

**Information Communication Technologies and Framing for Backfire in the Digital Rights  
Movement: the Case of Dmitry Sklyarov's Advanced e-Book Processor**

Hector Postigo

Associate Professor, Broadcasting Telecommunications and Mass Media

Temple University, Philadelphia PA, USA

## **Abstract**

In 2001, Dmitry Sklyarov was arrested for his role in designing the Advanced e-Book Processor, the software that cracked Adobe's e-Book encryption. Using historical data and situating itself within social movement theory, this article focuses on the case of Sklyarov's arrest to show how the digital rights movement, by using online networks, mobilized activists and framed the event in a manner that led to "backfire" against government prosecutors and Adobe Systems Inc. The case illustrates positive outcomes for social movements when they use movement-specific online networks – networks that help to rapidly define the meaning of issues and that have the potential to inform mass media outlets, and through them, broader publics.

**Keywords:** Social Movements and ICTs, Hackers, Digital Rights, DMCA, Copyright, EFF

## **Introduction**

### **The Digital Rights Movement**

The digital rights movement is a concerted international effort by activists, hackers,<sup>1</sup> student groups, academics, and social movement organizations to ensure digital media users' rights. In the U.S., the movement has focused on issues of privacy, free speech, user access to media, and freedom to innovate. Typically, the movement has reacted against changes in copyright law that have increasingly restricted the types of use consumers can make of their legally purchased digital media. Movement actors fight for a "user-centered" concept of fair use where consumers have greater freedom to access and use copyrighted content for creative and personal purposes.

The digital rights movement is situated within the current copyright debate that has occupied much scholarly work in the past ten years. The advent of the internet and the pervasive adoption of digital media by consumers prompted early policy makers to formulate restrictive interpretations of copyright law. Much of that policy formulation centered on fears that digital technologies, along with the connectivity of the internet, would allow for rampant copyright violation (Postigo, 2006). As law professor Jessica Litman has pointed out, this prompted media companies to interpret copyright law quite narrowly and support legislation that would criminalize copyright protection circumvention technologies while at the same time encourage the development of technological protection measures (TPMs) for license agreements and copyright (Litman, 2001).

The resulting legislation, the Digital Millennium Copyright Act (DMCA), is an amendment to the U.S. Copyright Statute that has drastically shifted the balance of copyright in favor of

copyright owners (Lessig, 1999, 2001a, 2001b, 2004; Litman, 2001; Samuelson, 1999). During its formulation and immediately thereafter, legal scholars and citizen organizations voiced their concerns over the DMCA's shortcomings, focusing primarily on its anti-circumvention provisions and the effects these would have on fair use, free speech, and innovation (Benkler, 1999; Boyle, 1997; Lessig, 1999; Litman, 1994, 2001; Samuelson, 1999).

The sections of the DMCA that have received the most criticism are the anti-circumvention provisions. These provisions prohibit the conduct of circumventing TPMs that control access to copyrighted content, making cracking or breaking a technological lock illegal. The anti-circumvention provisions also prohibit the manufacture and distribution of technologies that might help in carrying out circumvention. All together, they outlaw making and distributing technologies that might "hack" into protected media. Importantly, the DMCA puts a great stake in the deployment of TPMs for protecting digital content by implicitly accepting the impracticality of enforcing copyright in digital media and by de-legitimizing circumvention and the technologies that make it possible.

The digital rights movement has employed a host of tactics in its pursuit of a user-centered digital copyright regime, fighting court battles,<sup>2</sup> organizing protests, and lobbying for legislation.<sup>3</sup> Movement actors include organizations such as the Electronic Frontier Foundation (EFF), Downhillbattle.org, and the Free Software Foundation (FSF), as well as individuals such as legal scholar Lawrence Lessig, hacker Jon Johansen,<sup>4</sup> and Free Software guru, Richard Stallman (Postigo, 2006). The movement and its actors are held together by overlapping directorates and ideological structures. For instance, law professor Lawrence Lessig serves on the advisory boards of many organizations advocating digital rights such as the EFF, the Free

Software Foundation, the Berkman Center, and OurMedia.org, while also heading his own Creative Commons initiative. Legal scholar Pamela Samuelson holds an advisor position on the EFF board as well as Public Knowledge, a social movement organization, and ChillingEffects.com, an organization that tracks the effects on innovation by “Cease and Desist” letters issued against technology developers. Hackers also play an important role in the social movement and are loosely connected to more formal groups. By designing circumvention technologies with potential fair use applications, hackers often lend important tools of resistance to the movement, and formal actors in the movement often acknowledge that contribution. Hacker Jon Johansen, for example, is not officially associated with any social movement organization, yet received an award from the EFF for his work on an important hack to technological protection measures on DVDs (Postigo, 2006).<sup>5</sup>

In sum, the digital rights movement is a composite of organizations, leaders, and other actors that together resist current interpretations of fair use and the limits of user access. Their consistent vision of expanded user/consumer privileges binds these actors together. Their tactics are typical of most social movements, using institutional settings like the courts and the legislature and extra-institutional tactics like protests. Unlike other social movements, hacking, designing alternative technologies, and circumvention of TPMs play an important role as extra-institutional tactics (Postigo, 2006).

For the digital rights movement, legal cases against the manufacture of technological innovations and potentially legitimate circumvention technologies have served to galvanize and shape collective action and capture ideologically important frames for furthering the movement’s agenda. This article presents the case of Dmitry Sklyarov’s arrest for designing a circumvention

technology called the e-Book Processor (known as AEPBR). The AEPBR circumvented the encryption protection in Adobe's e-Book technology, allowing for extended uses of e-Books beyond publishers' licensing terms. Sklyarov's case was the first criminal prosecution under the DMCA. The case illustrates how digital rights movement activists and organizations discursively framed the meaning of Sklyarov's arrest and prosecution using movement-specific digital networks such as hacker web sites, online forums, and social movement organization websites. These same networks were used to organize mobilization and share information among activists and served as outlets for movement frames to broader publics. This case also illustrates how Adobe and the U.S. Department of Justice (DoJ) responded to movement interpretations of Sklyarov's arrest through their own counter-framing strategies. Ultimately, this article understands Dymitry Sklyarov's case as eliciting "backfire", where prosecuting Sklyarov resulted in outcomes that were negative for Adobe and the DoJ. The key facilitator for backfire in this case was the use of movement-specific online networks to deploy frames and organize mobilization. Through the use of these networks the movement was able to quickly present a unified campaign, define the central issues at stake, and mobilize its members. By the time mainstream media outlets (newspapers, radio, and television) began presenting the story in detail to broader publics, movement frames had become the most readily accessible and were carried over into the mainstream.

