Chapter 4

Hacktivism and State Autonomy:

The Transnational Politics of Policy Circumvention

Introduction

In the bull market of 1999, eToys stood out in the field of favored technology stocks. eToys was one of the hottest properties in online retail at that time, with a market capitalization of $8 billion in September of that year ("Toy retailing -- Trouble in toy town?" 2000). And like any big company, it wanted to protect its brand. Online, nothing is as essential to your brand as your domain name – the web address that lets people find your site (Waxer 2000; Whitman 2000).

So etoys.com was concerned that 20,000 customers a day were mistakenly visiting www.etoy.com (Ziegler). etoy – singular – was the digital home of a group of Zurich-based Internet artists. These artists had been online at etoy.com since 1995 – two years before the advent of eToys the retailer (Dugan 2000).

But that didn't stop eToys from using the usual means of protecting its corporate interests: the courts. On November 29, 1999, an LA court judge issued a judgement against the etoy artists, enjoining them from using the etoy domain or name (Smithers).

For the moment, it appeared that eToys had won. But the victory proved to be short-lived, as is apparent from eToys' share price (see Figure 13: eToys share price). No sooner had eToys won its day in court, then it confronted a new kind of challenge: the challenge of anti-corporate hacktivism.

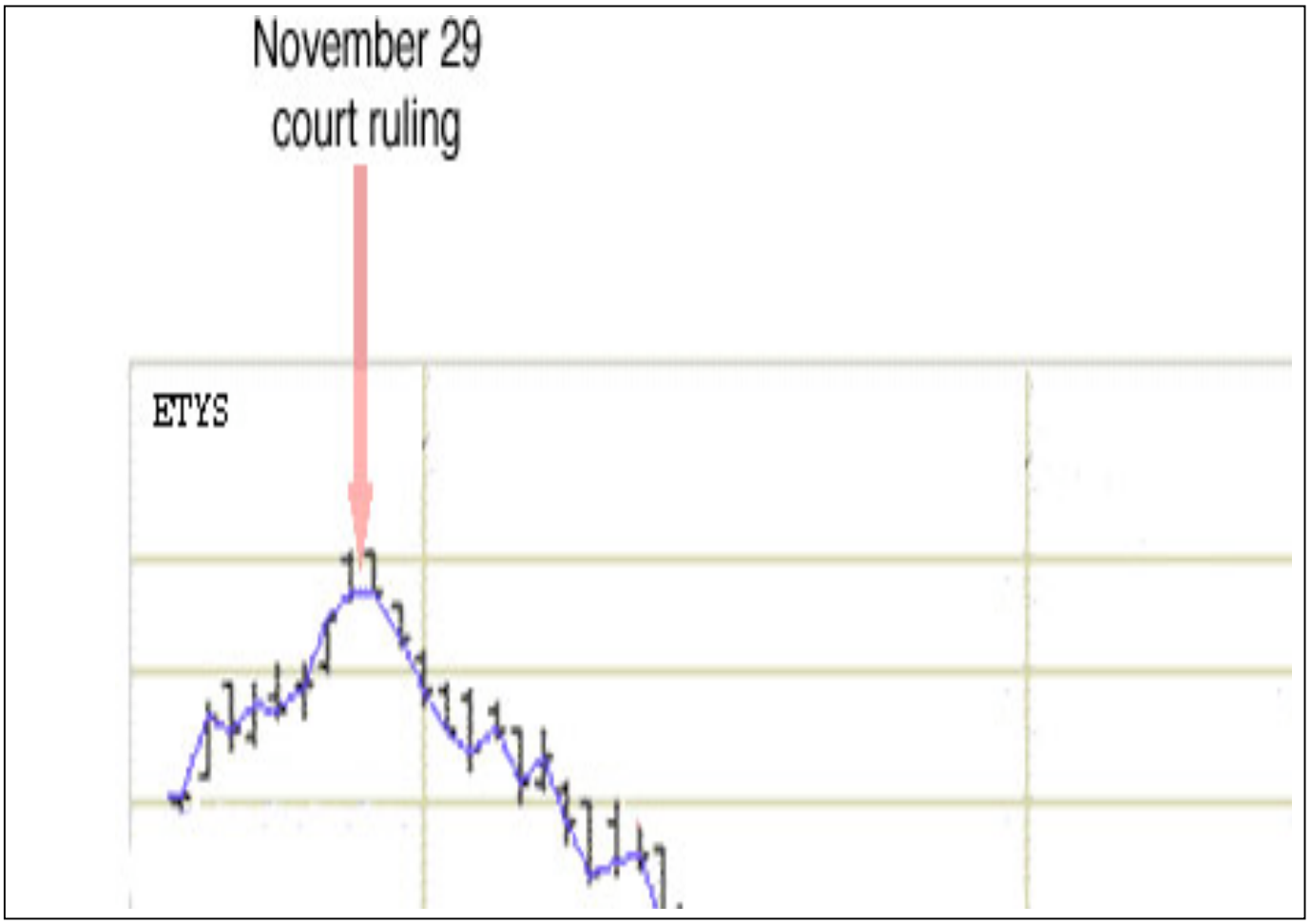

Figure 13: eToys share price
Source: (Grether 2000)

The challenge was mounted by a coalition of performative hackers and political coders, working together to create a variety of tools aimed at hobbling the eToys web site. Like the widely distributed e-mail that challenged etoy supporters to use e-mail, investor web sites, and protest sites to bring down eToys' share price (Grether 1999). Or the online "Toywar" game that inducted players into a community of anti-eToys activists by immersing them in a community of virtual etoy warriors (Kettmann 2000). Or the

little automated shopper who filled a virtual basket with Barbies and Legos, only to abandon its cart…after consuming plenty of server time (Grether 2000).

Within days, the eToys site fell prey to widespread complaints about its slow server and frustrating waits. And all this came during the Christmas shopping season – the season that was supposed to make good on the promise of eToys multi-billion market cap. While the "Toywar" campaign was not solely responsible for eToys' dwindling share price at that time (Leonard 2003), it has been cited as a contributing factor (Abreu 2000; Jones and Smith 2002; Nguyen 2002).

The hacktivist challenge showed that a court decision might *not* be the last word in a corporate dispute. But it is the *way* that this challenge was mounted that should interest scholars of policy, political participation, social movements, and transnational politics. These scholars expect political challenges to focus on efforts at policy influence. In the case of eToys, that might take the form of lobbying for a new system of domain name allocation, so that organizations like etoy would be better protected in the future.

Instead, the Toywar hacktivists pursued a strategy of policy circumvention, a political outcome that poses an as-yet-unrecognized challenge to state autonomy. Policy circumvention is here defined as legal noncompliance that:

a) is a strategic political response to a specific policy, law, regulation or court decision
b) focuses on nullifying the effect of a policy, law, regulation, or court decision, and
c) creates some non-excludable benefits (though there may be additional, excludable benefits of non-compliance).

Strategies of policy circumvention fall outside the models of transnational politics that are emerging from research into the anti-globalization, human rights and environmental movements. These models have successfully directed attention towards transnational civil society actors as a growing source of challenge to nation-states, focusing on challenges that come in the form of efforts at policy change. By focusing instead on efforts at policy circumvention, I hope to build on the transnational politics literature, demonstrating its utility in analyzing policy circumvention as well as policy change.

The promise of the transnational politics literature is clear from the moment we look at the possibility of applying its insights to the burgeoning phenomenon of hacktivism. At first glance, hacktivism would seem to share the four characteristics identified by Keck and Sikkink as typical of transnational advocacy networks: "the centrality of values or principled ideas, the belief that individuals can make a difference, the creative use of information, and the employment by nongovernmental actors of sophisticated political strategies in targeting their campaigns."(Keck and Sikkink 1998)

Hacktivism fits each of these criteria. While the values behind hacktivism vary quite markedly – political coders and crackers are often cyber-libertarians, while performative hackers have more in common with traditional leftists or anarchists – their actions and writings are usually framed in ideological or principled terms. A desire and belief in making a difference as an individual explicitly motivates many hacktivists.[34] Hacktivist activities like online parodies, virtual sit-ins, and information theft epitomize

[34] See, for example, comments from Hacktivismo members on page 189, below.

the very concept of "creative use of information." And hacktivists have demonstrated ever-greater precision and sophistication in targeting their campaigns, which may be aimed at domestic or foreign governments, or at corporations.

Yet Keck and Sikkink, along with other authors who follow them, do not envisage the full range of organizational strategies available to the networks they describe. Instead, they focus on the narrower subset of strategies focused on policy change. And in the case of hacktivism – which frequently aims not at policy change, but at policy circumvention – that means ignoring precisely those strategies and activities that may pose the greatest challenge to nation-states and their governments.

