Designed to 'Effectively Frustrate': Copyright, Technology, and the Agency of Users

Tarleton Gillespie
Dept. of Communication, Cornell University

appears in *New Media & Society*, v8n4, 2006, pp. 651-669.

Abstract
Recently, the major U.S. music and movie companies have pursued a dramatic renovation in their approach to copyright enforcement. This shift, from the 'code' of law to the 'code' of software, looks to technologies themselves to regulate or make unavailable those uses of content traditionally handled through law. Critics worry about the 'compliance' rules built into such systems: design mandates for manufacturers indicating what users can and cannot do under particular conditions. But these are accompanied by a second set of limitations: 'robustness' rules. Robustness rules obligate manufacturers to build devices such that they prevent tinkering -- not only must the technology regulate its users, it must be inscrutable to them. I examine this aspect of technical copyright regulation, looking particularly at the CSS encryption system for DVDs and the recent 'broadcast flag' proposed for digital television. In the name of preventing piracy, these arrangements threaten to undermine users' sense of agency with their own technologies.

Key words
broadcast flag • copyright • CSS • DRM • law • robustness • technology • open source • users

INTRODUCTION

The fundamental challenge of enforcing copyright law, at the base of all of the recent digital copyright controversies, is how to control how someone uses something that is freely handed to them. Commercial content owners wish to constrain what people do with their work -- play but not copy, transport but not distribute -- but they also wish to publish it, make it widely available, and typically secure some cash in return. How do you hand someone a valuable resource, then prevent them from fully exploiting it?

Until recently, copyright law and the mechanisms of enforcement were the primary means for imposing such regulations: legal prohibitions on copying and distribution, the threat of a lawsuit, fines for those found guilty in court.[1] Over the last three decades, and particularly with the emergence of the Internet, many commercial content owners are seeking to deploy technology as their first line of defense (Cohen 1998, 2003; Lessig 1999, 2001, and 2004; Samuelson 2003). By encrypting digital works, and designing machines and software applications so as to honor that encryption and prevent misuse, they hope to shift the leading edge of enforcement out of the courtroom and into the workings of the iPod, the DVD player, the e-book reader, the television, and the computer.

This 'digital rights management' [DRM] strategy, if it works, offers benefits over enforcement through law: DRM would regulate every single user automatically and without the bureaucracy of enforcement and adjudication; it would anticipate and preempt infringement before it has done financial damage; it would be much more precise, selective, and specified than legal measures; and perhaps most importantly, as a technique it would extend well beyond copyright regulation, potentially governing every aspect of the sale and use of digital culture -- not only what you can or cannot do, but how and when you pay for it.

However, establishing and enforcing technical copyright protection is no small task. The complexity only begins with the technical challenges. Constructing technology to regulate human activity, such that it limits all users in a fair and effective way, is never simply a technical matter. It is a heterogeneous effort in which the material artifacts, the institutions that support them, the laws that give them teeth, and the political and cultural mechanisms that give them legitimacy, must all be carefully aligned into a loosely regimented but highly cohesive, hybrid network (Gillespie 2004 and forthcoming).

This is not only regulating users of content through technological barriers, but regulating those who can elude those technical barriers. DRM must outpace the hackers who challenge it, not only through constant technical improvement and laws prohibiting its circumvention, but also by enlisting manufacturers to make circumvention more difficult. If the technology can be impervious to the hackers, its inner workings rendered invisible, the copyright rules implemented within can be perfectly enforced and never circumvented.

Whether this is even possible, the implications of this strategy -- for copyright, for innovation, and for users' experience with their technology -- are significant. The technology is not only being designed to limit use, but to frustrate the agency of its users. It represents an effort to keep users outside of the technology, to urge them to be docile consumers who "use as directed," rather than adopting a more active, inquisitive posture towards their tools. In other words, welding a car's hood shut makes a difference not only for what users can and cannot do, but for how users understands themselves as 'users' -- whether having agency with that technology is even possible, even conceivable.

In this essay, I would like to pursue this element of the DRM strategy, the requirement that devices be tamper-resistant. First I will examine the obligations on manufacturers written

into the license that governs DVD players and the proposal for similar rules for digital television. I will then explore concerns that have been raised about tamper-resistance by the open source software community. Finally, drawing on recent scholarship in the sociology of technology, I will consider the consequences of these rules for the experiential agency of users. If the technology is designed not to be opened, its internal workings built to be opaque to inquisitive and technically skilled users, how does that inscrutability position users as active or passive agents in relationship to their own tools, and what are the ramifications if this strategy is widely adopted?

EFFECTIVE FRUSTRATION

In the current technical approaches to copyright protection, it is the manufacturers and software designers who impose the rules, rules orchestrated by the content owners. If the content is encrypted, the manufacturer must provide users with a key; to get the key, they must sign a license; it is this license that imposes the design mandates that produce technologies that constrain the user. Designers are obligated by these licenses to build devices such that they limit the user's interaction with the protected work: allow or prohibit copying, restrict whether the user can transmit the file to another device, etc. The technology then is the perfect chaperone, only permitting users to behave appropriately.