### **Social Movements, Backfire, and New ICTs**

Scholarship in social movements and new digital information communication technologies (ICTs) has only recently started to focus on how new ICTs can be mapped onto established

social movement theory. Recently, R. Kelly Garret noted that the disparate literature on social movements and new ICTs could be organized around McAdams', McCarthy's, and Zald's tripartite theories explaining social movement dynamics: "mobilizing structures, political opportunity structures, and framing processes" (Garrett, 2006; McAdam, McCarthy, & Zald, 1996). Under this schema, new ICTs are understood in primarily functional ways, contributing to a movement's mobilizing structures, for example, by helping in organizing and thus affecting participation levels and contentious activity. New ICTs can also allow for transnational protest and organizing activities that in turn put pressure on national political structures, changing the political opportunities for movements (Garrett, 2006).

New ICTs provide novel opportunities for strategic framing within social movements. Framing has been shown to be a key process for communicating movement goals and worldviews and for providing ideological and cognitive cohesion. Frames generate metaphors and symbols that help publics conceptualize issues in an "evaluative form" and thus allow for imagining alternative modes and action (Zald, 1996). Furthermore, frames have been shown to be important for permanence and participation during mobilization (Snow, Rochford, Worden, & Benford, 1986), and social movement actors undertake strategic framing of events in movement histories, constructing "meaning, the portrayal of injustice, and the definition of pathways to change" (Zald, 1996).

The construction of frames by a social movement is seldom uncontested, and counter-frames are typically deployed by opposing sides of a given debate. In the framework of "backfire," counter-frames are deployed by those in power to devalue or de-legitimated the victims of repression and/or other actors in a movement. Because counter-frames are important

in controlling backfire, their failure to gain traction in movement constituencies and media or policy circles will have a negative consequence for their proponents. Proper framing strategies, on the side of a movement, are important for inspiring backfire among movement constituencies and beyond and they are important for movement opposition in controlling the repercussions of repression. Backfire is a specific process in social movement dynamics that describes “an action the recoils against originators...the outcome is not just worse than anticipated – it is negative, namely it’s worse than having done nothing at all” (Martin, 2007).

In the context of social movements the “action” is typically some repression or injustice perpetrated by the government or actors in positions of power on activists or other individuals associated with a movement. According to Martin (2007), because backfire can result in negative outcomes for those carrying out repression, these actors typically engage in strategies that attempt to inhibit the outrage that inspires backfire. These strategies include cover-ups, devaluation strategies that de-legitimize those being repressed, reinterpretations of the repressive events, use of official channels, and intimidation and bribery. To undermine these inhibition strategies, groups vested in eliciting backfire will inspire outrage by exposing cover-ups, validating the targets of repression, interpreting events as unjust, discrediting official channels, and resisting intimidation (Martin, 2007).

The role of communication is important in backfire because it can help in exposing cover-ups, validating targets, and discrediting officials. For these reasons, social movements have invested in strategies that bring about media coverage to frame repressive events in ways that inspire outrage (Ryan, 1991). Strategic framing that captures media attention (in a favorable way) and elicits backfire is not a given. The events under question must be newsworthy, be

ideationally framed,<sup>6</sup> and strategically constructed to have a dramaturgical quality (McAdam, 1996).

Because the media is not a reliable outlet for frames, mainly because mass media tend to echo the messages of official channels, and movements may not effectively capture the media's attention (Gitlin, 2003), alternative means of communicating an important frame can help a movement inspire backfire, mobilizing its constituency and external publics. Garrett, summarizing the work of Castells, Myers, Scott, Street and others, noted that ICTs have been shown to be an important mechanism for social movements to distribute their frames and achieve a global audience, as well as for moving beyond the limitations on resources created by lack of access to mass media (Castells, 1996; Garrett, 2006; Myers, 1994; Scott & Street, 2000).

Lastly, Earl and Schussman have discussed the role of online networks in social movements, especially with regard to social movement theory's ability to fully describe the role of social movement organizations in online movements (Earl & Schussman, 2003). Of interests to this article is their discussion of movement entrepreneurs (MEs) and their key role in decision making. Earl and Schussman's case study of strategic voting in the 2000 U.S. Presidential elections found that online movements do not rely on social movement organizations for key decisions but rather on MEs who strike out on their own to organize e-mobilization (Earl & Schussman, 2003). As the Sklyarov case study will show, hackers and online communities do exhibit the characteristics of MEs (by being early organizers of protest and deploying frames) but do not necessarily take a central role in decision making as described in Earl's and Schussman's work. Rather, in this case they work in concert with established social movement organizations like the EFF, which as the case progressed became a central hub of information dissemination

and negotiation. A key distinction between this study and the strategic voting case is that in the latter, mobilization occurred primarily via online networks, while the Sklyarov case was one in which the movement had significant offline presence and history thus there is a mixed level of participation and tactics that take place on and offline.

Ultimately the Sklyarov case illustrates many of the points discussed above. It shows how the digital rights movement used digital networks for facilitating organization, framing, and direct action (backfire against Adobe and the DoJ) and thus illustrates how movements can use new ICTs such as online networks in the manner described by Garrett et al. Moreover, it shows how being able to frame an issue quickly and coherently through online networks results in a readily accessible set of frames that can make a transition from movement-specific communication networks to mass media.

### **Note on Method**

The goal for this article is to show first, that movement-specific networks, using online outlets, responded quickly to Sklyarov's arrest by defining the frames of the case, organizing activists, and eliciting backfire. To that end, a number of specific online websites and forums where hackers and activists initially communicated information about Sklyarov's arrest were analyzed. The sites included: the usenet group "comp.text.pdf", planetpdf.com, EFF.org, slashdot.org, cryptome.org, and freesklyarov.org, . The sites were selected because they were the first to begin discussion about Sklyarov and ways of helping him, and they are also important hacker and developer sites. The sites were reviewed for how witnesses to Sklyarov's arrest and supporters initially talked about the crack of the e-Book encryption and Sklyarov's subsequent

arrest, how movement websites framed the issue, and how these framings proved consistent and sustained throughout Sklyarov's incarceration, release under an agreement to testify, and his employer's ultimate trial. The analytical approach taken to examine movement websites and communication outlets focused on identifying repetition and elaboration of themes within the discourses surrounding Sklyarov. The three most prominent were: fair use, free speech, and freedom to innovate technology. All are discussed further in subsequent sections.

Adobe's and the DoJ's counter-frames are developed through analysis of press releases, statements to the press, positions on their websites, and comments from their supporters, such as the America Publishers Association. It is worth noting that there is a dearth of these documents and statements, suggesting that a) Adobe and the DoJ failed to aggressively pursue counter-framing strategies early on in the case and b) that the counter-frames they did produce did not catch on in the mainstream media. Counter-frames from the DoJ and Adobe consisted of constructing Sklyarov as a nefarious hacker and the EAPBR as a technology meant to facilitate piracy.