This chapter endeavors to expand the study of transnational politics by directing our attention towards the as-yet unexamined phenomenon of policy circumvention. It begins with an examination of the still-young scholarship on transnational social movements and transnational actors, in order to demonstrate that literature's focus on efforts at policy change. From there, it turns to the challenge of policy circumvention, explaining why it merits study, and positing a model for predicting its emergence and success. Next, it introduces hacktivism as a fruitful field for testing the model of policy circumvention, and tests the model against two cases. Finally, it suggests directions for further research into hacktivist policy circumvention, and into the larger phenomenon of policy circumvention as a form of political action.

Transnational politics and policy change

Any examination of the literature on transnational social movements must begin with Keck and Sikkink's *Activists Beyond Borders*, a volume that has strongly influenced subsequent research into the rise of transnational networks of activists. Keck and Sikkink's object was to show that "advocacy networks are helping to transform the practice of national sovereignty" and are "an important part of an explanation for changes in world politics."(Keck and Sikkink 1998) These networks "try not only to influence policy outcomes, but to transform the terms and nature of the debate."(Keck and Sikkink 1998)

Keck and Sikkink's notion of network influence is explicitly focused on the question of how networks affect state policy-making. While they have an expansive notion of the influence process as one in which networks "must use the power of their information, ideas, an strategies to alter the information and value contexts within which states make policies"(Keck and Sikkink 1998), policy-making remains the central object of interest. This focus reflects the usual priority of network actors themselves; as Keck and Sikkink note, activists' "definition of effectiveness often includes some policy change by 'target actors' such as governments, international financial institutions like the World Bank, or private actors like transnational corporations." (Keck and Sikkink 1998) The successful cases of network advocacy cited by Keck and Sikkink are those that have achieved some sort of measurable policy change, such as the pan-American network of human rights activists who successfully pressured Argentina's military government into ending the kidnappings and disappearances of political prisoners (Keck and Sikkink 1998).

Subsequent scholarship has followed Keck and Sikkink's lead in focusing on how transnational activist networks achieve policy change. In her analysis of the role of transnational social movements in affecting ecological conservation, Lewis (2002) defines these organizations' effectiveness in terms of "the establishment of policies and practices that improve conservation."(Lewis 2002) Schmitz analyzes the impact of transnational activism on human rights in Kenya and Uganda in terms of its "important effects of governmental foreign and domestic policy decisions."(Schmitz 1999) Dalton and Rohrschneider (1999) see transnational activism as the logical means of pursuing an environmentalist policy agenda, since spillover effects mean that "the locus of responsibility for policies designed to redress grievances shifts from the national to the international level."(Dalton and Rohrschneider 1999)

Some of the literature does endeavor to locate the policy-change agenda within a broader set of social movement effects. Sperling et al. note that the political import of social movements may lie in effects that are not conventionally recognized as politics, such as community organizing, "because it occurs outside of formal, male-dominated economic and political institutions."(Sperling, Ferree, and Risman 2001) One widely-examined issue is the impact of transnational politics on political discourse or norms; according to Khagram, Riker and Sikkink, "a significant amount of [transnational network] activity is directed at changing understandings and interpretations of actors or, in other words, the creation, institutionalization, and monitoring of norms."(Khagram, Riker, and Sikkink 2002a)

But these effects remain implicitly – and often explicitly – linked to the goal of policy change. Risse and Sikkink are interested in the moment when governments are

socialized into "talking the human rights talk" (Risse and Sikkink 1999) because they see it as one stage in a five-phase "spiral" of human rights change, culminating in a shift in government policy towards full compliance with international human rights norms. Hawkins traces this kind of process in his examination of changing human rights norms in Chile, crediting changing human rights norms with the emergence of a Chilean human rights network; the successes of this network are seen in how "the military regime altered its agenda, discourse, policies, and practices." (Hawkins 2002)

The consistent return to mechanisms of policy change stems from the broader agenda of the literature on transnational social movements: to demonstrate that transnational advocacy is posing a challenge to state autonomy. As Smith and Johnston (2002) put it, "[m]ost social movement research takes the modern nation-state as the context of contemporary political contention…..Internally, states are increasingly constrained by an expanding web of commitments to other international actors." (Smith and Johnston 2002) Tarrow (2002) critically notes, "much of the early work on 'global civil society' assumed – without a great deal of evidence – a zero-sum relationship between the growth of transnational networks of organization and the decline of state power." (Tarrow 2002) Scholars of transnational social movements are thus trying to substantiate the argument that transnational politics constrains state autonomy; demonstrating the impact of transnational advocacy on domestic (or international) policy is perhaps the clearest way of establishing this claim.

Yet to focus on policy change is to take an unnecessarily narrow view of the ways in which transnational politics impinge on state autonomy. In focusing on policy change, we assume the importance of centralized policy-making bodies, most frequently – though

not always – states. That assumption constrains the transnational politics literature's ability to establish its primary claim: the diminishing of the nation-state.

The phenomenon of hacktivism suggests that the nibbling away at the edges of state authority extends beyond pressures on policy change. The most significant pressure exerted by hacktivism is the sidelining of the state as an arena for effecting political change: rather than pursuing an agenda of policy change, hacktivists often find ways of enabling the circumvention of state policy. By modeling the challenge of policy circumvention, we can see how the phenomenon actually lends greater credence to the core argument of the transnational politics literature: the argument that transnational social movements constrain the autonomy of the state.

Transnational politics and policy circumvention

Policy circumvention is more than just evasion of the law. It is a political strategy that enables resistance to a contentious policy, law, regulation, or court decision. Its effects may ultimately include policy change, but it does not depend on policy change in order to be effective.

But distinguishing policy circumvention from simple law-breaking demands clear criteria for identifying the specifically political dimensions of this form of extra-legal behavior. Let me address each of these criteria in turn:

1. Policy circumvention is a strategic political response to a specific policy, law, regulation or court decision. This criterion captures the deliberately political nature of policy circumvention: it is a protest against a policy, law, regulation or

court decision that is seen as unjust or impractical. The political content of the circumvention is generally conveyed through explicit statements by the entrepreneurs driving the circumvention, who link their actions to a given policy or law, and offer a principled argument about why that policy or law is illegitimate. The policy circumvention is frequently accompanied by other more conventional forms of protest, including those aimed at policy change, such as media outreach, lobbying, or legal action.

2. Policy circumvention focuses on nullifying the effect of a policy, law, regulation, or court decision. Where strategies of policy change focus on combating the root problem – the unjust or impractical policy – strategies of policy circumvention focus on combating the effects of that policy by rendering it moot. Instead of voicing opposition to a given government decision, policy circumventers vote with their feet by finding ways to render a particular policy ineffective or unenforceable.
3. Policy circumvention creates some non-excludable benefits (though there may be additional, excludable benefits of non-compliance). One key distinction between policy circumvention and simple law-breaking is that the consequences go beyond the benefits to the individual participant. While policy circumvention often offers immediate and tangible private benefits, stemming from participants' relief from the law, it also creates larger effects. These effects may include increased issue awareness, declining enforceability of a given policy or law, or even policy change itself. It's important to note that these non-excludable benefits are not necessarily important to all the participants in a given circumvention. While the

entrepreneurs responsible for initiating and facilitating the circumvention may be motivated by the larger political consequences of circumvention, much of the power of the circumvention strategy lies in the fact that many people will be drawn to participate strictly for the immediate tangible benefits of evasion.

Using these criteria, we can distinguish between cases of policy circumvention (some, but not all, of which occurs in the world of hacktivism), and cases of ordinary law-breaking:

Table 10: Policy circumvention vs. law-breaking

Policy circumvention	**Law-breaking**
Hacktivismo (software to circumvent Internet censorship)	Private consumption of child pornography
DeCSS distribution tools (enabling the distribution of DVD-decoding software)	Private copying of DVDs and CDs
Underground currencies, barter systems	Tax evasion
Medical marijuana buyers' clubs	Recreational drug dealing and use
Abortion clinic blockades	Trespassing

In identifying the specifically political phenomenon of policy circumvention, and distinguishing it from ordinary law-breaking, we uncover a world of political activity that has remained outside the scrutiny of the literature on transnational social movements. Yet this activity speaks to that literature's core concerns – and particularly, its interest in establishing the impact of transnational politics on state autonomy. Examining policy circumvention thus promises to advance the transnational politics research agenda in several ways.

First, policy circumvention is a major pressure on state autonomy – perhaps an even more fundamental challenge than pressures for policy change, because it relegates the state to the sidelines. Policy circumvention shunts the state to the status of a side-show whose cooperation is non-essential to obtaining desired political outcomes.