In the case of film and digital television, these rules are designed and these licenses are overseen by a coalition of the major U.S. movie studios and consumer electronics companies, each of whom consent to this arrangement. Independent manufacturers, even if they might not pursue a DRM strategy on their own accord, are compelled to agree to the terms of the license -- to refuse would practically close them out of the market entirely, as without the proper decryption keys they would be unable to even play the mainstream content their customers are likely to want.

Most of the criticism of technical copyright protection has centered on how the design of digital devices regulates use: Are DRM constraints in the best interests of the public? Do they foreclose the kind of fair uses copyright law is designed to allow? Do they extend control of content beyond what copyright law intended? Do they undermine consumers' privacy? But these 'compliance' rules are only part of the rules necessary for this elaborate system to work. Every time a particular encryption system is deployed, even with compliance rules firmly in place, a single hacker may disable it, and quickly alert others as to how it's done -- or worse, provide a circumvention tool that even the technically inept could use. This is no small setback. By the time a DRM encryption system enters the market, it has already been extensively researched, imposed on millions of files, built into millions of devices. Having to upgrade or replace it would be costly and daunting.

The major U.S. film and music industries have sought to win -- or better yet, avoid -- this digital arms race, first, by supporting laws like the Digital Millennium Copyright Act [DMCA], which prohibits not only the circumvention of encryption systems but also the provision of information or tools that help others do so. The problem with a legal approach, however, is that the damage cannot be undone -- a hacking tool, once posted, cannot be effectively erased from the Web, no matter how swift the injunction or harsh the punishment. While a court victory has symbolic value, and may deter casual users from posting the offending app and thus making it somewhat harder to find, it by no means solves the problem. This is the scenario Hollywood faced in Universal v. Reimerdes, when a Norwegian teenager discovered the secret to the CSS

encryption, designed 'DeCSS' and shared it far and wide over the Internet, rendering the encryption that protected DVDs vulnerable to circumvention.

The initial appeal of DRM as a mechanism for copyright is that it can conceivably preempt infringement instead of responding to it post hoc. Content owners want a way to preempt circumvention as well. Therefore, they have pursued a second strategy: thwart hackers with unbreakable encryption and impenetrable devices. This is embodied in a second set of rules for how to design digital media hardware and software: 'robustness' rules. These require manufacturers to make their technologies harder to circumvent, more resistant to hacking and tampering, and more unwilling to give up the secrets of how they work. Manufacturers find themselves contractually obligated to join the effort of beating hackers at their own game -- and, perhaps more importantly, to be liable for the cost if (or when) they fail.

DVD

The Content Scramble System [CSS] that protects DVDs combines compliance and robustness rules in this way. CSS encryption was developed by the Copy Protection Technical Working Group [CPTWG], an inter-industry coalition that includes the major U.S. movie studios and key players in the business of consumer electronics. It is currently imposed on all major Hollywood films released on DVD; only devices that include the correct decryption keys will be able to even play the films locked onto those discs. The distribution of these keys includes a license agreement administered by the DVD Copy Control Association [DVD-CCA] (an organization established by the same the major studios and the largest of the consumer electronics companies, solely to administer encryption licenses).

Amidst the compliance rules required by this license are restrictions designed to frustrate hackers and tinkerers. Whether it be software or hardware, the manufacturer of a DVD player must be 'reasonably certain' that the device is

> clearly designed in a manner that would effectively frustrate each of the following: (1) attempts to defeat the copy protection functions... (2) attempts to discover decrypted confidential DVD Keys embodied therein; (3) attempts to discover Highly Confidential Information in the form of CSS Security Algorithms. (DVD-CCA, 6.2.5.1)

The license goes on to specify how this 'effective frustration' might be achieved: encrypting the encryption process and the decryption keys themselves; 'closely coupling' the elements of the device that handle authentification and decryption with elements that handle other functions, such as playback; building in mechanisms that self-check the integrity of the system, and fail if it has been compromised.

Clearly, this makes very specific demands on design, driven not by functional efficiency, cost, user-friendliness, or engineering aesthetics, and certainly not to facilitate the user's easy comprehension of the device's inner workings. This has consequences not only for the design of DVD players, but also for their repair; the license acknowledges this, and in fact demands it: 'Licensee shall not disclose to end users any diagnostic information relating to such implementations and shall protect the confidentiality of integrated circuit specifications relating to CSS.' (DVD-CCA, 6.2.5.3)

By designing DVD players and applications to be resistant to investigation, manufacturers aim to render the workings of the CSS encryption so obscure within a deliberately complex artifact that those who might want to circumvent it will be unable to figure out how. Encryption protects the data from unauthorized technologies, the authorized technologies honor the encryption; compliance rules dictate the available functions of that technology, and the 'robust' design of the technology frustrates invaders.

Though it may seem counterintuitive, the fact that CSS has been circumvented actually supports the viability of this approach. DeCSS came not from a user violating the compliance rules, but from the failure of one manufacturer to follow the robustness rules. Jon Johansen, the designer of the offending tool, found a CSS decryption key when he discovered that RealNetworks had failed to adequately obscure the decryption process inside their XingDVD player. From one key Johansen made educated guesses on several hundred others (Patrizio, 1999). DeCSS, then, is not so much a lockpick as it is a keyring of copied keys, modeled on one accidentally left on the back porch. Had RealNetworks made its application more robust, as the license required, it is not immediately obvious whether the encryption would have been broken.