In the course of this analysis, this article documents the mobilization that occurred as the case developed. This is done by citing media coverage of protests and other activities to illustrate the level of backfire that Adobe and the DoJ experienced. The same media coverage is used to illustrate Adobe's and the DoJ's limited attempt at counter-framing the case and inhibiting backfire. Lastly, to show that mainstream media outlets adopted the movement frames as the case developed, a survey of newsprint publications was taken (found through a search on ProQuest and Lexis-Nexis Academic using "Sklyarov," "Adobe" and "ElcomSoft" as keywords), as well as a survey of transcripts from television and radio reports on the case (using

Lexis-Nexis Academic search). The search resulted in 128 relevant newsprint publications and 13 relevant broadcast media reports. Reports were then analyzed to see if they used movement-specific frames or counter-frames to describe the issues at stake in the Sklyarov case. Since social movement activists and Sklyarov's supporters were the first to report on the case, the movement frames defined in this article were drawn from review of their discussions and publications. The counter-frames from Adobe and the DoJ were drawn primarily from court documents and press releases from each organization. These frames were then used to gauge the nature of mainstream media coverage.

The majority of news reports mentioned that Sklyarov was charged with potential copyright infringement and that he was the first to be tried under the DMCA. Early on in the case most reports were mainly of a brief nature, giving the public only basic facts of the case. However, the research found that as the case progressed and news outlets began to report the story in depth, most coverage used the social movement frames extensively while only seldom/tangentially using counter-frames from Adobe and the DoJ. In fact, the majority of newspaper, radio, and television outlets reviewed for this study almost always quoted a movement activist and his or her take on the case, allowing him or her to discuss fair use, free speech, and the freedom to innovate technology, and only seldom did one elaborate on the perspectives of Adobe and the DoJ. The survey, for example, resulted in 163 coded statements that referenced movement frames and DoJ/Adobe counter-frames; of those, 126 statements referenced movement-frames and only 37 referenced counter-frames. Of the 126 statements referencing movement frames, over 35% discussed fair use, often citing activist/movement perspectives, 30% referenced free speech, and the rest referenced innovation and other issues,

such as Adobe's awkward position at criticizing the DoJ for arresting Sklyarov. Of the 37 coded statements that referenced DoJ/Adobe frames, almost one third explained how the AEBPR would allow piracy. Interestingly, of all the articles reviewed in the survey, many used the term "hacker" but its meaning shifted over the course of media coverage of the case, a point discussed in later sections. Ultimately, the DoJ and Adobe failed to aggressively pursue counter-framing strategies early on and thus, as the case progressed, the most prominent frames were those generated by the digital rights movement. The most significant attempt at strategic reframing of the issue on the part of Adobe was its call for Sklyarov's release after backfire, in the form of protests and recriminations, became unavoidable. This strategy itself backfired and the media and some movement activists portrayed Adobe as foolishly having to eat its words.

As the case is reviewed below, it is important to keep in mind that mainstream media's adoption of these frames was tangential to mobilization and backfire. Activists mobilized protests before mainstream media adopted their frames and as such we see the usefulness of each of these parallel information networks. The intra-movement network of online communication (web sites such as slashdot.org, the EFF, freesklyarov, etc.) served to frame the issue for the movement, bringing about rapid mobilization. The speed of frame development and its deployment may have determined why mass media outlets adopted their frames. They were in essence the frames that were most readily available. As noted previously, backfire inhibition strategies were limited and did not find fertile ground in mainstream media coverage. In fact, the data shows that after Adobe critiqued the DoJ for Sklyarov's arrest, the DoJ generally refused to comment on Sklyarov's incarceration and trial and so its counter-framing strategies were greatly limited or ill-advised.

### **Movement Frames: Dmitry Sklyarov, the e-Book Processor, and e-Book Encryption**

In January 2001, Adobe Systems Inc., authors of the ubiquitous “PDF” internet document format, released the Adobe Acrobat e-Book Reader as a free download to internet users. Adobe released its product in conjunction with the online book distributor *BarnesandNoble.com*, which made available a series of e-Books that could be purchased and accessed using Adobe’s application. Adobe’s e-Book Reader advertised a “true to print” look for works rendered through its interface and included a built-in browser that would allow users to purchase content from distributors such as *BarnesandNoble.com*.

Adobe’s e-Book Reader also came bundled with a type of TPM known as a digital rights management (DRM) system. DRM systems for e-Books vary depending on the reader (Microsoft Reader being another popular electronic book reader). However, regardless of the manufacturer, e-Book DRM works more or less in the same fashion: *the DRM system ties the e-Book to the reader application and the computer that originally loaded it*. The flexibility of the e-Book DRM technology is determined by the publisher. For example, Adobe’s e-Book Reader allowed publishers to set permissions for whether e-Books could be shared,<sup>7</sup> whether they could be printed and to what extent, whether one could make copies or gift the e-Book, and whether a user could utilize the reader’s “Read Aloud Function” for the visually impaired.

Within five months of the e-Book Reader’s release, the Russian software company, ElcomSoft, began selling the Advanced e-Book Processor or AEPBR. On June 22, 2001, the company announced:

Advanced e-Book Processor lets users make backup copies of e-Books that are protected with passwords, security plug-ins, various DRM (Digital Rights

Management) schemes...enabling them to be readable with any PDF viewer...In addition, the program makes it easy to decrypt e-Books and load them onto Palm Pilots and other small, portable devices. This gives users - especially users who read on airplanes or in hotels - a more convenient option than using larger note-Books with limited battery power to read their e-Books... With Advanced e-Book Processor, these PDF files can be decrypted, opened, and used without any of these restrictions. (Katalov, 2001).

Framed as a tool that could help legal owners of e-Books have more freedom with their media, ElcomSoft challenged the technological restrictions on the use of e-Books. ElcomSoft's AEBPR undid the DRM system on Adobe's e-Book and prompted *BarnesandNoble.com* to suspend sale of e-Books until Adobe made changes to its encryption so that AEBPR would not work. As Adobe became more adamant on its charges towards ElcomSoft, the Russian company also framed the technology and their activities as a response to a discovered security flaw in Adobe's e-Book encryption – a flaw they claimed they had notified Adobe about as part of a “white hat” service.<sup>8</sup>

For its part, Adobe framed the technology as a circumvention tool that would allow rampant copying and file sharing of e-Books over online networks. In its cease and desist letter to ElcomSoft on June 25, just three days after the release of the AEBPR, Adobe charged that the Russian company was guilty of contributory copyright infringement, claiming that the only outcome of using its circumvention would be piracy (Adobe, 2001b). Furthermore, Adobe contacted ElcomSoft's internet service provider, Verio Inc., and requested that the company's site be taken down. Adobe also contacted RegNow, ElcomSoft's fee collecting agency in the U.S., and demanded that they cease collecting fees for the sale of the AEBPR. On its website, Adobe posted a “Frequently Asked Questions Section,” attempting to discredit ElcomSoft's claim that it had developed a tool for helping users, and that in the process it had notified Adobe

of the security flaws in its e-Book encryption. Adobe insisted that the AEBPR was a piracy tool and that ElcomSoft had never contacted it in good faith to inform it of the security concerns with the e-Book (Adobe, 2001a).