Recognizing and understanding policy circumvention should be part of the agenda for mapping both the challenges to the nation-state, and the consequences of those challenges.

Second, policy circumvention is itself an additional pressure for policy change – making it a crucial missing piece of models that attempt to predict transnationally-driven policy change. Some efforts at policy circumvention act as a public demonstration in support of policy change; others help raise awareness of a key policy issue. The story of policy circumvention is thus not only an important counterweight to arguments about policy change, but must also be incorporated into the arguments and models of those authors who study the role of transnational movements in precipitating domestic policy change.

Third, policy circumvention changes norms about policy compliance, including the norms that govern the relations between states. The transnational social movements literature has widely argued that changing international norms act as the mechanism for translating transnational advocacy into domestic political change. (Hawkins 2002; Keck and Sikkink 1998; Khagram, Riker, and Sikkink 2002b) As we will see from the hacktivist cases below, policy circumvention is an effective pressure on both individual and state norms of behavior. Widespread policy circumvention changes ideas about which laws are legitimate, about the necessity of legal compliance, and about the use of noncompliance as a political tool. These effects can be seen most powerfully in the case of states who themselves adopt policy circumvention as a new tool of international relations.

If the transnational politics literature has something to learn from the study of policy circumvention, it also has much to offer to the project. Building upon the literature on new social movements, the transnational politics literature has underscored the importance of several core concepts for modeling contentious politics: repertoires of contention, mobilizing structures, and political opportunity structures.

Repertoires of contention and cultural framings

The notion of "repertoires of contention" was coined by Charles Tilly, who defined a repertoire as "the whole set of means [a group] has for making claims of different kinds on different individuals or groups." (Tarrow 1994) The related notion of cultural framings is analogous to a set of "discursive repertoires [that] provide contenders with a vocabulary of motives that can be used to legitimate their actions."(Traugott 1995) Keck and Sikkink applied the notion of evolving repertoires to their examination of the transnational slavery campaign, in order to comprehend how "technological and institutional change can alter the 'moral universe' in which action takes place, by changing how people think about responsibility and guilt, and by supplying them with new ways to act." (Keck and Sikkink 1998)

The preoccupation with how repertoires evolve and diffuse suggests the utility of the concept for considering policy circumvention. Since policy circumvention represents an expansion in the repertoire of transnational contention, at least as recognized by scholars of transnational politics, thinking of circumvention in terms of repertoires of contention allows us to usefully frame the phenomenon.

Resource mobilization and mobilizing structures

Resource mobilization theory, led by the work of McCarthy and Zald, has drawn attention to the ways in which mobilizing structures enable or constrain social movement organizing. By looking at mobilizing structures, we are able to examine "how movement organizations are affected by the availability of resources the effectiveness of organizational structures, and the constraints and opportunities provided by their larger environment." (Halcli 1999)

These structures have proven equally significant to the activities of transnational social movement organizations. In her examination of the role of NGOs in addressing violence against women, Joachim emphasizes the importance of "the mobilizing structure which these civil society actors have at their disposal, including the presence of organizational entrepreneurs, an international constituency, and experts."(Joachim 2002) Legler's investigation of transnational opposition to the Free Trade Area of the Americas found that limited mobilizing structures, particularly due to financial disparities among civil society participants, imposed significant constraints on the Hemispheric Social Alliance (Legler 2000).

The transnational politics literature has taken particular note of one emergent mobilizing structure: the Internet. Scholars have moved from seeing the Internet "as a form of communication, one that facilitated the rapid diffusion of information about contentious episodes among chains of movement actors" to "regarding the Internet itself as a form of organization itself." (Tarrow 2002) This has been borne out by specific case studies, such as Smith and Smythe's work on the defeat of the Multilateral Agreement on Investment (MAI); the authors found that "Internet technology contributed to the capacity

of groups to communicate, to quickly mobilize and widely disseminate critical information, outside the control of national elites."(Smith and Smythe 2001) Similarly, Pickerill's study of British environmental movements found that information technology "enables groups to co-ordinate campaigns without the need for a central office, newsletters, or the physical presence of activists" (Pickerill 2001).

The mobilizing structures literature encourages us not only to attend to the technologies of mobilization, but also to organizational resources, such as elite leadership, or movement entrepreneurs. These entrepreneurs prove crucial in understanding the transnational dynamics of policy circumvention.

Political opportunity structures

The notion of political opportunity structures allows us to capture the degree to which a political system is open or vulnerable to political change. McAdam, McCarthy and Zald describe political opportunity structures as encompassing four dimensions:

1. The relative openness or closure of the institutionalized political system
2. The stability of that broad set of elite alignments that typically undergird a polity
3. The presence of elite allies
4. The state's capacity and propensity for repression (McAdam, McCarthy, and Zald 1996)

Recent scholarship suggests that these dimensions can be translated to the transnational level. "Social movement theorists…speak of 'multilayered' opportunity structure, including a 'supranational' layer or a 'multilevel polity,' or they highlight how international pressures influence domestic opportunity structures."(Khagram, Riker, and Sikkink 2002a) As Reimann establishes in the case of Japanese environmental NGOs,

these transnational opportunity structures can sometimes provide a way of escaping from a domestic opportunity structure "highly unfavorable to advocacy NGOs."(Reimann 2002) Transnational pressures can also have dramatic effects on the domestic political opportunity structure, for example by strengthening or limiting the state's capacity for repression. (Maney 2002)

Together, the notions of repertoires of contention, resource mobilization, and political opportunity structures help us conceptualize the phenomenon of policy circumvention. First, we can frame policy circumvention as an extension of the repertoire of contention, beyond the conventionally recognized tactics of policy change. As I will show toward the end of this chapter, this extension represents an innovation in our capacity to recognize policy circumvention, as much it does the popularization of this form of contentious politics.

Next, we can use these notions to help predict the emergence and success of political action that meets the three criteria by which we recognize policy circumvention. Resource mobilization theory helps us understand the emergence of political strategy, such as a strategy of political circumvention. In particular we see that entrepreneurs, organizational capacity, and financial resources are key resources for mobilization. The notion of opportunity structures helps us comprehend the potential costs and benefits of efforts to nullify policy or law. In particular we see that political institutionalization, and the state's capacity for repression, may affect the viability and costs of efforts at nullifying policy. The variables affect the costs of participation in policy circumvention for individual actors, and thus shape the strength and force of the effort at nullification. Finally, the literature on mobilizing structures helps us hypothesize the circumstances

under which law-breaking might generate some non-excludable benefits. Inverting the literature that asserts the role of movement entrepreneurs in creating excludable benefits as an incentive for movement participation, we can imagine that movement entrepreneurs might also facilitate the creation of non-excludable benefits.

Fusing the insights of social movement theory with the main criteria for recognizing policy circumvention, we can thus posit three variables for predicting the emergence and success of policy circumvention:

1. Political entrepreneurs are necessary for the emergence of a policy circumvention effort (though not sufficient to ensure its success). These entrepreneurs frame the circumvention as a strategic response to a particular policy, and design the circumvention in a way that creates non-excludable as well as excludable benefits of participation.
2. Policy circumventions that face a low cost of failure are more likely to succeed. Depending on the policy area, the cost of a failed circumvention may be low or high. Policy areas in which the costs of failure are high will face difficulties in mobilizing participation. Low costs of failure therefore create a more favorable mobilizing structure for policy circumvention.
3. Policy circumvention is more likely to succeed when the state faces political constraints on repression. We can assume that any state would ideally wish to repress law-breaking of all kinds, including policy circumvention. Yet some states face political constraints on their capacity for law enforcement, particularly when dealing with policy circumvention. These constraints create a political opportunity structure that is more favorable to policy circumvention.

Hacktivist policy circumvention offers fertile ground for testing this three-part model of policy circumvention. The desire to circumvent conventional political engagement, and to transcend the limitations of the policy process, is widely described by hacktivists themselves. Furthermore, hacktivism encompasses a range of efforts at policy circumvention, and thus allows us to examine variation in the variables that account for success or failure.

This chapter will focus on two contrasting instances of hacktivist policy circumvention. The first, successful, example of policy circumvention is the case of DeCSS distribution; the distribution of banned code that allows the decoding and viewing of DVDs on Linux machines. (Remember that success here is defined not by the usual standard of policy change, but by the demonstrated incapacity of the state to enforce a given law or policy.) The second, less successful, example of policy circumvention is the case of Hacktivismo, a project designed to evade Internet censorship in China and other non-democratic regimes. Significantly, while Hacktivismo has had only limited success in defeating the effectiveness of censorship policies, there are reasons to think it may be more successful in precipitating policy change.