DTV

That the locus of control is in an industry license means that such arrangements are less likely to come under public scrutiny. However, precisely because it is difficult to get every manufacturer to agree to such arrangements, those pursuing DRM strategies sometimes must look to government to help impose these rules, and this is where they become most available to challenge. The Consumer Broadband and Digital Television Promotion Act [CBDTPA], known also as the Hollings Bill, was the most visible attempt to impose copy protection obligations on manufacturers of all digital media technologies; it included the requirement that such security standards be 'resistant to attack.' The bill was scuttled after outcry both from the public and from many technology manufacturers. More recently, the film industry and its closest technology partners sought the government's help in developing a DRM system for digital broadcast television.

Congress and the Federal Communications Commission [FCC] have been orchestrating a shift from analog to digital broadcast television [DTV] since the 1990s; on the current schedule, U.S. broadcasters must turn over their analog frequencies to the FCC by the end of 2006 in exchange for the digital ones they were given back in 1997 (NTIA, 1998). Hollywood has taken this as an opportunity; they have been crafting a DRM system for the new television technology to match that of DVDs and music downloads.

In 2001, the same coalition of movie studios and technology manufacturers that produced CSS formed the Broadcast Protection Discussion Group [BPDG] to consider protection schemes for DTV (BPDG, 2002). The 'broadcast flag' plan, originally developed by the Fox Corporation and then technically updated by the '5C' companies [Sony, Matsushita/Panasonic, Intel, Toshiba, and Hitachi] was brought to the group for consideration. After a contentious internal debate, the BPDG forwarded it to the FCC and, after a period of public discussion, in November of 2003 the FCC mandated that the broadcast flag be put into use. The order would have established conditions for the design of all televisions, tuners, and computer applications capable of receiving and displaying DTV broadcast signals (FCC, 2003). However, a federal court later ruled that the FCC had overstepped its jurisdiction. (ALA v. FCC, 2005) The broadcast flag is

currently on hold, although there have been hints that Congress could pass a measure giving the FCC the authority it would need to reinstate the plan.

The broadcast flag plan depended first and foremost on a set of compliance rules for manufacturers, to produce technologies that regulate users and thus manage the reproduction and distribution of digital television content. A watermark would accompany a digital broadcast at the behest of its owner, indicating that it should be protected. DTV devices would be required to check for the watermark and encrypt flagged content with one of a set of approved DRM encryption systems.[2] According to the licenses accompanying each particular encryption technology, the device would limit copying of the encrypted work, and prevent 'indiscriminate redistribution' of that work over the Internet (FCC, 2003).

Along with these compliance rules, the FCC's mandate made an oblique reference to robustness requirements similar to those in the CSS license, leaving the details of their implementation vague: 'The content protection requirements set forth in the Demodulator Compliance Requirements shall be implemented in a reasonable method so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment.' (FCC, 2003: 43) The 'reasonable' tone belies the prickly controversy that preceded it. Several of the points of contention in the BPDG debates and in comments that followed during the FCC discussion period concerned the scope of these requirements.

The central issue was how robust DTV devices needed to be, i.e. who or what they must be designed to frustrate. Must a digital television tuner be able to withstand a skilled hacker trying to crack the system, or just an average user trying to avoid the restrictions? Is this aspiring to be a leak-proof container or just 'curb-high deterrence' (NRC: 218) against casual infringement? The Motion Picture Association of America [MPAA] and 5C companies argued for a higher standard, defined in terms of frustrating, as critics worried, 'even the most knowledgeable professional technicians' (BPDG 2002: 14), or in terms of the tools that might be used, i.e. professional grade software as well as the household screwdriver. IT companies and consumer advocate groups argued for a lower standard, requiring manufacturers only to frustrate ordinary users from getting around the technical barriers they would erect (BPDG, 2002: 14-15) -- a less costly and technically demanding standard. The FCC mandate adopted the slightly modified 'ordinary user using generally-available tools or equipment' standard, though they also made sure to emphasize that this standard was only a minimum, one that 'represents a floor that manufacturers are free to exceed.' (FCC, 2003: 23)

THE OPEN SOURCE CRITIQUE

The disputes around the broadcast flag mandate are important ones. For manufacturers, whether the standard of robustness is the ordinary user with generally available tools, or the expert user with professional resources, sets the terms for how much they have to do to produce an 'effectively frustrating' artifact, and how liable they could be if they fail. For consumers, the kind of information necessary to repair these devices would be held exclusively by a limited community of technicians, especially those employed by or closely linked to the manufacturers. They may also affect the market for these devices; critics of the broadcast flag proposal fretted that it would further privilege the entrenched consumer electronics manufacturers by authorizing a limited set of DRM systems, beginning with those designed by the 5C companies, those most closely aligned with the movie studios and the BPDG effort. Robustness rules also make design

more costly, further closing out upstart manufacturers who might otherwise offer innovative alternatives.

Perhaps those most affected by robustness rules are those overlooked by the implicit dichotomy between ordinary users and professional manufacturers: users who are skilled but not professionalized, who are capable of developing uncommon tools and able to make them easily available online. The most obvious of these is open source software designers. Not only are they overlooked in these arrangements, lumped in with the criminals and hackers the rules are written to constrain. The design principles required by 'robustness' run precisely counter to the philosophy of open source -- a philosophy that is itself a challenge to traditional design dynamics.