What followed over the next 30 days (June 28 to July 17, 2001) were a series of public statements on hacker bulletin boards and user forums by ElcomSoft as it attempted to frame the issues for its constituencies: users of e-Books and the PDF format. Alexander Katalov of ElcomSoft accused Adobe of designing a weak protection system for e-Books and threatened to release the source code for AEBPR on the internet under the protection of the free software movement's GNU, General Public License (GNU-GPL). In a post to their web site and to the hacker newsgroup *comp.text.pdf*, Katalov angrily noted:

Now it's time for the brutal truth on Adobe e-Book protection. We claim that ANY e-Book protection, based on Acrobat PDF format (as Adobe e-Book Reader is), is ABSOLUTELY insecure just due to the nature of this format and encryption system developed by Adobe. The general rule is: if one can open particular PDF file or e-Book on his computer (does not matter with what kind of permissions/restrictions), he can remove that protection (by converting that file into "plain," unprotected PDF. Not very much experience needed ("United States v. Dmitry Sklyarov: Affidavit of Complaint," 2001).

[On whether Adobe's legal campaign will work] I should say that it will not work. We'll just move our site to another ISP, in another country (where there is no Digital Millennium Copyright Act (DMCA)). And/or make our software available for free, under the GNU license (planetebook.com, 2001a).

Thus the framing of the AEBPR as either a tool for piracy or one geared towards enabling user rights, as either an illegal crack or the product of good research on encryption, began before Sklyarov's arrest. But it was Sklyarov's arrest that elicited swift mobilization and outrage on the part of activists.

As the recriminations between Adobe and ElcomSoft continued, Adobe contacted the FBI and asked that it investigate ElcomSoft for possible criminal copyright infringement under the anti-circumvention provisions in the DMCA. Adobe informed the FBI that Dmitry Sklyarov, who had helped develop AEBPR for ElcomSoft, would be in the U.S. for the hacker conference *DefCon 9* in Las Vegas, Nevada, on July 15, 2001, setting the stage for Sklyarov's arrest during the most popular and well attended hacker conference in the world.<sup>9</sup> Highly visible, due to the press coverage leading up to his presentation at the conference and surrounded by tech-savvy friends and supporters, Sklyarov was arrested by U.S. federal agents on July 16, 2001 as he was leaving the Alexis Hotel in Las Vegas. It took less than six hours for his arrest to be reported by internet outlets associated with hacker groups and technology experts.

Sklyarov's arrest was immediately perceived by those directly involved as repressive. A recounting of the event by an eyewitness to Sklyarov's arrest painted a picture of an innocent man being overwhelmed by agents of the state:

From July 11th to 16th together with colleague Dmitri Sklyarov, who was presenting a report, I attended the Defcon 9 conference in Las Vegas. On the morning of July 16th Dmitri and I left the hotel with the intention of going to the airport. We still had half an hour before the flight was supposed to leave when right at the front entrance to the hotel we were approached by two young men, yelling "Hands on the wall, FBI!"...The men, in a very rough manner, repeated, "Hands on the wall!!" A little bit later Dmitri was brought in wearing handcuffs. Dmitri asked to re-cuff his hands in front of his body as it was uncomfortable for him to sit down. The request was denied. The initiator of the judicial process was Adobe Software. The FBI men refused to give any further details saying that they were only following orders...On my way to the airport I was trailed, very obviously actually. As soon as I tried to make a phone call in the airport a policeman ran up to a neighboring phone and pretended to call. He never did call anybody. (Katalov, 2001)

This early account of the arrest was posted on the hacker website slashdot.org and it framed the event as unjust. The image that the account brings forth is one where a programmer is

surprised, bullied, and arrested by the DoJ. This account tapped digital networks that were outside of mainstream media but that were a central and important source of information for programmer groups that would be deeply invested in the events. Using online networks, those directly involved brought the arrest, happening in relative isolation (a hotel lobby in Las Vegas), to the attention of hackers and activists in the digital rights movement. The key to this transition was the rapid framing of the events as repressive – a message that spread quickly over the online communication networks immediately available to those vested in the events.

Following Sklyarov's arrest, accounts of the event surfaced on planetebook.com, a technology site frequented by hackers and developers interested in the pdf. file format, followed by slashdot.org, the best known hacker forum on the internet.<sup>10</sup> On slashdot.org and throughout the hacker community, support of Sklyarov was strong. For example, out of almost 400 comments posted on slashdot.org the day following his arrest, almost all were supportive of Sklyarov (Postigo, 2006). Many were critical of the DMCA's effect on free speech and technological innovation and they were critical of Adobe's tactics. Below are some examples of calls for reprisals:

In its short life we have seen many security consultants and even college and university professors threatened with prosecution under DMCA for exposing weaknesses in computer security ... activity which would otherwise be protected under the First Amendment and the traditions of academic freedom (Anonymous, 2001).

I have had entirely enough of this new adversarial stance of theirs. Let me just delete /opt/Acrobat4... Their UNIX software sucks anyway. The rest of it isn't much better. **Any software company that enforces or relies upon the DMCA should go on our blacklist** (Anonymous, 2001)!

I am writing to express my disappointment that Adobe would have a person arrested for pointing out flaws in one of its products. As a customer who cut my chops on Illustrator 1.1, it saddens me to think that Adobe now cares so little

about the quality of its...products that it seeks to harass...those who point out their weaknesses. Some will call it 'hacking' since it involved disabling a security routine, but I see it for what it is - pointing out a flaw in a product. Any company that would have someone arrested for protecting me can no longer enjoy my business (Negro, 2001).

The last of these quotes points to one of the most troubling consequences for Adobe resulting from Sklyarov's arrest. Due to the attention given to Adobe's e-Book as a result of the release of the AEBPR, security experts and hackers generally rejected it as a secure technology for copyright protection. The critique of the technology, in fact, was quite scathing. One hacker, quoted on the popular e-Book technology site *e-Bookweb.org*, wrote, "How totally absurd PDF security really is. It is so weak and so lame that no self-respecting hacker or cracker would even bother breaking it. It simply isn't worthy of one's efforts" (Sperberg, 2001). As Adobe's role in Sklyarov's arrest became apparent, hacker groups became increasingly convinced that Adobe was attempting to cover up poor encryption design.

