of the law, only vaguely aware of the law, or only aware of the effects of the law (i.e., allows a company to hire a legal firm to send cease and desist notices), rather than the law itself.

In many nations, the legality of posting DeCSS will not be known until someone brings a case against DeCSS posters under a national law (rather than that of a lower jurisdiction). Further, anti-circumvention law is highly

complex, subject to different codifications from country to country in the EU and possibly even different interpretations in the jurisdiction of different regional courts within nations (e.g., the US Circuit Court system). It seems unrealistic to expect DeCSS posters to fully grasp all of its intricacies of the emergent law. However, Rawls' framework seems to suggest that in order for protest to qualify as civil disobedience, protesters must clearly understand that that they are breaking the law. In cases where individuals believe that they are not breaking the law, or they show a lack of understanding of the law, it is unclear whether the DeCSS posting qualifies as an act of civil disobedience, although the posting might still be considered a moral form of protest.

Other protest behaviour

Rawls' definition of justified civil disobedience also requires that prior attempts to change the law through normal political institutions have been unsuccessful. Most of the Websites we observed did not provide sufficient information to determine what other protest actions, if any, that DeCSS posters have taken. Larger public interest groups have taken steps to try to change copyright laws associated with DeCSS. For example, within the United States, groups such as the American Library Association (ALA) and Association of Computing Machinery (ACM) have lobbied Congress for changes to or exemptions from the current law, and have lobbied against passage of new laws that would place even further restriction on consumer use of digital works. Finally, numerous Free or Open Source software groups protested in person during the *Corley* trial in the United States. If we assume that these groups have tried and failed to persuade lawmakers and rule makers to change the law, then individual DeCSS posters actions seem more justified. Further information is needed about the activities of public interest groups in other nations that have passed, or are considering passage of anti-circumvention laws.

Types of DeCSS code

The U.S. *Corley* legal proceedings related to DeCSS attempted to distinguish between functional types of code (e.g., source code or executable files) that can be easily downloaded and used, and non-functional types of code such as discussions of code. Dr. David Touretzky of Carnegie Mellon University created a 'DeCSS Gallery of Descramblers' that displays a collection of the various incarnations of DeCSS including t-shirts, poems, music, and encoded prime numbers. In creating the Gallery, Touretzky wished to draw attention to the difficulty of drawing meaningful distinctions between computer code and other forms of expression protected by free speech rights (Touretzky 2001; Touretzky 2000).

Despite Touretzky's criticism, the *Corley* court viewed the functional (executable) code posted in that case as regulable under the First Amendment largely because an executable file can directly result in a computer performing activities that are unprotected by free speech principles with virtually no human action. So, with an executable file, merely clicking a mouse results in the computer engaging in unprotected activity (Universal City Studios v. Corley 2001). In contrast, with a non-functional form of code, the code is analogous to a blueprint, a recipe, or a piece of sheet music. It can do nothing on its own and acts more as a medium of communication between and among humans; computer programmers in particular. In our studies, we observed that some authors chose to post a non-functional form of DeCSS. We have no information about their intentions, but arguably they did so in order to minimize the possibility of being sued. If national anti-circumvention laws are interpreted to permit the distribution of a non-executable version of the DeCSS code, then posting non-functional forms of DeCSS would not be viewed as e-civil disobedience because the Website authors would be choosing not to break the law (as it was defined in the *Corley* case). But since the law distinguishing between the legality of different types of code is murky at best, one could argue that posting any type of DeCSS code entails potential legal action.

Geography

The anti-circumvention and anti-trafficking laws in the DMCA and their application in the *Corley* case were part of a larger, global development in copyright law brought on by the World Intellectual Property Organization (WIPO) Internet treaties. The treaties call on signatories to pass laws restricting the circumvention of copyright protection devices (WIPO 2004). The implementing legislation for the treaties in the US and the EU were the DMCA and the EU Copyright Directive respectively. While neither the WIPO treaties nor the EU Copyright Directive impose obligations directly on individuals, seven of the fifteen pre-2004 EU countries have passed national anti-circumvention laws to comply with the Copyright Directive (as of 1 January 2004), and these laws are directly binding on citizens.

With the increased ease of real-time communication across national borders, citizens are more aware of the actions of other governments; and citizens in one nation regularly protest other nations' laws or larger global institutions such as WIPO or the World Trade Organization (Cunningham 1999; Florini 2000). Assessment of protest activity must therefore consider 'transnational resistance' in which actors protest against other nations' laws or against larger global institutions that do not necessarily directly affect them (Tarrow 1998).

This raises the question of whether the concept of civil disobedience can encompass protesting against laws that do not directly apply to the protester, either because they are laws of another nation, or they are international treaties that do not directly bind individuals. Our DeCSS posters from nations without anti-circumvention laws, or with laws that arguably permit non-commercial DeCSS posting, may consider themselves 'global citizens' resisting larger transnational institutions or legal trends rather than national-level laws and legal rulings (Cunningham 1999; Florini 2000; Tarrow 1998). This suggests that ethical frameworks must account for protest actions aimed at broader legal trends that could result in undesirable social impacts, or longer-term undesirable changes to national level laws, rather than focusing solely on protest actions aimed at a directly applicable national law.