Open source is a catch-all term for a number of approaches and philosophies regarding the software design. Unlike most commercial software, which is typically designed within a single corporation and in which the code itself is withheld from both users and competitors as valuable corporate property, open source advocates suggest that software is better designed in loosely organized collaborative teams, where code is freely made public to any and all interested contributors. Code worked over by many interested and disparate designers, they argue, is more responsive to the needs of multiple user groups, suffers from fewer bugs, and benefits from unexpected innovations.

This approach has produced a number of successes: the Linux operating system, Apache web servers, the Mozilla Firefox web browser. Many argue that open source efforts produce better and more innovative software than does traditional commercial design, and that the non-hierarchical and non-proprietary approach is more politically progressive than that of the vertically-scaled software market (for more on open source software design, see David, 2004; Nichols and Twidale, 2003; Ratto, 2003; Raymond, 1999; Stallman, 2002; Torvalds, 2001; Weber, 2004). At the very least, it is a compelling and provocative experiment in the social choreography of design, oriented along different economic and political axes -- what Benkler has more broadly described as "commons-based peer production." (Benkler, 2003)

One of the foundational principles of open source software design is that code must be made public and available to anyone. Once code is locked away, early design directions are ratified, subsequent innovations are squelched, and overlooked bugs persist. It is this principle that is crucially at odds with the 'robustness' component of the DRM strategy, where the technology must be designed so as to frustrate investigation. Robustness also requires that those specifically authorized to know the workings of the tool must be clearly demarcated from those who are not. The open source community is generally reluctant to draw tight boundaries around those who are participants in the design process and those who are not; anyone who expresses interest may contribute, and the aggregate achievement is better for it -- which means the boundary of what is inside and outside of the technology, the design process, and the community is rendered blurry, if not non-existent.[3]

It is no surprise, then, that critics have pointed to open source as an example of why DRM systems like CSS and the broadcast flag may undermine our technological future, in that open source itself represents a challenge to the corporate 'monoculture' (Crawford, 2004) that currently dominates software design. As the Electronic Frontier Foundation [EFF] pointed out in the broadcast flag discussions,

> Although one can imagine open source software developers creating a 'compliant' demodulator or downstream application, requiring that such a demodulator or

> application be 'robust' against user modification is the problem... To the extent the open source development model embraces the freedom to modify, however, this necessarily means that open source software cannot be made 'tamper-resistant' in the fashion contemplated by the broadcast flag mandate. (EFF, 2004: 2)

Tamper resistance is antithetical to the open source design philosophy, where design is tampering, where innovation demands investigation. The robustness standard, then, functionally prohibits open source designers from ever participating in the market for digital television software. Any tool designed according to open source standards will be a violation of the FCC's regulations, and perhaps of the DMCA.

The DRM systems being imposed onto digital film and television raise significant concerns regarding the future of innovation for these technologies, and for the as-yet-imagined possibilities for distributing and using digital media. More importantly, robustness rules shape who can be an expert and who cannot. The impact of these rules on open source software design is only a sign of how this strategy, if embraced, could impact all "amateur experts." This category of users is much larger than the open source community, and certainly not exclusive to software and the Internet -- its precedents include kit car builders, early radio enthusiasts, and 'homebrew' computer hobbyists (Greenberg 2004). But on the Internet they can more easily form communities of interest and share their expertise, and, when the technology is itself digital, they can even circulate and collaborate on the tools themselves. Bruckman argues that the Internet blurs the seemingly bright-line distinction between amateurs and professionals in the art world, offering venues and distribution networks for 'semi-published artists' (Bruckman, 2002). The same may be said for all manner of creative work, including mechanical and software design. Those interested in and skilled at a particular practice can become, if not professionals in the traditional sense (i.e. marked by the trappings of career, institutions, and widely agreed-upon standards of performance), then a community of expert practitioners, ranked by reputations loosely determined by their peers.

Robustness rules that require established manufacturers to wall off the workings of their devices push apart users and designers just as these new experiments in technology production and innovation are working to blur and reconsider this dichotomy. By excluding the open source approach from any market where technology is asked to regulate in this way, the risks extend well beyond the worry that innovation in digital media technology may be limited; it risks tipping the scales in the debate about technological design itself, marginalizing an approach to technology that challenges the simple dichotomy between passive consumers and professional designers.

USER AGENCY

What is really at issue here is not just expertise and innovation, but a broader question of user agency: a software design community that encourages it, a regulatory constraint that forbids it. As the EFF noted:

> This discussion betrays a fundamental confusion regarding the difference between security -- securing a PC for its owner -- and 'tamper resistance' -- securing a PC against its owner. Open source software has been very successful at the former

> goal (in fact, products based on open source software have proven to be more secure than closed source software). The latter goal—enforcing restrictions against the wishes of a computer's owner—is much harder in an open source environment, where the owner can modify the software. (EFF, 2004: 3)

What the robustness rules require is security against the owner of the technology, something that can only now be contemplated because of encryption and the support for techno-legal regulation strategies that depend on it. To the extent that the DRM approach needs its technologies to hide their workings from their users and be fortified against committed inquiry, it is fundamentally at odds not only with open source design philosophies, but also with broader cultural presumptions about technology.