The next group to take up Sklyarov's case and its interpretation were networks of activists closely tied to or composed of the hacker community. For example, the EFF, along with online community activists linked through the *freesklyarov.org* site and mailing list, articulated that Sklyarov's arrest under the provisions in the DMCA should be understood. In a letter to Attorney General Ashcroft, the EFF noted that the case was one in which free speech, fair use, and the freedom to innovate technology were being put at risk. The EFF stated:

Now as law, it [the DMCA] is used as a powerful sword to squelch speech and competition and kill fair use. Congress never intended for the DMCA to destroy fair use, in fact it expressly tried to protect it. As Attorney General, we ask that you honor this intent and your obligation to uphold the Constitution by dropping the charges against Dmitry Sklyarov and allowing him to return home to his wife and two small children (Steele, 2001).

Activists and the EFF were also part of a group of movement actors who quickly organized collective action to protest the arrest. By the end of the day on July 17, 2001, just over 24 hours after his arrest, the EFF released statements on Sklyarov's behalf and began his legal defense campaign. Furthermore, the EFF directed members to a website called *freedmitry.org*, where interested parties could contribute to a defense fund and get information on Sklyarov's condition by signing up for the free-Sklyarov email list. Furthermore, other websites appeared on the internet protesting Adobe's role in Sklyarov's arrest. One such site, *boycottadobe.com*, organized a campaign to boycott Adobe products. The early framing of the event by hackers, activists, and organizations like the EFF led to rapid mobilization which, three days after Sklyarov's arrest, had coalesced into planned protests at Adobe's headquarters in California, as well as protests at other offices across the United States and Europe.

With the DoJ refusing to elaborate on its position and noting only that Sklyarov had been arrested for violating the anti-circumvention provisions of the DMCA, Adobe did not have much of a chance to craft significant counter-frames that would inhibit the mounting backfire. Adobe was unable to control the backlash against it stemming from Sklyarov's arrest primarily because it could not refute or reframe the events leading up to and including the arrest. The events were so meticulously chronicled on the internet and their accounts so quickly disseminated, that Adobe found itself trying to play catch-up as the movement portrayed Sklyarov as a poor unsuspecting graduate student ambushed while visiting Las Vegas as his wife and child waited for his safe return back in Russia. Furthermore, the speed with which the network of activists coalesced speaks to the coordinating ability of the internet and to the poor

planning on Adobe's part. While Adobe struggled to control public relations, the movement printed pamphlets and anti-Adobe T-shirts (see fig.1).

(Figure 1 Here)

**Figure 1. Pamphlet of Dmitry Sklyarov and his wife and children distributed by the EFF, freedmitry.org, and freesklyarov.org. T-shirt of a protester outside Adobe Head Quarters in San Jose, CA. July 23, 2001.**

For Adobe it was a difficult position to be in. As noted earlier, at the time of his arrest Sklyarov was surrounded by tech-savvy friends and colleagues. He was detained shortly after *the most popular hacker conference in the world*; his immediate social circle was in position to take up opposition almost instantaneously using a medium that would strike close to home against Adobe. Sklyarov's arrest struck at a key value in the hacker community: the free sharing of information. Although Adobe had enjoyed the support of the internet hacker/technologist community for some time, it now faced rebuke and boycott on an international scale with protests organized around the globe just five days after Sklyarov's arrest.

Sensing that the framing battle was lost and facing protests (organized by the EFF, freedmitry.org, freesklyarov.org, and the Coalition to Free Dmitry), Adobe withdrew support for the DoJ's handling of the AEBPR case.

Adobe tried to distance itself from Sklyarov's arrest in an attempt to recapture some of the public relations ground it had lost at the hands of activists who had painted Adobe as a bullying

corporation. Adobe's reversal of position was sudden. As late as the morning of July 23, 2001, Adobe stated its position on its website as follows:

Adobe fully supports the U.S. Government's decision to investigate the potential violation of U.S. copyright laws by ElcomSoft and has cooperated with their investigations. Adobe's goal is to help protect the copyrighted works of authors, artists, developers and publishers, and to stop the sale of this cracking software in the U.S. (planetebook.com, 2001b).

Less than four hours later, after negotiations with the EFF and with protesters outside its doors, Adobe, in a joint statement with the EFF, turned its back on the government stating that "We strongly support the DMCA and the enforcement of copyright protection of digital content...However, the prosecution of this individual [Sklyarov] in this particular case is not conducive to the best interests of any of the parties involved or the industry" (planetebook.com, 2001b).

For its part, the DoJ continued its silence on the case, refusing to comment on it except to say that even though Adobe had withdrawn its support of Sklyarov's arrest it would go forward with criminal prosecution. Even though Adobe and the DoJ eventually diverged in their approach to the Sklyarov case, activists saw little difference between the actions of the two. Often Adobe's actions (getting the DoJ to arrest Sklyarov) and the DoJ's response in pursuing his prosecution were referenced together, and Adobe carried the blame for Sklyarov's predicament. After Adobe withdrew its support for Sklyarov's criminal prosecution, activists used that to further frame their case that Sklyarov's arrest was a miscarriage of justice. If anything, some news publication portrayed Adobe as having been put in a position to contradict itself and the government was seen as utterly misguided and as an instrument of corporate control (Millar, 2001; Streitfeld, 2001).

## Discussion

### Movement Frames in Context

By the time Sklyarov had his day in court a number of important frames were present on both sides of the case. For its part, the digital rights movement framed the issue primarily as a case against the legitimacy of the DMCA and exemplary of how the law could be used to damper fair use, free speech, and technological innovation. These frames were initiated within movement and activist online networks but in time made their way to news reports on the case by mass media outlets. A number of rhetorical strategies were used by the movement to frame Sklyarov's arrest along these lines.

In terms of fair use, Sklyarov's company, activists, and the EFF all noted that e-Book encryption prevented users from carrying out legally permissible uses of purchased media. For example, the EFF and others noted that AEBPR allowed for the visually impaired to read an e-Book aloud or that it gave users flexibility in terms of which reading platform to use (a laptop or PDA, for example). Legal scholars and lawyers for the EFF, weighing in for Sklyarov, noted that because AEBPR allowed users to exercise their fair use privileges, it was clear that it had other legitimate purposes and thus was not a technology that should be outlawed under the DMCA. As for mass media, it is apparent in the articles surveyed for this study that as the case developed, newsprint and broadcast reports consistently noted that fair use was one of the issues at stake.<sup>11</sup>

Movement organizations and activists also referenced a number of themes to couch the case as a threat to free speech. For example, they rhetorically framed the AEBPR as "research"

and the presentation of Sklyarov's work at DefCon 9 as a presentation on cryptography and weak encryption systems. Even prior to Sklyarov's arrest, ElcomSoft, Sklyarov's employer, had been couching their work as contributing to beneficial encryption research by pointing out flaws in Adobe's e-Book. Following Sklyarov's arrest, the rhetoric became more pronounced as hackers and other technologists on sites such as planetpdf.com and slashdot.org argued that Adobe was attempting to suppress information that was critical of its weak encryption system. Sklyarov's lawyers and the EFF made similar arguments, suggesting that the DMCA could potentially silence important research on trusted systems if the DoJ succeeded in prosecuting Sklyarov. It is also worth noting that concurrent developments in the Ed Felten/SDMI case<sup>12</sup> had already prepped the broader activist community to the potential threats to free speech posed by the DMCA and thus the activist community was ready to talk about the case as a free speech issue. Yet because the Sklyarov case was the first criminal prosecution under the DMCA, it took on a much more pressing feel. Researchers, said activists, could now go to jail for speaking about their work. Importantly, popular media outlets adopted the language of the movement as it pertained to the free speech frame. In fact, this frame seemed to resonate most. Media reports surveyed for this article often quoted activists articulating their belief that free speech was at risk while reporting that the DoJ had refused to comment on the case. In some instances (primarily among press reports from outside the U.S.), news media stopped referring to DefCon as a "Hacker Conference" and began to refer to it as a "technology conference" or an encryption research conference.