Policy circumvention: the case of DeCSS

In October 1999, a fifteen-year-old Norwegian named Jon Johansen got frustrated with the fact that he couldn't play his DVDs on his computer. His computer was running the Linux operating system, and the motion picture industry had yet to license software to play DVDs on a Linux machine. So he joined an online group that was working on Linux

DVD software. Ultimately, he successfully reverse engineered the DVD's encryption technology, and came up with a piece of software that would let Linux users watch DVDs. The software was dubbed "DeCSS" – a reference to the "Content Scrambling System" (CSS) encryption that the motion picture industry used to encode DVDs. That software was posted online, and quickly distributed across the Net (Harmon 2000).

But there was one little problem with Jon's program. The CSS encryption technology that Jon cracked didn't just keep DVDs from playing on Linux machines; it prevented DVDs from being copied. In order to play DVDs on his computer, Jon had been forced to crack the encryption system that had been devised as a form of copy protection. So even though Jon's intention was just to watch his own DVDs, his software had much broader implications.

These implications worried the Motion Picture Association of America, which quickly spearheaded a campaign to crack down on DVD cracks. Within a month, Johansen had heard from the MPAA's lawyers. At the MPAA's behest, Johansen was prosecuted under Norwegian law for breaking into his own DVDs ("Norwegian Teenager Jon Johansen Acquitted in DVD Case" 2003). Others who tried to distribute his code – most notably, the hacker magazine 2600 – were prosecuted under US law. While Johansen was acquitted by a Norwegian court in December 2002, an appeals court has subsequently agreed to hear an appeal of the acquittal (Gross 2003a). Meanwhile, in the 2600 case, two US courts have ruled that DeCSS code is not protected by the First Amendment; two other court cases have so far left the First Amendment question unresolved (Gross 2003a).

The motion picture industry's legal actions scarcely put an end to the DeCSS phenomenon, however. CSS descrambling code spread across the Net, distributed by a variety of tactics. Some people embedded the DeCSS code in images – using a technique known as steganography (Touretzky 2000c). Someone else embedded the code in song lyrics, and distributed the song (Touretzky 2000c). You could download a couple of animated characters who would explain the DeCSS code to you(Touretzky 2000c). Or look up a haiku that contained the descrambling algorithm (Touretzky 2000c). All of these approaches exploited the legal distinction between protected forms of speech, like artistic expression, and the unprotected status of executable code.[35]

The proliferation of DeCSS distribution mechanisms – though not DeCSS itself – represents a clear example of policy circumvention. The original DeCSS hack was not, at the time, an explicitly political act; it was a solution to the technical problem of wanting to play a DVD on a Linux machine. The fact that Johansen later became the focal point of

---

[35] For more on this distinction see (Touretzky 2000b) and (McCullagh 2001). As explained by one definition:

> Initially, a programmer writes a program in a particular programming language . This form of the program is called the *source program,* or more generically, *source code*. To execute the program, however, the programmer must translate it into machine language , the language that the computer understands. The first step of this translation process is usually performed by a utility called a compiler . The compiler translates the source code into a form called object code. Sometimes the object code is the same as machine code; sometimes it needs to be translated into machine language by a utility called an assembler.("Source Code" 1996)

The ability to exchange source code is crucial to programmer's abilities to read and improve each other's code(Touretzky 2000a), which makes it crucial to assuring the quality of computer programs, and to the growth of the open source movement (in which programmers constantly exchange and improve code). It is thus only executable code – code that is usable to the *hoi polloi* of computer users who are not themselves programmers -- that one might even consider regulating.

As many analysts have pointed out, however (Felten 2002; Touretzky 2000a) the legally useful distinction between source code and executable code does not always hold up in practice. Some scripting languages allow users to run source code without compiling it, effectively collapsing the distinction between the two; while other languages may create additional forms of code beyond source and executable.

a political and legal battle over DeCSS, and that he became an effective spokesperson for the rights of free software developers, should not lead us to retrospectively interpret his original hack in political terms. The political act that constituted policy circumvention was the outpouring of mechanisms for distributing Johansen's banned algorithm, despite the ban.

This proliferation of DeCSS distributions has successfully circumvented the US and international laws intended to enable the protection of copyrighted material such as DVDs. While some DeCSS authors have been prosecuted under the D.M.C.A. and trade secrets law,[36] the widespread availability of DeCSS code renders the Act largely ineffective in preventing the decoding or duplication of DVDs. Executable DeCSS code has been harder to distribute than the non-executable (but still theoretically usable) code distributed through steganography and other techniques, but even executable code is still available on the Internet.[37]

These distribution mechanisms were most certainly strategic, political responses to the decisions to prosecute Johansen, 2600 magazine, and others; to the American Digital Millennium Copyright Act (D.M.C.A.), which provided the legal basis for US

---

[36] DVD-CCA v. McLaughlin, Bunner et al. (and the related Pavlovich case) were prosecuted in California under trade secrets law; Universal Studios et al. v. Eric Corley was prosecuted under the D.M.C.A.. (Gross 2003b)

[37] As per the executable/source code distinction, the sites distributing executable code face greater legal jeopardy, as reflected in terms of use like:

> By accessing this site, you agree under the penalty of perjury [sic], you are not an agent or representative of any local, state, or federal law enforcement agency. You also agree that you are NOT collecting any evidence of any sort to incriminate this page's author, the [sic] or the authors of any files located on this site. You also agree that you are not accessing this site to collect information which could lead to, but is not limited to, shutting this site down or making its contents unavailable to the general public. ("Terms of Use" 2000)

prosecutions; and to the court decisions that banned 2600 from publishing or linking to DeCSS code. Dave Touretzky, who created the Gallery of CSS Descramblers, was "determined to show these movie industry types that it was a BAD IDEA to try to use trade secret law to interfere with free speech." (Touretzky 2003b) Of ten contributors to the gallery interviewed by this author[38], seven cited an explicitly political motive as the primary or exclusive reason for getting involved in the DeCSS issue. One contributor said that "it gave me an opportunity to talk to [my classmates] about the D.M.C.A., DeCSS, and code as speech"(Michaels-Ober 2003); another became interested in the DecSS issue because"[i]ntellectual freedom, and the ability to record, store and transmit information are dear to me."(Sandberg 2003b)

The fact that DeCSS distributors saw their distribution mechanisms as specific political responses to the D.M.C.A. and court decisions shows that DeCSS distribution meets the first test of a policy circumvention. The distribution schemes displayed in the Gallery of CSS Descramblers are not quite as clearly focused on nullifying these policy and court decisions – making the second test of policy circumvention a little harder. Most contributors to the Gallery expected that their distributions had limited practical impact; of the ten Gallery contributors interviewed, nine described their code as unlikely to be used, and estimated that no more than three people would have downloaded it.

---

[38] The Gallery of CSS Descramblers listed sixty-one unique contributors as of May 12, 2003. Of these, I attempted to contact twenty-two contributors via e-mail. Six e-mails bounced; four contributors did not reply; two more agreed to interviews, but failed to return their answers. Ten interviews were successfully completed, nine via e-mail, and one via online chat. I interviewed an additional five DeCSS distributors (distributors not listed in the gallery) via e-mail, for a total of fifteen interviews.

As Dave Touretzky observed, “If someone just wants to play or copy movies, they can get executables from other sites like doom9.net. I think people visit my site for intellectual stimulation, not to download code they want to use.”(Touretzky 2003b)

And indeed, the Gallery contributors make a point of noting the inevitability of DeCSS distribution. The role of the Gallery distributions is to underscore the fact that DeCSS distribution effectively nullifies the court and policy decisions. “I think my DeCSS webpage caused people to understand how ludicrous it was to try and stop the distribution of decryption code,” said one contributor. (Hocevar 2003) “I expect that the criminalizing of software tools will not remove the software from world wide availability distribution,” said another. (Miller 2003) In slightly grander terms, one Gallery contributor wrote that:

> I am optimistic that in the long-term, a balance will be achieved between "promoting the progress of science and useful arts" and totalitarian digital rights management. This balance will only be achieved once the intellectual property owners concede that hackers will always be one step ahead of them technologically.(Michaels-Ober 2003)

These comments were echoed by the views of the other (non-Gallery) DeCSS distributors, who offered comments like,

> I believe open source CSS code is now available fairily widely, and due to the international and anonymous nature of the internet, I don't believe it is going away anytime soon.(Steve 2003)

and

> There's no way to stop it. The internet is a free society. No content has ever been successfully banned from the internet.(Eisley 2003)

It is also clear that many distributors of executable DeCSS code also see distribution in political terms, and/or as a way of nullifying the court and policy decisions

on DVD encryption.[39] One former distributor[40] (since forced to remove DeCSS from his site) writes:

> this software is simply software to allow linux users to view DVD movies from their hard-drives. Based on all information available to me, I believe it is 100% legal to post this code….I am providing this content because I believe it is legal, and useful information.(Gadd)

A web site linking to a list of DeCSS mirrors (web sites that make DeCSS available for download) describes itself as "[t]he tool that every major film studio in Hollywood doesn't want you to know even exists,"("Humpin.org: King of the Road") and maintains a news page containing criticisms of the court decisions limiting DeCSS distribution. Another web site distributing DeCSS posted a restraining order it had received via e-mail, with the comment, "Note to all 'ye sharks out there: this site is located in Luxembourg. Hence I fail to understand how the rules and opinions of a Californian court (where the hell is that?!) would be relevant to this site or to me. In two words: Shove it."("DeCSS: watch your DVD's on your favorite OS")

The view that DeCSS distribution makes court decisions unenforceable is also widely reflected in discussions of the broader digital community[41]: a 1999 Slashdot discussion of one DeCSS distributor included comments like:

---

[39] The distributors of executable code are harder to track down, however, since their web pages so quickly disappear in the face of legal threats. See, for example, http://home.worldonline.dk/luke_s/

[40] The distributor notes that he was forced to remove DeCSS from his site after the MPAA contacted his Internet service provider. In spite of this, the author clearly believes that distribution has made the DeCSS unenforceable, writing, "If you are looking for DeCSS, be sure to check the DeCSS mirror list. I'm sure there are some sites up that are hosted on servers outside the reach of MPAA's lawyers."(Gadd)

[41] I use this term to distinguish between the "digital community" and the "Internet community." The digital community consists of the online community of Internet and technology professionals, experts, and enthusiasts. The Internet community is the much broader universe that includes all Internet users, many of whom have only limited interest in technology, and use the Internet strictly as a tool for pursuing other

> There's simply no way it can be stopped.
>
> Once the genies [sic] is out of the bottle it's very hard to put it back in.
>
> Well, it happened, The RIAA found out the hard way that you can't bolt the barn door once the Horse has run…The RIAA played rough, they found that netizens can get very rough indeed, and if they want any sympathy from me, Merriam-Webster comes to mind.
>
> Of course there's no way to stop this thing from being widely distributed, just like there is no way to prevent mp3 distribution or commercial software distribution. ("deCSS listed on Download.com" 1999)

The unenforceability of the DeCSS ban is thus widely cited, not only by source code distributors, but also by distributors of executable DeCSS code, and by the larger community. That such comments are common accompaniments to any DeCSS distribution page[42] shows that such distributions are aimed at nullifying court and policy decisions, and as such, meet the second criterion for recognizing policy circumvention.

Finally, we can see that DeCSS meets the third criterion for recognizing policy circumvention in its provision of non-excludable benefits. These include the benefits of raising awareness of the D.M.C.A. and other copyright laws, making it harder to crack down on violations of copyright laws, exposing flaws in DVD encryption technology, undermining public support for copy protection, and promoting awareness and use of open source software[43]. In addition, it provides the excludable benefit of allowing anyone who downloads or accesses the software to watch (or copy) DVDs on a Linux machine.

---

interests and relationships. Slashdot – self-titled as "News for Nerds" – is a major hub for the digital community.

[42] I am distinguishing here between web pages dedicated to DeCSS distribution, and DeCSS files made available on web sites dedicated to distributing pirated software, music, and movies (often known as warez sites). Warez sites are not typically political endeavors, but use the distribution of free software, etc. as the basis for selling advertising and/or pornography.

[43] The Linux operating system, for which DeCSS was designed, is the premiere example of open source software. "Open source" is software for which the source code is made publicly and freely available. This allows other programmers to inspect, improve, and extend the software, and usually allows the end

The DeCSS distribution phenomenon has raised awareness of the D.M.C.A. and other copyright laws by creating a wide range of web sites that draw attention to the problems with enforcing these laws, by precipitating a series of prosecutions under these laws, and by sparking discussion of copyright laws and their consequences. A Google search found more than forty thousand web pages referring to DeCSS in connection with the D.M.C.A. or other copyright issues.[44] There have been at least four court cases precipitated by DeCSS distributions; two in California, one in New York state, and one in Norway(Gross 2003a). A Usenet search for comments on DeCSS and copyright found more than four thousand postings to Internet discussion groups.[45] As previously discussed, many of the DeCSS distribution sites, as well as much online discussion, have drawn attention to the unenforceability of copyright laws in this instance.

DeCSS distribution has drawn attention to the technologies as well as the policies of copy protection. Many observers have noted that the CSS encryption scheme used to prevent DVD copying was relatively weak, since US export restrictions on encryption technologies prevented the industry from using anything stronger than 40-bit encryption.[46] CSS (the Content Scrambling System) has been variously described as

---

user to use the program free of charge. Open source has been praised as an accessible alternative to costly proprietary software (such as Windows), as more robust (because bugs can be identified and fixed more rapidly), and as more secure (because security holes can be identified and fixed).

[44] An April 9, 2003 Google search on *DeCSS (D.M.C.A. OR "intellectual property" OR copyright)* yielded 41,800 results.

[45] An April 9, 2003 search of Google's Groups archive on *DeCSS (D.M.C.A. OR "intellectual property" OR copyright)* yielded 4,060 results.

[46] The strength of different encryption schemes is represented by the number of bits in the encryption key; "[t]he bigger the number, the longer it takes for computer(s) to crack….It is computationally feasible to crack a 40 bit key. For this reason 40 bit encryption is rarely used."("SSL Certificate Encryption Strength" 2003)

"simplistic" (Stevenson 1999), "pathetically weak," (LuNaTiK) and "amazingly weak" (Simons 2000). The inherent weakness of the encryption scheme was compounded by the fact that one licensor of the DVD decryption technology failed to encrypt its key; this provided DeCSS developers with an easy way of cracking the system (Patrizio 1999). By drawing attention to DeCSS, and the encryption flaws that made it possible, DeCSS distribution undermines confidence in the technologies of copy protection.

Finally, DeCSS has served as the latest advertisement for open source software, open source development, and the Linux operating system. DeCSS was necessitated by the fact that Linux lacked a license agreement for the CSS encryption scheme, and "the very philosophy behind the Linux OS [made] it unlikely that such an agreement [would] be reached anytime soon." (Burke 2000) By drawing attention to DeCSS, and through it, to the Linux operating system, DeCSS distributors have expanded awareness of open source software. To many members of the digital community, increasing awareness (and ideally, use) of open source software represents a great leap forward from proprietary software. As one Linux developer writes,

> Open source is a disruptive technology. Disruptive technologies change our relationship to the world—how we travel, communicate, work. The railroad was a disruptive technology to the horse and buggy, the automobile to the railroad. Technologies that don't evolve, disappear. We believe the proprietary software development model is a horse and buggy whose time has come and gone….With open source software development, everybody collaborates, the best software wins. Not just within one company, but among an Internet-connected, worldwide community. ("What is Open Source")

Promoting open source software, exposing flaws in the technologies and policies of copyright protection, and increasing awareness of copyright issues are all non-excludable benefits of DeCSS distribution. These seem to be important benefits to DeCSS distributors, many of whom see copyright laws (as applied to source code) as

infringements of free speech rights. “I was outraged when I first read about the case, and I think I even downloaded the code "just because". Intellectual freedom, and the ability to record, store and transmit information are dear to me,” said one contributor (Sandberg 2003a). “I do believe that DeCSS in all its forms is ‘pure speech,’” said another. (Stevenson 2003) As one distributor described the film industry’s anti-DeCSS lawsuits,

> Say my house is burglarized, and afterwards, one of my neighbors puts up a sign saying "he has no locks on his windows." Yes, I'd conclude he's a asshole. I could say that he's encouraging crime, but he's not actually committing it. He's exercising free speech. And I'd be sure to put locks on my windows (and maybe put up a sign describing his diamond collection). It's not a perfect analogy, but it's a start.(Goldstein 2003)

We thus see that DeCSS distribution schemes meet all three criteria by which we recognize policy circumvention. They are a strategic political response to specific policy and court decisions, specifically, the D.M.C.A. and the court decisions restricting DeCSS distribution. They are attempts to nullify these policy and court decisions by rendering them unenforceable in the face of a flood of different distributions, many of them taking forms that use the shelter of protected speech. And they offer the non-excludable benefits of raising awareness of copyright issues, of flaws in copyright technology and policy, and of open source software. Finally, we can recognize it as a successful instance of policy circumvention because DeCSS remains widely available throughout the Internet.