Technological design anticipates users and build in roles for them. 'Along with negotiations over who the user might be, comes a set of design (and other) activities which attempt to define and delimit the user's possible actions' (Woolgar, 1991: 61). These roles can be quite compelling, preferred subject positions that users are likely to inhabit. But beyond anticipating the user and preferring some uses over others, the robustness principle asks designers to also design against the very possibility of user agency.

What is at stake here is not only a user's ability to act with a tool and on that tool, but also the user's perception of their ability and right to do so. To frustrate people's agency is less politically problematic than to convince them they have no such agency to be frustrated. Giddens' (1984) theory of structuration and Orlikowski's (1992) extension of that theory to technology suggest that the capacity for a user to act in the world is bound both by institutional and semiotic structures -- though these structures are themselves the result of human action. Our assent to these structures is implicit in our choice to act, and we legitimate these structures in doing so. At the same time, structures can be transformed through reflective action. But within this understanding of human agency, it is worth focusing on the way the very possibility of acting is staged, made visible or invisible, encouraged or quietly rebuked.

My sense of agency with my own tools is constituted by a set of interconnected social dynamics. I am encouraged to examine, manipulate, and even redesign my car by a number of sociocultural mechanisms: books about car maintenance and detailing, courses on automotive repair, friends sharing their love of tinkering, local competitions and 'aficionado' subcultures that celebrate amateur ingenuity, third party manufacturers offering add-on components. Furthermore, there are financial incentives: not only savings on repairs, but also the possibility that my clever innovation could lead to a career in the auto industry. Property law also suggests that what is mine is therefore something I may investigate, change, break, or rebuild, so long as I do not endanger others in the process. These are all subtle reminders that I can be both user and re-maker of my car, conceiving of it both as a tool I use and an object I can re-imagine. Conversely, I may be discouraged from tinkering with my car by similar social dynamics: warranty and insurance regulations that in which protections are voided by my actions, official warnings about the physical danger of doing so, the time required to develop the necessary skills and the cost and availability of the right tools.

Alongside these legal, commercial, and social forces, I am also encouraged by the technology itself: the latch that opens the hood, the kickstand that props it up, the orientation of the engine towards my line of sight. These are opportunities to be electrocuted, of course, but they are also invitations to experience myself as having agency with the technologies that surround me: not just the agency of use, but the creative potential to trick out, to tinker, to

disassemble, to invent. I may never take advantage of these possibilities or anything innovative with my car, but I am regularly reminded that I could. And even if I don't do so with my car, I might with my computer, or my VCR, or my broken toaster.

Historians of technology have noted the importance of this give-and-take between users and their tools, both for the cultural life of these technologies and for their subsequent innovation:

> People are not merely malleable subjects who submit to the dictates of a technology; in their consumption, they are not the passive dupes suggested by crude theorists of ideology, but active, creative and expressive -- albeit socially situated -- subjects. People may reject technologies, redefine their functional purpose, customize or even invest idiosyncratic symbolic meanings in them. Indeed they may redefine a technology in a way that defies its original, designed and intended purpose... However, the appropriation of a technology cannot be entirely separated from its design and development: technologies are designed for particular purposes. (Mackay and Gillespie, 1992: 698-9)

The possibility that users can re-imagine technology in ways unexpected by the designer suggests that technologies do not develop along independent trajectories, either inherent in the thing itself or as intended by its makers.

User appropriations of technologies are not so rare or idiosyncratic as one might imagine. Kline and Pinch describe rural farmers removing the wheels of their Model Ts and connecting farm equipment to the driveshafts and axles, transforming their cars into stationary power sources. Such innovations quickly spread beyond individual farmers: magazines publicized some of the more clever solutions; third-party manufacturers developed devices that facilitated the connection between auto and farm tool; some auto manufacturers even referenced these uses in their advertising. (Kline and Pinch, 1996: 774-5) Digital-age parallels abound: open source software, freeware, and peer-to-peer networks -- one can hardly tell the story of the Internet without noting the varied and unanticipated contributions of users. User agency, in negotiation with the technology itself (what's possible) and the efforts of designers and manufacturers (what's intended), throws unexpected and often productive wrenches into the seemingly linear paths of innovation these technologies might otherwise follow.

Perhaps most importantly, user appropriation can be an important challenge to authoritative systems of power by those marginal to the centers of technological production. (Eglash, 2004) When farmers transform Model T's into stationary power generators, when hackers crack filtering software to reveal what sites they block, when researchers turn toy robot dogs into roving "sniffers" that can identify hazardous chemicals in residential areas,[4] the act of appropriation, making the technology one's own in action and in material design, can turn the tool back on the systems of power it is otherwise ideologically compatible with.

What if such user innovations are rendered impossible by the technology itself -- if the hood is welded shut? If prying it open anyway is illegal? If this strategy increasingly becomes the norm, and the next generation of users never knows there was a hood at all? If the tools available for the consumption and circulation of music, movies, e-books, and digital art are designed to robustly withstand user intervention, not only will such innovations be impossible, the extent to which we see ourselves as even having technological agency could diminish. In this sense, the 'black box' (Latour, 1987) of technology is itself being black boxed. Technologies

already designed to obscure their workings for users who want only inputs and outputs and a user-friendly interface are being further redesigned to adamantly obscure their workings (especially) against those who want to investigate them.