Conclusion

Others have argued that the political intentions and ethical dimensions of many instances of e-civil disobedience tend to be overlooked (Manion & Goodrum 2000). This suggests that we need articulated tools to help us consider the moral implications of acts that some perceive as *electronic civil disobedience*. This paper examined the case of Internet Websites posting the DeCSS circumvention software for DVDs. The paper's analysis of DeCSS posting in terms of ethical frameworks offers numerous lessons that can be applied more widely in the ethical examination of other types of electronic civil disobedience, and particularly in other examples of Internet based circumvention device distribution. Comparing empirical findings of studies of DeCSS posting with ethical electronic civil disobedience or hacktivism frameworks, this paper identified relevant considerations that an ethical framework for circumvention device posting should include.

Recent history suggests that as more digital works come to be protected by DRM, circumvention tools to break those DRM will be created and posted on the Internet. Those wishing to draw attention to the political and ethical dimensions of circumvention device posting need to define the conditions under which they consider the posting of circumvention devices to be ethical, and they need to develop methodologies for determining the degree to which the defined conditions are met.

Past authors have emphasized the need to analyze the statements left by hacktavists to determine their motivations (Manion & Goodrum 2000), but our analysis of the DeCSS data shows that most posters did not make clear elaborated arguments for posting DeCSS. Further, our examination of DeCSS posting and its relation to Free or Open Source software affiliation pointed out that some groups might have more moral standing to post DeCSS. We also found it difficult to determine whether DeCSS posters had any knowledge of the law. Further, sometimes determining the nature of the law is difficult given the changing and untested nature of the law itself. This is even more the case with respect to the posting of non-functional forms of DeCSS.

The frameworks drawn from the literature assume a good deal of knowledge about the DeCSS poster. The problems we experienced draws attention to the limitations of content analysis as a methodology, and the need for interviews or ethnographies to better determine motivation, group affiliation, and legal knowledge. Further, the ethical frameworks suggest that in order to determine whether civil disobedience is justified, more detailed knowledge is needed of the state of anti-circumvention laws in particular nations and protest activities related to those laws.

References

- Bing, J.J. (2003, January). *Sunde vs. Johansen* (English Translation). Oslo: Norwegian Research Center for Computers and Law.
- Camp, L. (2003, June). First principles of copyright for DRM design. *IEEE Internet Computing*, **7**(3), 59-65.
- Cunningham, H. (1999). The ethnography of transnational social activism: understanding the global as local practice. *American Ethnologist*, **26**(3), 583-604.
- Delio, M. (2003, December 13) Russian hacker charges dropped. *Wired News.* Retrieved 9 July, 2006 from http://www.wired.com/news/politics/0,1283,49122,00.html

Denning, D. (1999). Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy. In, John Arquilla and David Ronfeldt, (Eds.). *Networks and Netwars: the future of terror, crime, and militancy* (pp. 239-288) Santa Monica, CA: RAND Corporation. Retrieved 9 July, 2006 from http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