Establishing that DeCSS is indeed a successful instance of policy circumvention is only the first step, however. The next challenge is to demonstrate that the three-variable model can indeed account for its success.

The first element – political entrepreneurs – clearly played a major role in the emergence of DeCSS distribution. Jon Johansen and other members of the Livid listserv (whose members were searching for a way to decrypt CSS) led the creation of the DeCSS

code. The large number of webmasters who immediately placed DeCSS on their sites got the code into distribution. By writing about the DeCSS phenomenon, and publishing the code, the editors of 2600 Magazine increased the profile and availability of DeCSS. By lending its legal services to the 2600 editors, and other DeCSS defendants, the Electronic Frontier Foundation ensured that the copyright and free speech issues around DeCSS received court, media, and public consideration. Dave Touretzky's Gallery of CSS Descramblers "helped to alert people to the issues raised in the 2600 case…. took some of the wind out of the MPAA's argument …[and] completely destroyed any hope of claiming that CSS is still a trade secret." (Touretzky 2003b) Contributors to the Gallery further muddied the distinction between source and executable code, and made it harder to distinguish between legitimate and illegitimate distributions. Together, these entrepreneurs made it possible for an inestimable number[47] of Internet users to download DeCSS code, despite legal efforts to suppress it.

DeCSS distribution also fits the second element of the model, in that the technical costs of a failed circumvention were and are very low. If a would-be DeCSS user downloaded a version of DeCSS that was incomplete or corrupted, she would simply be unable to watch a DVD on her computer; hardly a matter of life and death. If DeCSS distributors failed to make DeCSS widely available, the aggregate consequences would

[47] The extent and decentralization of DeCSS distribution makes it impossible to tally the number of DeCSS downloads or users. Based on the number of downloads reported by some mirrors, however (in the hundred per month) we can be confident that DeCSS users number in the tens if not hundreds of thousands. One web site reported 26,000 downloads in just five days(Harrison 2000); another small distributor reported a steadily growing pace of downloads from 300 per month in February 2002, to 800 per month as of April 2003.

likewise be minimal: Linux would simply remain a platform that did not support DVD playback.

Note that the costs of failure constitute a separate issue from the legal consequences of distributing the code. The purpose of DeCSS distribution is not to hide the identity of the distributor, but to make the code itself freely available. Indeed, many DeCSS distributors have made no attempt to hide their identities. The legal consequences that some DeCSS distributors have faced do not indicate a failed circumvention; if anything, they testify to the MPAA's perception that DeCSS distribution presents a meaningful threat to DVD encryption.

The low costs of failure have been crucial to the success of the DeCSS distribution phenomenon. Because the consequences of a failed distribution are minimal, anyone can participate in distributing the software. Creating an artistic source code distribution (as per the Gallery contributions) likewise presents no risk greater than leaving a line out of the code. Even the legal consequences of failure have been minimized: with so many DeCSS distributors in the game, the MPAA has been unable to prosecute more than a token handful. Most DeCSS distributors report no legal consequences greater than a "cease and desist" request, often filtered through an Internet service provider. Faced with only minimal costs of failure, many people have joined in distributing DeCSS, ensuring that the software remains widely available despite the legal crackdown.

Finally, DeCSS fits the third element the model: states have faced significant constraints on their efforts to crack down on DeCSS distribution. The two states that have been at the center of the storm – the United States and Norway – are both states with

strong liberal norms, reflected in both law and public opinion. These norms act as legal and political constraints, limiting the extent to which states can identify or prosecute DeCSS distributors.

One such constraint was the scope given to reverse engineering[48] under Norwegian law. The January 2003 acquittal of Jon Johansen specifically noted that Johansen's use of reverse engineering techniques "does not represent a violation of the penal code"("Jon Johansen Court Decision" 2003). Indeed, Norwegian copyright law "expressly permits reverse engineering of computer software."(Stevenson 2000) Reverse engineering has been framed as a freedom of expression issue, since it is sometimes "used by innovators to determine a product's structure in order to develop competing or interoperable products" and "is also an invaluable teaching tool used by researchers, academics and students in many disciplines, who reverse engineer technology to discover, and learn from, its structure and design".("Reverse Engineering") The freedom of information perspective on reverse engineering is reflected in the Norwegian copyright provisions pertaining to reverse engineering, which allows such action if "the information necessary to achieve interoperability has not previously been readily available."(Bing 2000) The liberal norms of freedom of information and freedom of expression are thus directly responsible for the reverse engineering provisions that limited the prosecution of Jon Johansen, and indeed, facilitated the creation of DeCSS in the first place.

The liberal commitment to freedom of expression also acted as a constraint on the repression of DeCSS distribution under American law. DeCSS distributors exploited the

---

[48] Reverse engineering "is taking apart an object to see how it works in order to duplicate or enhance the object." ("Reverse Engineering") Jon Johansen reverse engineered one element of the CSS system in the process of developing DeCSS.

particular protection afforded expressive speech in order to shelter some distributions of DeCSS source code. They then used the widespread availability of DeCSS source code to challenge the distinction between source and executable code, and to underline the difficulty in enforcing restrictions on DeCSS distribution.

By the time Judge Lewis Kaplan issued a ruling on DeCSS in the case of Universal Studios v. Eric Corley (the 2600 Magazine case), at least one US court had already ruled that source code was protected speech. In a case concerning the export of encryption software, the court ruled that

> Software relating to encryption is simply a topic of speech employed by some scientists involved in applied research. Hence, Snuffle [Bernstein's encryption program] is speech afforded the full protection of the First Amendment not because it enables encryption, but because it is itself speech. ("CDT Analysis of Berstein Decision" 1996)

In a different encryption case, the Sixth Circuit Court of Appeals had ruled that "computer source code, whether expressive or functional, is protected by the First Amendment."(Ghosh 2000) The Universal v. Corley ruling stuck a delicate balance between these positions, noting that "this Court assumes for purposes of this motion, although it does not decide, that even the executable code is sufficiently expressive to merit some constitutional protection. That, however, is only the beginning of the analysis."(Kaplan 2000)

The court noted that the DeCSS case demanded some balancing of the free speech principle, along the lines of the "fair use" provisions of copyright law.(Kaplan 2000) The challenge was thus to balance "the public interest in the restriction against the public interest in the kind of speech at issue." Because "DeCSS enabled anyone with even a basic understanding of computer programming to figure out a way around the protections on copyright-protected material…therefore, DeCSS was subject to greater

restrictions."(Morris 2000) In the words of the court, while "DeCSS has at least some expressive content, the expressive aspect appears to be minimal when compared to its functional component."(Kaplan 2000)

By arguing that the protected status of code depended on its expressive value, the court set the stage for the next stage of the DeCSS distribution effort: the Gallery of CSS Descramblers was developed to challenge this distinction. The entries in the Gallery are specifically designed to maximize the expressive value of the code, by embedding the code in recognized forms of expression like music and art. As Dave Touretzky writes in his introduction to the Gallery,

> If code that can be directly compiled and executed may be suppressed under the D.M.C.A., as Judge Kaplan asserts in his preliminary ruling, but a textual description of the same algorithm may not be suppressed, then where exactly should the line be drawn? This web site was created to explore this issue, and point out the absurdity of Judge Kaplan's position that source code can be legally differentiated from other forms of written expression. (Touretzky 2000b)

Because the US courts had acceded to the framing of DeCSS as a free speech issue, the Gallery (along with other forms of DeCSS distribution) collected many contributions from developers who saw the battle as a battle for speech rights. A student who included DeCSS code in his high school yearbook statement said that it "gave me an opportunity to talk to [other students] about the D.M.C.A., DeCSS, and code as speech."(Michaels-Ober 2003) The creator of an animation that embedded DeCSS code said he was motivated by the fact that "[i]ntellectual freedom, and the ability to record, store and transmit information are dear to me." (Sandberg 2003a) Another admitted that his musical contribution had "[a]esthetic value only. Many people had already adequately pointed out that deCSS and source code in general is really a form of speech. Anything beyond that is just for fun."(Schrepfer 2003)

As Touretsky's introduction to the Gallery pointed out, this playfulness had a serious purpose: to underline the difficulty, if not futility, of treating only some forms of software code as protected speech. The fact that US law and public opinion accords so much weight to freedom of expression created a major constraint on the suppression of DeCSS distribution. As long as even some forms of software code were acknowledged as protected speech (a point already conceded in law), the state would be heavily constrained in suppressing the distribution of DeCSS.