This strategy is a relatively new one. With traditional machinery, it is possible to prevent users from exploring a technology only by regulating their access to it; I cannot open the hood of a train because the panels are locked, because the crew is authorized to stop me, because doing so is illegal. This depends on the fact that the technology is either a public resource, or owned by an entity with the legal and financial authority to exclude me from it. Such restrictions are lent legitimacy both by the tenets of property law (I can't tamper with what isn't mine) and safety measures (I shouldn't tamper when doing so might cause bodily harm). However, when the technology is a privately-owned commodity, it has until now been nearly impossible to prevent its owner from opening it up and seeing how it works.

In Kline and Pinch's story, some car manufacturers were troubled by the farmers' innovations; their reaction, however, was to discourage them by contractually obligating dealers not to perform conversions for their customers. (Kline and Pinch, 1996: 790-1) When AT&T wanted to discourage the use of third-party peripherals such as the Hush-a-Phone mouthpiece, they turned to the FCC and the courts -- and failed. (Horwitz: 230-231) What these industry giants did not do is redesign their devices to make the user innovation impossible, presumably because they couldn't. No device could be closed that could not also be opened. Ownership implied the right to access, and the authority to grant others access. However, with digital technology and particularly encryption, the software I buy today can work for me, without ever being open to me. This offers a new level of control to the designer, and therefore to the designers' economic allies -- in this case, the movie industry: secure 'against' the technology's owner and user, 'for' content owners.

A 'RIGHT OF INQUIRY' FOR TECHNOLOGY AND CULTURE

Our experiential relationship to our technology has already shifted dramatically over the last two centuries, from one where we were primarily the makers of our own tools to one where our tools are largely mass-produced for us elsewhere, but we at least in principle retain access to their inner workings as potential tinkerers. (Smith, 1994) With the robustness rules built into DRM systems, this relationship may shift again, to one in which we are discouraged from investigating our own tools and from using them in ways other than intended and authorized. The roles designed into these technologies not only urge some uses and forbid others; they encourage a passivity towards the technology itself.

Perhaps unsurprisingly, this strategy of designing against user agency demonstrates a striking parallel to the politics of the major content industries around copyright and the use of culture. Cutting up films into a digital montage, generally protected by fair use, arguably requires a kind of cultural agency. The maker must be able to experience culture not as something to be consumed but as raw material for more production, and to experience themselves as having agency with that material. Opening up a television or digital application, reworking it to make it different and better, and passing it along to others requires a similar sense of technical agency. Both are structurally disabled by DRM systems, where technical barriers squelch both cultural and technical innovation in their effort to inhibit infringement. The fear of users tampering (whether with the content or the tool) seems to justify measures that, because it is so difficult to discern between circumvention and creative tinkering, simply prohibit both.

In the end, the impact on our experience with culture and with technology may be the same. Content owners are relegating users of culture to being mere consumers through a technological DRM architecture. To fortify that architecture against tampering requires designing for the same passivity with the technology: operators rather than agents. It is a politics of culture and technology that's arguably at odds with our commonsense and democratic notions of what individuals should be able to do with both, but neatly fits the principles of consumer culture.

A comment from the EFF is telling; before focusing their argument on concerns for innovation, they also worried that fair use would be squelched by the broadcast flag:

> Manufacturers and the public, including hobbyists and individual technologists, have a basic right of inquiry, to access any unencrypted signal and to process it as they wish. No technological restrictions on the ability to process, record, transmit, play, or otherwise handle signals should be created, promulgated, or perpetuated. (BPDG, 2002: Tab N1)

Regulatory strategies like the broadcast flag work to close down this 'basic right of inquiry,' be it cultural or technical. The 'freedom to tinker,' as Felten puts it, can be squelched by this regulatory strategy and all that it entails. And this strategy is likely to continue. Technical content protection continues to be consistently and energetically pursued by MPAA and the Record Industry Association of America [RIAA] lobbyists, their concerns have gained ground with legislators and regulators, and consumer electronics and information technology manufacturers are increasingly embracing this approach rather than resisting it. As much as DRM may help curb copyright infringement, more importantly it promises to renovate how we purchase and consume culture, in ways beneficial to its producers. For that reason alone, DRM is intensely appealing to an industry that feels it has yet to fully maximize the return on their investments.

Too often the details of these arrangements are overlooked as a part of the public debate about digital copyright. Because the broadcast flag was proposed as an FCC mandate, it enjoyed a level of scrutiny by activist organizations, but private contracts like the CSS license rarely do. To consider the impact of such ancillary arrangements that support DRM systems requires investigating the rules introduced and imposed through such contracts, blessed by a copyright law that legitimates such licenses but has little authority to scrutinize how they actually work. We might also consider whether a "basic right of inquiry" extending both to information and to technology might be an appropriate policy measure; such a right will not likely emerge inside of the kinds of 'consumer protections' recently proposed, such as the Digital Media Consumer's Rights Act languishing in the House since 2003. In fact, it may be the seductive power of the term "consumer" itself that is most problematic here. To the extent that lawmakers so often frame their role in terms of protecting the interests of 'consumers' rather than the protecting the rights of 'users' or 'citizens,' such concerns about free inquiry and creative tinkering are difficult to even conceive.