Lastly, the movement framed the Sklyarov case as one that could result in chilling effects for technological innovation. Many hackers noted that Sklyarov was being prosecuted for doing

his job or doing what many programmers working for technology firms would do if, for example, they needed to reverse engineer a technology or create plug-ins for an application. The EFF also framed the AEBPR as an innovative technology that had positive legal uses and argued that the DMCA was potentially making innovation impossible.

The frames deployed in the Sklyarov case were rooted in a number of ideological commitments that have been prevalent among the communities that took up activism against Adobe and the DoJ. For example, for hackers, many of the frames were rooted in hacker culture, specially in what Stephen Levy calls the “Hacker Ethic” where the practice of sharing information held a strong sway over communities of programmers (Levy, 1984). Importantly, the hacker ethic’s mores of sharing information found confluence with law and found a rhetorical synergy in the ideas of fair use, free speech, and innovation.

For broader publics, the fair use, free speech, and innovation frames are rooted in master frames in society; thus, by linking the issues at hand with broader societal values, the movement attempted to articulate the case in a way that those outside the movement could understand. For its part, mass media carried those interpretations faithfully by showcasing editorials written by activists, quoting activists in reports, and at times describing the DMCA as “controversial.”

All of the arguments presented by activists in the discourse of the case found their way into the legal proceedings; for example, ElcomSoft’s lawyer attempted to have the charges dismissed on constitutional grounds (the motion was denied). Importantly, showing whether these frames affected the outcome of the case (ElcomSoft was acquitted) is not the point; rather, the aim is to show the manner in which the frames made their way through internal movement networks (thus giving them cognitive cohesion and inspiring backfire) and how those frames, by

being readily available, made it out to broader publics – how they entered the broader conversation of media consumption in the digital age.

### **Counter-Frames: Adobe and the Department of Justice**

On the other hand, Adobe's and the DoJ's frames were starkly different from the movement's. The original complaint from Adobe framed the AEBPR as a pirating technology whose only real purpose would be to allow for rampant e-Book sharing online. The DoJ and Adobe attempted to frame the outcomes of releasing the AEBPR to the public as allowing for "pirates" to rampantly copy and distribute e-Books online. This frame was rooted in rhetoric used since the formulation of the DMCA and the deliberations for regulation of the National Information Infrastructure (NII, the precursor term for what became the internet and the world wide web) (Postigo, 2006). These deliberations constructed users as willing pirates in a free-for-all of content grab that was envisioned by policy makers as they crafted the DMCA.

Framing of the Sklyarov case also involved portraying him as a hacker (in the pejorative sense). The meaning of hacker has a strong impact among mass media audiences because a hacker is often reported as a criminal who broke into a secure computer network or website to steal private information or valuable data. Yet, how hacker culture defines the term and how mass media has defined it are markedly different. For hackers, the term is usually benign, and they make distinctions between white hat hackers (seen as tinkerers and security experts) and black hat hackers (those that have criminal intent). Often in hacker culture black hat hackers are also called "crackers" to make the distinction more absolute. To counter these interpretations, activists deployed a picture of Sklyarov with his family and portrayed him as a shy family man

and computer science student, not some nefarious hacker. Mass media adopted the term hacker and it appeared in many news reports; however, as the case progressed and the term came to be juxtaposed with the favorable tropes of fair use and free speech its negative connotations appeared at odds or not part of the meaning of the reports and thus it lost its rhetorical force. These frames were for the most part deployed via official channels, such as press releases from the DoJ and in court documents, but also through some media outlets. For example, the American Publishers Association was very supportive of Sklyarov's arrest, noting that the arguments about Sklyarov being a researcher were spurious and that hacking for the sake of research did not excuse the action's illegality (Kirby, 2001). The dynamics of framing and counter-framing in this case are in line with what "backfire" predicts as it was discussed in the introductory section of this article. It is important to keep in mind that backfire is more than a framing contest. It describes actions on the part of the movement and broader publics as a result of the process of 1) repression and 2) its framing. Backfire relies in part on the framing contests that give the struggle a "dramaturgical" quality, inspiring outrage.

An important development in the case was Adobe's refusal to continue to support the DoJ's prosecution of Sklyarov. This was a result of the backfire (protests) that the framing of Sklyarov's arrest had produced and can be counted as a victory for the movement. But it also added to the dramaturgical quality of the case because movement and media outlets reported on it by noting that Adobe had backtracked and that the DoJ was left to clean up a public relations mess.

## Conclusion

The Sklyarov case remains important for the digital rights movement because it helped hackers, the EFF, and other activist networks (such as BoycottAdobe.com, FreeSklyarov.org, and FreeDmitry.org) frame the issue as one of unjust repression and it elicited backfire against the federal government and Adobe. The case helped the movement solidify its frames and position them as issues of fair use and freedom of speech, tapping into ideological commitments within hacker/activist communities and generating outrage and backfire. It is important to note the distinction between backfire and framing struggles. Success in framing struggles can lead to backfire (in this case, protests and negative publicity that ultimately forced Adobe to retreat from its original position). The success of the framing struggle in the Sklyarov case was due to the speed at which movement-specific networks responded by first articulating their frames and then acting on them. As a theoretical device for understanding the dynamics of this social movement, backfire in Sklyarov's case works to show the importance of rapid frame mobilization in winning framing contests. This is relevant both for framing issues within a social movement but also for publics outside of it. One can certainly imagine that other movements with digitally connected constituencies can, in instances of repression, use digital networks to rapidly develop frames, ahead of counter-framing strategies. This can allow for quick cohesion of a movement, inspiring outrage and leading to backfire. Also, by quickly developing interpretive frames of repressive events, movements can lead mass media's understanding of a given case.