Finally, DeCSS distribution benefits from the difficulty the state has in identifying distributors. In the initial case brought by the DVD Copy Control Association (DVD-CCA) against DeCSS, the plaintiff listed five hundred unnamed defendants along with those it was able to identify[49]. As the complaint put it:

> DVD CCA is unaware of the true names and/or capacities of the defendants sued herein under the fictitious names Does 1-500, pursuant to Code of Civil Procedure Section 474, who each were responsible in some way for the acts and omissions complained of herein. DVD CCA will seek leave of court to amend the complaint to allege such names and capacities at such time as they are ascertained. ("DVD CCA Complaint in DVD CCA v. McLaughlin, Bunner, et al." 1999)

The inability to identify many of the DeCSS distributors obviously represented a major limitation in the ability to enforce policy and court decisions pertaining to DeCSS. This difficulty was partly a function of the many tools that Internet authors and users can adopt in order to remain anonymous. But the availability of those tools is itself a function of liberal protections, like freedom of speech, that are enshrined in the constitutions of many Internet-connected countries (Froomkin 1997). The only way of preventing anonymous participation in policy circumvention would thus be to eliminate liberal

---

[49] This case ultimately became three separate cases: Pavlovich v. DVD-CCA, DVD-CCA v. McLaughlin, Bunner, et al., and Universal City Studios et al. v. Eric Corley et al.

protections for anonymous speech, and to disconnect from the Internet (where other countries may still provide digital havens for anonymous activity). Since a liberal state like the United States is unable to take those measures, it is fundamentally constrained in its ability to identify, punish, or discourage anonymous participation in policy circumvention.

The recognition of reverse engineering as an issue of freedom of information, the framing of software code as a form of protected speech, and the inability to prosecute anonymous distributors all demonstrate the constraints that liberal norms impose on state efforts to repress policy circumvention. The case of DeCSS distribution is thus consistent with the third element of the predictive model.

Reviewing the case as a whole, DeCSS distribution appears to meet all the criteria for recognizing a successful policy circumvention. It is a strategic political response to particular policy and court decisions. It attempts to nullify these decisions by creating such a volume of DeCSS distributions that neither plaintiffs nor law enforcement can begin to stem the tide. In addition to offering DeCSS downloaders the excludable benefit of being able to watch DVDs on their Linux computers, it offers non-excludable benefits like raising awareness of copyright issues, of flaws in copyright technology and policy, and of open source software. We can see that DeCSS is not only a policy circumvention, but a successful one, because the software remains widely available online.

Furthermore, this success can be fully accounted for by the predictive model. We have political entrepreneurs, in this case the creators and distributors of DeCSS, who make it possible for many others to participate in the policy circumvention simply by downloading the DeCSS software. We have a policy area in which the costs of failure are

relatively low, in that the consequences amount to whether or not someone is able to watch a movie on his or her Linux-based computer. And finally, we have states that are severely constrained in repressing the policy circumvention, due to liberal norms that limit their law enforcement and prosecution capacity.

Policy circumvention: the case of Hacktivismo

Hacktivismo is a group created to "study ways and means of circumventing state sponsored censorship of the Internet and will implement technologies to challenge information rights violations."(Hacktivismo and Cult of the Dead Cow 2001) An offshoot of the Cult of the Dead Cow, a hacker group that "expanded the domain of hacking into the realm of the political" (Thomas 2002), Hacktivismo became its own group in 2001. Its members are drawn primarily from Canada, the US, and Germany but also reportedly include members in Israel, Korea, Taiwan, and China.

Hacktivismo was conceived by cDc member Oxblood Ruffin as a way to take on the large state-sponsored firewalls that limited access to the Internet in countries like Saudi Arabia, Cuba, Tunisia, and China. Firewalls

> act as intermediaries between users and the rest of the Internet. In countries where the Web is censored, the only way to access the Internet is through the firewalls. A user enters a URL - the address of a Web page - into his or her browser. This URL gets passed to the firewall, which checks to see if it is one of those banned by the government. If the URL is not on the list, the firewall forwards the request for the Web page and the contents of the page are relayed back to the user, who can then read it. If the URL is on the banned list the firewall refuses to forward the request and sends a page back to user indicating that the page he or she requested cannot be viewed by order of the government. ("About the Peekabooty Project")

Hacktivismo's first project, Peekabooty, was a software package that was intended to circumvent these firewalls. As Peekabooty's mission statement explains,

> Peekabooty is software that enables people inside countries where the Web is censored to bypass those censorship measures. The theory behind it is simple: bypass the firewalls by providing an alternate intermediary to the World Wide Web. …A user in a country that censors the Internet connects to the ad hoc network of computers running Peekabooty. A small number of randomly selected computers in the network retrieves the Web pages and relays them back to the user. As far the censoring firewall is concerned, the user is simply accessing some computer not on its "banned" list. The retrieved Web pages are encrypted using the de facto standard for secure transactions in order to prevent the firewall from examining the Web pages' contents. Since the encryption used is a secure transaction standard, it will look like an ordinary e-business transaction to the firewall. ("About the Peekabooty Project")

While Peekabooty has since spun off into its own entity, Hacktivismo has continued to create tools aimed at challenging Internet censorship. Its projects to date include Camera/Shy, a steganography program that "enables users to share censored information with their friends by hiding it in plain view as ordinary gif images" (Hacktivismo 2002); HESSLA ("The Hacktivismo Enhanced-Source Software License Agreement"), a legal framework that allows software developers to impose political terms of use on their users; and Six/Four, a peer-to-peer protocol for enabling censorship-free Internet traffic.

Hacktivismo meets each of the three criteria by which we define a policy circumvention. First, it is a strategic political response to policies of Internet censorship in at least twenty countries around the world (Reporters Without Borders 1999). Internet censorship has long been a motherhood issue for members of the digital community, spawning such efforts as the Electronic Frontier Foundation's Blue Ribbon campaign, in which web sites display a blue ribbon in support of free speech, and 1996's Black Thursday, when web sites turned their pages black to protest Bill Clinton's signing of the Communications Decency Act ("Why is this page black?" 1996). Internet censorship by authoritarian regimes has been a hacktivist target since at least 1998, when Bronc Buster,

a member of the Legions of the Underground, defaced China's official human rights web site on the day it was launched, leaving the message:

> China's people have no rights at all, never mind Human Rights. I really can't believe our government deals with them. They censor, murder, torture, maim, and do everything we take for granite [sic] left the earth with the middle ages….The Chinese communist government is made out of a gang of 100+ year old thugs and bullies who hide in seclusion. This pitiful effort of trying to change the hearts and minds of the world is a joke!("Crackers Attack China on Rights" 1998)

Bronc Buster later became one of the founding members of Hacktivismo, conceived by cDc "Foreign Minister" Oxblood Ruffin in the summer of 1999 ("The Hacktivismo FAQ v1.0"). Hacktivismo defined its mission as an explicit response to state policies of censorship:

> we DECLARE:
>
> THAT FULL RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS INCLUDES THE LIBERTY OF FAIR AND REASONABLE ACCESS TO INFORMATION, WHETHER BY SHORTWAVE RADIO, AIR MAIL, SIMPLE TELEPHONY, THE GLOBAL INTERNET, OR OTHER MEDIA.
>
> THAT WE RECOGNIZE THE RIGHT OF GOVERNMENTS TO FORBID THE PUBLICATION OF PROPERLY CATEGORIZED STATE SECRETS, CHILD PORNOGRAPHY, AND MATTERS RELATED TO PERSONAL PRIVACY AND PRIVILEGE, AMONG OTHER ACCEPTED RESTRICTIONS. BUT WE OPPOSE THE USE OF STATE POWER TO CONTROL ACCESS TO THE WORKS OF CRITICS, INTELLECTUALS, ARTISTS, OR RELIGIOUS FIGURES.
>
> THAT STATE SPONSORED CENSORSHIP OF THE INTERNET ERODES PEACEFUL AND CIVILIZED COEXISTENCE, AFFECTS THE EXERCISE OF DEMOCRACY, AND ENDANGERS THE SOCIOECONOMIC DEVELOPMENT OF NATIONS.
>
> THAT STATE-SPONSORED CENSORSHIP OF THE INTERNET IS A SERIOUS FORM OF ORGANIZED AND SYSTEMATIC VIOLENCE AGAINST CITIZENS, IS INTENDED TO GENERATE CONFUSION AND XENOPHOBIA, AND IS A REPREHENSIBLE VIOLATION OF TRUST. (Hacktivismo and Cult of the Dead Cow 2001)

If Hacktivismo was an explicit response to state policies of Internet censorship, it was equally clear about its intentions: to render those policies impotent and ineffective.