More generally, these cases afford an opportunity to investigate and deepen our understanding of the dynamics of user agency around technologies. Scholarly investigation into technology has only recently 'discovered' the user, having focused for too long on the artifact itself and its impact on society. This case suggests that users' agency is in part about a sense of having agency; this sense is shaped by cultural and institutional suggestions of whether users

have agency and under what conditions, suggestions materialized in the tools themselves and inscribed into laws and contracts that dictate how such tools are built. This points to the possibility of more carefully cataloguing the social, cultural, and technological dynamics by which agency is encouraged or inhibited -- what Karaganis and Jeremijenko call 'structures of participation' (Karaganis and Jeremijenko, forthcoming) -- and the consequences of frustrating, obscuring, or legislating away the capacity to act on one's tools, not just with them.

Finally, it speaks back to the current state of the copyright wars, which remain a vital and crucial discussion about how copyright should work, towards what ends, and how the design of technology intervenes in and shifts this cultural project. We have benefited as a culture from the balance struck by copyright law, between the rights of the owners of cultural works and the ability of the public to not only enjoy but also fruitfully build off of that work. This balance is arguably being tipped by the efforts of the major U.S. movie and music distributors, to take advantage of encryption technology that can lock up cultural work and move use towards passive consumption. DRM robustness rules should remind us that we have also benefited from a balance between different modes of technological innovation -- closed, hierarchical, corporate design as well as the messier contributions of a curious public of tinkerers -- and that this balance is similarly at risk.

Notes

1 As Lessig reminds us, it's important not to think of the law in isolation. Along with the threat and consequence of legal enforcement, the market and the existing technologies helped make purchasing a work a more viable and satisfying option that copying it; some generalized societal pressure against 'stealing' rounded out the regulatory environment. See Lessig, 1999, 2001, 2004.

2 The broadcast flag approach could not encrypt the data before delivery, as the DVD does, for two reasons. First, it would require the upgrading of all televisions capable of receiving DTV signals already sold, which might cause customer frustration the broadcasters and the FCC want to avoid. Second, since broadcast television has often been considered a public good, some argued that it had to be broadcast "in the clear" -- a curious requirement that makes a nice gesture toward the principle of publicly supported television, but one that is only symbolic if a broadcast flag mandate then requires the device to immediately encrypt the content and regulate what users can do with it.

3 This boundary between designers and users is one that is constantly managed by designers and marketers themselves and built into the logic of the artifact itself; see Woolgar (1991) for a discussion of how designers maintain this tense distinction even in moments when they are purportedly attempting the bridge that divide.

4 Natalie Jeremijenko's project can be seen at http://xdesign.ucsd.edu/feralrobots/

References

American Library Association, et al., v. FCC, et al., No. 04-1037 (D.C. Circuit) decided May 6, 2005.

Benkler, Y. (2003) 'Freedom in the Commons: Toward a Political Economy of Information', *Duke Law Journal* 52(6): 1245-93. UR: (consulted November 19, 2005): http://www.law.duke.edu/shell/cite.pl?52+Duke+L.+J.+1245

Broadcast Protection Discussion Group (2002) 'Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group', submitted June 3. URL (consulted March 6, 2005): http://www.cptwg.org/Assets/TEXT FILES/BPDG/BPDG Report.DOC

Bruckman, A. (2002) 'Studying the Amateur Artist: A Perspective on Disguising Data Collected in Human Subjects Research on the Internet.' URL (consulted March 6, 2005): http://www.nyu.edu/projects/nissenbaum/ethics_bru_full.html

Cohen, J. (1998) 'Copyright and the Jurisprudence of Self-Help', *Berkeley Technology Law Journal* 13(3): 1089-1143.

Cohen, J. (2003) 'DRM and Privacy', *Berkeley Technology Law Journal* 18(2): 575-616.

Consumer Broadband and Digital Television Protection Act, S. 2048. URL (consulted March 6, 2005): http://www.eff.org/IP/SSSCA_CBDTPA/20020321_s2048_cbdtpa_bill.pdf

Crawford, S. (2004) 'The Biology of the Broadcast Flag', *Hastings Communication and Entertainment Law Journal*, 25(2): 603-652. URL (consulted March 6, 2005): http://ssrn.com/abstract=500763

David, S. (2004) 'Opening the Sources of Accountability', *First Monday*, 9(11), URL (consulted March 6, 2005): http://www.firstmonday.org/issues/issue9_11/david/index.html

DVD Copy Control Association, 'CSS Specifications', version 1.1. URL (consulted March 6, 2005): http://www.dvdcca.org/css/

Eglash, R. (2004) "Appropriating Technology: An Introduction", in R. Eglash, J. Croissant, G. Di Chiro, and R. Fouche (eds.) *Appropriating Technology: Vernacular Science and Social Power*. Minneapolis: University of Minnesota Press.