In sum, by using digital networks, the movement was able to quickly inspire outrage among constituencies and discredit Adobe's and the U.S. Government's claims that the AEBPR was a "hack" with nefarious intentions designed by criminals. The counter framing strategies

applied to Sklyarov and ElcomSoft largely did not work, and the discourse in online outlets and news media outlets largely mirrored the movement's language on the issue. This article posits that this was a direct result of the speed with which the movement used digital networks to propose its interpretation of events and the fact that those using the networks were vested in hacker values. Because digital networks meticulously chronicled the events, the mainstream media tended to follow their lead. The movement enjoyed the positive glow of championing free speech and fair use in digital media. In August of 2001, a *Washington Post* editorial noted:

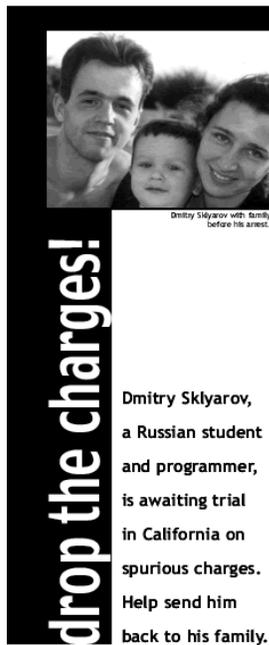
[Sklyarov's arrest] is...one of the most oppressive uses of the law [DMCA] to date -- one that shows the need to revisit the rules Congress created to prevent the theft of intellectual property using electronic media... Programs to break copy protection schemes can be used to facilitate fair use, as well as infringing uses of copyrighted material. Simply banning the dissemination of such programs, without reference to the purpose of the dissemination, inhibits the use of intellectual property far more broadly than does the copyright law itself" (Editorial, 2001).

The Sklyarov case propelled activists into action, helping the movement articulate how the DMCA and TPMs were affecting fair use, free speech, and innovation. The media attention and the opportunity to challenge the U.S. Government and Adobe gave the movement a tangible issue and a sympathetic figure with whom those previously outside the movement's orbit could identify. The movement itself ably used digital networks to deploy sympathetic images of Sklyarov with his family and children, showing him not as some evil "hacker" being rightly prosecuted but as an educated, family oriented, shy looking young man who exercised academic freedom by presenting his findings on e-Book security and was arrested for it.

The consequences of the case for the movement and for copyright policy in digital works continue to be debated. As more technologies with legitimate uses run afoul of copyright law, the movement gains favorable exposure and grows in its ability to speak to a sense of injustice in

the way copyright is now being understood. Since the Sklyarov case, legislators have been debating the feasibility of the anti-circumvention provisions and their fairness to users. Various amendments to the statute have been considered (such as Digital Media Consumers' Rights Act and the BALANCE Act) and technologists continue to deride TPMs as unworkable means of enforcing law and contract,<sup>13</sup> yet there have been no substantive changes to the law. The digital rights movement continues to fight in the courts and other institutional settings, but as Congress and copyright owners remain unresponsive it appears that extra-institutional tactics may take center stage. Hacking of DRM systems is on the rise<sup>14</sup> and hackers are taking center stage in the movement's activities.

## Figures



**Figure 1. Pamphlet of Dmitry Sklyarov and his wife and children distributed by the EFF, freedmitry.org, and freesklyarov.org. T-shirt of a protester outside Adobe Head Quarters in San Jose, CA. July 23, 2001.**

## References

Adobe. (2001a). *Adobe FAQ: ElcomSoft Legal Background*. Retrieved November 2008, from <http://www.adobe.com/aboutadobe/pressroom/pressreleases/200108/elcomsoftqa.html>

Adobe. (2001b). *Cease and Desist: INFRINGING MATERIAL OR ACTIVITY FOUND*.

Retrieved November 2008, from

[http://groups.google.com/group/comp.text.pdf/browse\\_thread/thread/37e0e8b28f55a217/7d418fa5f2047f29?lnk=gst&q=elcomsoft#7d418fa5f2047f29](http://groups.google.com/group/comp.text.pdf/browse_thread/thread/37e0e8b28f55a217/7d418fa5f2047f29?lnk=gst&q=elcomsoft#7d418fa5f2047f29)

Anonymous. (2001). *Fallout From Def Con: Ebook Hacker Arrested by FBI*. Retrieved June, 2005, from

[http://yro.slashdot.org/comments.pl?sid=13272&threshold=1&mode=nested&commentso  
rt=0&op=Change](http://yro.slashdot.org/comments.pl?sid=13272&threshold=1&mode=nested&commentso rt=0&op=Change)

Benkler, Y. (1999). Free as the Common Air to Use: First Amendment Constraints of the Enclosure of the Public Domain. *New York University Law Review*, 74(354).

Boyle, J. (1997). *A Politics of Intellectual Property: Environmentalism for the Net?*, from <Http://www.law.duke.edu/boylesite/intprop.htm>

Castells, M. (1996). *The rise of the network society*, . Cambridge: Blackwell Publishers.

Earl, J., & Schussman, A. (2003). The New Site of Activism: Online Organizations, Movement Entrepreneurs, and the Changing Location of Social Movement Decision Making. *Social Movements, Conflicts and Change*, 24, 155-187.

Editorial. (2001, August 21). Jailed Under a Bad Law. *The Washington Post*.

- Garrett, R. K. (2006). Protest in an Information Society: A review of literature on social movements and ICTs. *Information, Communication & Society*, 9(2), 202-224.
- Gitlin, T. (2003). *The whole world is watching : mass media in the making & unmaking of the New Left*. Berkeley, CA: University of California Press.
- Katalov, V. (2001). *Advanced Acrobat eBooks are NOT Really Secure*. Retrieved June, 2005, from <http://www.planetpdf.com/mainpage.asp?webpageid=2393>
- Kirby, C. (2001, August 6). Martyr or criminal? Debate over electronic copyright law rages as Russian programmers sits in a San Jose jail. *San Francisco Chronicle*, p. 1.
- Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.
- Lessig, L. (2001a). *The future of ideas : the fate of the commons in a connected world* (1st ed.). New York: Random House.
- Lessig, L. (2001b, July 30). Jail Time in the Digital Age. *The New York Times*.
- Lessig, L. (2004). *Free culture : how big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press.
- Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. New York, NY: Penguin Books.
- Litman, J. (1994). *Comments Submitted for the Public Hearing of the National Information Infrastructure Task Force Working Group on Intellectual Property*: United States Department of Commerce; U.S. Patent and Trademark Office.
- Litman, J. (2001). *Digital copyright : protecting intellectual property on the Internet*. Amherst, N.Y.: Prometheus Books.
- Martin, B. (2007). *Justice ignited : the dynamics of backfire*. Lanham [Md.]: Rowman & Littlefield Pub.

McAdam, D. (1996). The Framing Function of Movement Tactics: Strategic Dramaturgy in the American Civil Rights Movement. In D. McAdam, J. D. McCarthy & M. N. Zald (Eds.), *Comparative perspectives on social movements : political opportunities, mobilizing structures, and cultural framings* (pp. 338-255). Cambridge [England] ; New York: Cambridge University Press.