- DVD Copy Control Association (n.d.) 'Frequently Asked questions' Retrieved 9 July, 2006 from http://www.dvdcca.org/faq.html
- DVD-cracking teen acquitted. (2003, January 7) *Wired News*. Retrieved 9 July, 2006 from http://www.wired.com/news/politics/0,1283,57107,00.html
- DVD Jon strikes again. (2004, August 15) *Wired News*. Retrieved 9 July, 2006 from http://www.wired.com/news/privacy/0,1848,64591,00.html
- Eschenfelder, K.R. & Desai, A.C. (2004). Software as protest: the unexpected resiliency of U.S. based DeCSS posting and linking. *The Information Society*, **20**(2), 101-116.
- Eschenfelder, K.R., Desai, A.C., Alderman, I., Sin, J. & Shen Yi (2005). The limits of DeCSS posting: a comparison of Internet posting of DVD circumvention devices in the European Union and China, *Journal of Information Science*, **31**(4), 317-331
- Eschenfelder, K.R., Howard, R.G. & Desai, A.C. (2005). Why do Website authors post DeCSS?: a content analysis of political speech on Websites posting DVD decryption software. *Journal of the American Society for Information Science and Technology*, **56**(13), 1405-1418
- Felten, E. (2003). A skeptical view of DRM and fair use. *Communications of the ACM*, **46**(4), 56-59.
- Florini, A.M. (2000). *The third force: the rise of transactional civil society*. Washington, DC: Carnegie Endowment for International Peace: Brookings Institution Press
- Foroughi, A., Albin, M. & Gillard, S. (2002). Digital rights management: a delicate balance between protection and accessibility. *Journal of Information Science*, **28**(5), 389-395.
- Grove, J. (2003). Viewpoint: legal and technological efforts to lock up content threaten innovation. *Communications of the ACM*, **46**(4), 21-22.
- Habermas, J. (1974). The public sphere. *New German Critique*, **1**(3), 49-55.
- King Jr., M. L. (1969). Letter from the Birmingham jail. In R. Goldwin (Ed.), *On civil disobedience: american essays, old and new* (pp. 61-78). Chicago, IL: Rand McNally & Company.
- Krippendorf, K. (2004). *Content analysis: an introduction to its methodology*. Thousand Oaks, CA: Sage.
- Kruger, B. (2002). Assessing the potential of Internet political participation in the United States: a resource approach. *American Politics Research*, **30**(5), 476-498.
- Lessig, L. (2002). *The future of ideas*. New York, NY: Random House.
- Lessig, L. (2004). *Free culture: how big media uses technology and the law to lock down culture and control creativity*. New York, NY: Penguin Press.
- Lievrouw, L. (2003). When users push back: oppositional new media and community. In M. Huysman, E. Wenger & V. Wulf (Eds.), Communities and technologies: proceedings of the First International Conference on Communities and Technologies. (pp. 391-406). Dordrecht, Netherlands: Kluwer.
- Lipinski, T. (2003). The myth of technological neutrality in copyright and the rights of institutional users: recent legal challenges to the information organization as mediator and the impact of the DMCA, WIPO and TEACH. *Journal of the American Society for Information Science and Technology*, **54**(9), 824-835.
- Litman, J. (2001). *Digital copyright*. Amherst, NY: Prometheus Books.
- Manion, M. & Goodrum, A. (2000, June). Terrorism or civil disobedience: toward a hacktivist ethic. *Computers and Society*, **30**(2), 14-19.
- McAdam, D., Tarrow, S. & Tilly, C. (2001). *Dynamics of contention*. Cambridge: Cambridge University Press.
- McAughey, M. & Ayers, M. (2003). Introduction. In M. McAughey & M. Ayers (Eds.), *Cyberactivism: online activism in theory and practice* (pp. 1-19). New York, NY: Routledge.
- McGee, M. C. (1990). Text, context, and the fragmentation of contemporary culture. *Western Journal of Speech Communication*,**54**(3), 274-289.
- Rawls, J. (1999). *A theory of justice*. Cambridge, MA: Belknap Press.
- Raymond, E. (1998). The cathedral and the bazaar. *First Monday*, *3*(3). Retrieved 9 July, 2006 from http://www.firstmonday.org/issues/issue3_3/raymond/index.html
- Russell, C. (2004). *Complete copyright: an everyday guide for librarians*. Washington DC: American Library Association Office for Information Technology Policy.
- Samuelson, P. (2002). Legally speaking: reverse engineering under siege. *Communications of the ACM*,**45**(10), 15-20.
- Samuelson, P. (2003). DRM {and, or, vs.} the law. *Communications of the ACM*, **46**(4), 41-45.

Simons, B. (1999). To DVD or not to DVD. *Communications of the ACM*, **42**(5), 31-32.
- Stallman, R. (2002). *Free software, free society*. Boston, MA: GNU Press
- Tarrow, S. (1998). *Power in movement: social movements, collective action and politics*. Cambridge: Cambridge University Press.
- Taylor, J. (2001). *DVDs demystified*. New York, NY: McGraw-Hill.
- Tien, L. (2000). Publishing software as a speech act. *Berkeley Technology Law Journal*, **15**(2), 629-712.
- Touretzky, D. (2000). *Source code vs. object code: a false dichotomy*. Pittsburgh, PA: Carnegie Mellon University Retrieved November 2004 from http://www-2.cs.cmu.edu/~dst/
- Touretzky, D. (2001). *Gallery of DeCSS descramblers*. Retrieved 9 July, 2006 from http://www.cs.cmu.edu/~dst/DeCSS/Gallery.
- Touretzky, D. (2001). Free speech rights for programmers. *Communications of the ACM*, **44**(8), 23-25
- Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000)
- Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001)
- Vaidhyanathan, S. (2001). *Copyrights and copywrongs*. New York, NY: New York University Press.
- Vegh, S. (2003). Classifying forms of online action. In M. McAughey & M. Ayers (Eds.), *Cyberactivism: online activism in theory and practice* (pp. 71-95). New York, NY: Routledge.
- Weber, L., Loumakis, A. & Bergman, J. (2003). Who participates and why? *Social Science Computer Review*, **21**(1), 26-42.
- World Intellectual Property Organization. (n.d.). WIPO Treaties. Retrieved 9 July, 2006 from http://www.wipo.int/copyright/en/treaties.htm.
- Zulick, M. (1997). Generative rhetoric and public argument: a classical approach. *Argumentation and Advocacy*, **33**(3), 109-119.