Electronic Frontier Foundation (2004) 'Reply Comments, in the matter of: Digital Broadcast Content Protection', submitted March 15, 2004. URL (consulted March 15, 2006): http://www.eff.org/IP/Video/HDTV/EFF_FNPRM_Reply.pdf

Federal Communications Commission (2003) 'Report and Order and Further Notice of Proposed Rulemaking, in the matter of: Digital Broadcast Content Protection', FCC No. 03-273, adopted November 4, 2003. URL (consulted March 15, 2006): http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.pdf

Federal Communications Commission (2002). *In the Matter of Digital Broadcast Copy Protection*, Notice of Proposed Rulemaking, MB Docket No. 02-230, August 9. URL (consulted March 15, 2006): http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.pdf

Giddens, A. (1984) *The Constitution of Society: Outline of the Theory of Structure*. Berkeley, CA: University of California Press.

Gillespie. T. (2004) 'Copyright and Commerce: The DMCA, Trusted Systems, and the Stabilization of Distribution', *The Information Society* 20(4): 239-254.

Gillespie, T. (forthcoming, 2007) *Wired Shut: Copyright and the Re-alignment of Digital Culture*. Cambridge, MA: MIT Press.

Greenberg, J. (2004) "Hackers and Tinkerers and Amateurs... Oh My!" unpublished manuscript.

Horwitz, R. (1989) *The Irony of Regulatory Reform: The Deregulation of American Telecommunications*. Oxford: Oxford University Press.
Karaganis, J. and Jeremijenko, N. (eds.) (forthcoming) *Structures of Participation in Digital Culture*. Durham, NC: Duke University Press.
Kline, R. and Pinch, T. (1996) 'Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States', *Technology and Culture* 37(4): 763-795.
Latour, B. (1987) *Science in Action: How to Follow Scientists and Engineers through Society*. Cambridge, MA: Harvard University Press.
Lessig, L. (1999) *Code, and Other Laws of Cyberspace*. New York: Basic Books.
Lessig, L. (2001) *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House.
Lessig, L. (2004) *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: Penguin Books.
Mackay, H. and Gillespie, G. (1992) 'Extending the Social Shaping of Technology Approach: Ideology and Appropriation', *Social Studies of Science* 22(4): 685-716.
National Research Council (2000) *The Digital Dilemma: Intellectual Property in the Digital Age*. Washington D.C.: National Academy Press.
National Telecommunications and Information Administration (1998) *Charting the Digital Broadcasting Future: Final Report of the Advisory Committee on Public Interest Obligations of Digital Television Broadcasters*. Washington D.C.: U.S. Dept. of Commerce.
Nichols, D. and Twidale, M. (2003) 'The Usability of Open Source Software', *First Monday* 8(1). URL (consulted March 6, 2005): http://www.firstmonday.org/issues/issue8_1/nichols/index.html
Orlikowski, W. (1992) 'The Duality of Technology: Rethinking the Concept of Technology in Organizations', *Organization Science*, 3(3): 398-427.
Patrizio, A. (1999) 'Why the DVD Hack Was a Cinch', *Wired News*, November 2. URL (consulted March 6, 2005): http://www.wired.com/news/technology/0,1282,32263,00.html
Ratto, M. (2003) 'The Pressure of Openness: The Hybrid Work of Linux Free/Open Source Software Developers', dissertation, Department of Communication, University of California, San Diego, USA.
Raymond, E. (1999) *The Cathedral and the Bazaar*. Beijing, O'Reilly.
Samuelson, P. (2003) 'Digital Rights Management {and, or, vs.} the Law', *Communications of the ACM* 46(4): 41-45.
Smith, M. R. (1994) 'Technological Determinism in American Culture', in M. R. Smith and L. Marx (eds.) *Does Technology Drive History? The Dilemma of Technological Determinism*, pp. 1-36. Cambridge: MIT Press.
Stallman, R. (2002) 'Why Software Should Not Have Owners', in *Free Software, Free Society: Selected Essays of Richard M. Stallman*, pp. 45-50. Cambridge Mass.: Free Software Foundation.
Torvalds, L. (2001) 'What Makes Hackers Tick? a.k.a. Linus' Law', in P. Himanen (ed.) *The Hacker Ethic*, pp. xiii-xvii. New York, Random House.
Weber, S. (2004) *The Success of Open Source*. Cambridge, MA: Harvard University Press.
Woolgar, S. (1991) 'Configuring the User: The Case of Usability Trials', in J. Law (ed.) *A Sociology of Monsters: Essays on Power, Technology, and Domination*, pp. 58-97. London: Routledge.

Acknowledgments
This research was assisted by a grant from the Digital Cultural Institutions Project of the Social Science Research Council, with funds provided by the Rockefeller Foundation. The essay benefited from the suggestions made by Joe Karaganis, Geoffrey Bowker, and the participants of the 'Digital Cultural Institutions and the Future of Access: Social, Legal, and Technical Challenges' workshop at the Center for Science, Technology, and Society, Santa Clara University, October 21-23, 2004, as well as from Julie Cohen.

TARLETON GILLESPIE is an assistant professor in the Department of Communication at Cornell University, with an affiliation with the Department of Science & Technology Studies and the Program in Information Science. His book *Wired Shut: Copyright and the Shape of Digital Culture* will be published by MIT Press in early 2007.