McAdam, D., McCarthy, J. D., & Zald, M. N. (1996). *Comparative perspectives on social movements : political opportunities, mobilizing structures, and cultural framings*. Cambridge [England] ; New York: Cambridge University Press.

Postigo, H. (2006). The digital rights movement: The role of technology in subverting digital copyright. Unpublished Dissertation, Rensselaer Polytechnic Institute, Troy.

Millar, S. (2001, July 28). Hackers plan to hit back as FBI detains Russian: Copyright crackdown provokes worldwide protests. *The Guardian*, p. 14.

Myers, D. (1994). Communication Technology and Social Movements: Contributions of Computer Networks to Activism. *Social Science Computer Review*, 12(2), 250-260.

Negro, D. (2001). *Fallout From Def Con: Ebook Hacker Arrested by FBI*. Retrieved June, 2005, from <http://yro.slashdot.org/comments.pl?sid=13272&threshold=1&mode=nested&commentsort=0&op=Change>

planetebook.com. (2001a). *Adobe Acrobat eBook Reader updated after security issue Adobe Systems threatens legal action for alleged copyright infringement*. Retrieved June, 2005, from <http://www.planetebook.com/mainpage.asp?webpageid=157>

planetebook.com. (2001b). *Adobe and Electronic Frontier Foundation Want Dmitry Sklyarov Released*. Retrieved June, 2005, from

<http://www.planetebook.com/mainpage.asp?webpageid=191>

Raymond, E. (Ed.). (2001). *The Cathedral & the Bazaar : Musings on Linux and Open Source by an Accidental Revolutionary*: O'Reilly Media, Inc.

Ryan, C. (1991). *Prime time activism : media strategies for grassroots organizing* (1st ed.). Boston, MA: South End Press.

Samuelson, P. (1999). Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised. *Berkeley Technology Law Journal*, 14(519).

Scott, A., & Street, J. (2000). The use of popular culture and new media in parties and social movements. *Information, Communication & Society*, 3(2), 215-240.

Snow, D. N., Rochford, E. B., Worden, S. K., & Benford, R. D. (1986). Frame Alignment Processes, Micromobilization, and Movement Participation. *American Sociological Review*, 51(August), 464-481.

Sperberg, R. (2001). *The Adobe Security Imbroglia: Roger Sperberg Looks at Russian Software that Decrypts Purchased Adobe eBook Files: Part 2*. Retrieved June, 2005, from <http://www.ebookweb.org/opinion/roger.sperberg.20010715.aebpr.htm>

Stallman, R. (2002). *Free Software Free Society: Selected Essays of Richard Stallman*. Boston: GNU Press.

Steele, S. (2001). *EFF Letter From Executive Director Shari Steele*

to Attorney General John Ashcroft (July 20, 2001). Retrieved June, 2005, from

[http://www.eff.org/IP/DMCA/US\\_v\\_Elcomsoft/20010720\\_eff\\_ashcroft\\_letter.html](http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010720_eff_ashcroft_letter.html)

Streitfeld, D. (2001, August 23). E-Book Case Negotiations Continuing. *Los Angeles Times*, p. C.3.

United States v. Dmitry Sklyarov: Affidavit of Complaint (United States District Court, Northern District of California 2001).

Zald, M. N. (1996). Culture, Ideology and Strategic Framing. In D. McAdam, J. D. McCarthy & M. N. Zald (Eds.), *Comparative Perspectives on Social Movements* (pp. 261-274). Cambridge, UK: Cambridge University Press.

---

<sup>1</sup> Here it is important to note that the term “hacker” is not being used in the fashion popularized by the mass media which has equated hackers with those who break into computer systems or design malicious computer viruses. These are more properly referred to as “crackers” or “phreaks.” Hackers, in my use of the term, is consistent with the meaning ascribed to the terms by those early authors describing hacker culture such as Stephen Levy, Richard Stallman, Eric Raymond (Levy, 1984; Raymond, 2001; Stallman, 2002). In their case hacker are more like technology tinkerer than anything else.

<sup>2</sup> For example the Electronic Frontier Foundation (EFF) and other social movement organizations took important organizing roles in *U.S. v. ElcomSoft*, *Universal v. Corley*, and *DVD-CCA v. Brunner*.

<sup>3</sup> For example the Digital Media Consumers’ Rights Act and the BALANCE Act.

<sup>4</sup> Johansen is the hacker credited with helping develop DeCSS, the hack to the content scrambling system (CSS) on DVDs, as well as spearheading a hacking campaign against Apple’s iTunes TPM.

<sup>5</sup> The EFF awarded Johansen its Pioneer Award in 2002 for his work on the crack for the DVD protection mechanism, CSS.

<sup>6</sup> An ideational frame is one that resonates with broader meanings in society, such as “free speech” or “equality.”

---

<sup>7</sup> This feature works so long as the computers are networked and the e-Book reader on one computer can check on the originating computer so that multiple instances of the book are not opened. However, most publishers will not allow for this sharing. The Microsoft Reader does not have this feature and allows you to only read the book on two authorized machines.

<sup>8</sup> “White Hat” hackers are hackers that routinely check for security flaws in encryption, firewall, and network systems and openly report those flaws to law enforcement and business as a public service.

<sup>9</sup> The FBI concluded that Dmitry Sklyarov, “willfully and for financial gain imported...a technology... primarily designed...for the purpose of circumvention a technological measure that effectively controls access to a work protected under” the DMCA ("United States v. Dmitry Sklyarov:Affidavit of Complaint," 2001).

<sup>10</sup> Within the next 48 hours, the news of Sklyarov’s arrest would be reported by not only hundreds of internet sites but also by conventional media outlets such as The New York Times, Pravda, Reuters, ZDNet, MSNBC, CNN, CNET, Wired, and others.

<sup>11</sup> Please see methods section for the breakdown of coded statements.

<sup>12</sup> Edward Felten is a Princeton computer science professor who entered the Secure Digital Media Initiative (SDMI, a consortium of media and technology firms) Challenge to remove watermarking technology from CDs. His research group was threatened with criminal liability by the SDMI and he subsequently sued the SDMI, asking the court for declaratory judgment on the legality of SDMI’s claim. The Felten case was four months in the making at the time of Sklyarov’s arrest.

<sup>13</sup> Recently Steve Jobs of Apple noted:

“...what benefits do they [music companies] get from selling the remaining small percentage of their music encumbered with a DRM system? There appear to be none. If anything, the technical expertise and overhead required in creating, operating and updating a DRM system has limited the number of participants selling DRM protected music. If such requirements were removed, the music industry might experience an influx of new companies willing to invest in innovative new stores and players. This can only be seen as a positive by the music companies.”

---

<sup>14</sup> As noted earlier, Apple's DRM had hacks explicitly designed by hackers to allow fair use of legally purchased music (Postigo, 2006).