> We're hackers, not social justice activists. Let's put it this way. Some groups and individuals are well suited to fight for social and economic progress around the world. If

> as a result of an initiative in Africa, for instance, economic standards were raised and more people could obtain computers -- that would be a good thing. But what kind of Internet would they eventually have access to? One where censorship or the proliferation of vulnerable software left them at risk? We're not willing to sit by and watch that happen. We think of hacktivism and the Internet the same way that homeopathist's think of the body: you have to introduce a little poison to create health. Code has consciousness and healing power whether you like it or not…We are trying to intervene to reverse the tide of state-sponsored censorship of the Internet through the inventive use of code. This is what Oxblood is referring to when he uses the term "disruptive compliance". It's the opposite of "civil disobedience". We favor using disruptive technologies that comply with the spirit and original intent of the Internet. ("The Hacktivismo FAQ v1.0")

Finally, Hacktivismo meets our third criterion: the creation of non-excludable benefits. Indeed, Hacktivismo's mission is such that it primarily creates non-excludable benefits, since it makes its software and tools available not only to its participating coders but to all users of the Internet. In addition to these concrete benefits, Hacktivismo creates larger non-excludable benefits, like greater awareness of Internet censorship, and perhaps, inhibition in the development and maintenance of censorship technologies. While it creates some excludable benefits for members, like the social rewards and prestige of belonging to a high-profile hacker project, these are overshadowed by the non-excludable benefits that constitute its primary focus.

Hacktivismo is thus clearly an effort at policy circumvention: it is a strategic political response to censorship policies; it aims at nullifying the effects of censorship policies; and its primary benefits are non-excludable. But Hacktivismo can not be as clearly defined as a *successful* instance of policy circumvention. It has been bedeviled by internal conflicts, technical challenges and political constraints that have slowed its progress and limited its ability to effect policy circumvention (although it has had some notable successes in promoting policy change). These limitations largely stem from the ambitiousness and significance of the project: taking on the information controls of the

government of China is a much taller order than letting people watch a few DVDs. As a result, Hacktivismo's primary deliverables – the Six/Four system, and its cousin, Peekabooty – remain at the beta stage even after several years of development. The specific ways in which Hacktivismo has been held back, however, clearly support the three-variable model as an explanation for the relative success or failure of policy circumvention.

Hacktivismo certainly possesses the first element of the model: political entrepreneurs have played a major role in its efforts. Oxblood Ruffin[50], the self-styled "Foreign Minister" of the Cult of the Dead Cow, initially conceived of Hacktivismo in 1999, and has continued to drive much of its activities, and particularly, its public profile. At age 53, Ruffin's offline political experience remains relatively limited; he has only voted twice in his life, and has not attended a live political event since his one-time participation in a 1969 antiwar protest, when he was chased down the street after throwing a bucket of red paint. (Ruffin 2002) He worked in the United Nations community for about ten years, first in the media, and later as a political consultant on General Assembly affairs; but his political commitments are now strictly online. For Ruffin, hacktivism is necessarily about Internet freedom: "We're just trying to maintain as much Internet freedom as possible," he said in a September 2002 interview. "One person truly can make a difference. Body mass is not a requirement." (Ruffin 2002)

---

[50] While Ruffin uses his hacker "handle" or nickname in all his activities around cDc and Hacktivismo, and is referred to as "Oxblood Ruffin" in all coverage of Hacktivismo, his real name is essentially an open secret; his handle does not serve to disguise his identity or activities from legal authorities.

Nonetheless, Ruffin has been the nexus for recruiting more bodies to the Hacktivismo team. After founding Hacktivismo with the blessing of his fellow cDc members ("All this hacktivism stuff is cool," Ruffin was told by the cDc's leader, "but don't turn into Joan Baez." (Ruffin 2002)), Ruffin recruited Bronc Buster, known for his attacks on Chinese firewalls, to help in the project. Other early recruits included Mixter, a young German hacker best known for releasing a DDoS tool and related security report[51]; the Pull, who went on to create Hacktivsmo's Camera/Shy tool, and Drunken Master (a.k.a. Paul Baranowski), who became the lead programmer on Peekabooty. Later recruits were drawn from Ruffin's professional colleagues in Toronto, Mixter's hacking colleagues in various chapters of the Chaos Computer Clubs, and other connections forged online, bringing Hacktivismo's current membership to some forty members (Ruffin 2002).

Together, these members constitute a political elite that offers its programming, web design, and other skills to the creation of anti-censorship software tools. Much of its activities are modeled on programming practices in the open source community, in which programmers publish their source code so that others can improve or extend it. Working through a members-only e-mail list, in which all subscribers are expected to tangibly contribute to the work of Hacktivismo (Ruffin 2002), members are able to share their code-in-progress, and exchange ideas about strategy for both individual software tools

---

[51] A DDoS, or Distributed Denial-of-Service attack, is one of the most common methods used for attacking and paralyzing Internet servers. After a large-scale DoS attack in February 2000, Mixter's DDoS tool was briefly suspected of being the tool of the attack. In fact, another tool was used; and as Mixter takes pains to point out, his tool and white paper were released "according to full disclosure security policy", in which hackers publicly release security exploits in order to draw attention to key weaknesses that need to be repaired.(Mixter 2002a)

and the overall project. This working group of entrepreneurs, who are volunteering their own time, effort and knowledge in order to create software for use by a much wider audience, is the core of Hacktivismo's efforts.

Nor are their entrepreneurial efforts limited to software development. Different members bring different skills to the table, such that even non-programmers can be active participants in the project. Ca$h Money worked on the design of the Hacktivismo web site, and maintains its news feeds. (Money 2002) Mr. Happy's role is to maintain the web site, including writing content. (Happy 2002) Oxblood Ruffin admits that he's "not what you'd call a hard-core hacker," but plays a major role "at the strategic level," (Ruffin 2002) using his media skills to commandeer extensive press attention for Hacktivismo's activities. "Everyone's respected for what you do," according to Ca$h Money. "You are respected for how much work you do. What you contribute equals your status or prestige."

Many of Hacktivismo's participants seem drawn to the entrepreneurial role by the belief that here – as compared with offline politics – they can make a difference. "I don't think demonstrations can make a change. You make a change by making something productive….It's more important to have a goal and achieve that goal." (Mixter 2002b) Similarly, metac0m likes the idea that Hacktivismo "produces something tangible, rather than just protest. Something people can use." (metac0m 2002) "I like to concentrate on things that change something," said Jules (Jules 2002). Ca$h Money had a more modest notion of his contribution, comparing himself to the NASA janitor who, when asked what his job is, says it's to send a man to the moon: "I'm not changing the world," he said. "I am contributing in however small a way." (Money 2002)

If Hacktivismo has succeeded in building the corps of political entrepreneurs necessary for policy circumvention, it also illustrates that political entrepreneurs are not sufficient to ensure that circumvention's success. When we come to the second element, the need for low costs of failure, Hacktivismo is crucially lacking. Far from facing low costs of technical failure, the costs of a technical failure by Hacktivismo's tools may be very high indeed. In the words of one of Hacktivismo's early participants, "you need to create plausible deniability" for Hacktivismo users, because in some countries (like China) it is illegal even to request censored content (Baranowski 2002); that means that the software must not only make it possible to access banned content, but to disguise any trace of both the request and the software used to make it. If the software leaves a trail, the user could end up under arrest, or even executed.

These high costs of failure in turn impose a very significant burden on Hacktivismo's programmers, particularly considering that none of them are paid for their Hacktivismo work, Developing code that is robust enough to resist failure is a tall order – one that takes many hours of programming to fill. How those hours are divided up among an all-volunteer work force became a source of contention, and one that has proven very divisive among Hacktivismo volunteers.

Hacktivismo's first undertaking, Peekabooty, split off into its own project after a dispute over relative contributions to the effort. "For one and a half years I did all the work and he got all the credit," Baranowski said of Ruffin. Other Hacktivismo members had a different perspective on Baranowski's role within the project. Ca$h Money criticized Baranowski's attitude as "my way or the highway," and suggested that he was unused to working with an open source model.(Money 2002) Mr. Happy attributed the

break-up to “matters of ego and recognition” and said it had “nothing to do with coding.”(Happy 2002) Ruffin offers his own typically colorful account of the dispute:

> Hacktivismo progressed as a group but encountered a serious hiccup when the lead developer for Peekabooty rewrote the entire code base and decided [to] hijack the project and leave the group. It's amazing what some people will do when they figure they aren't getting enough press. When it was first announced on our listserv there were several days of chaos and rage. Some members wanted to crucify our little fame seeker, but it seemed best to let him go. He had been a disruptive force in Hacktivismo for months and things weren't getting any better. Plus when his code was reviewed it left our security experts dumbfounded. Peekabooty had been rewritten to conform to design specs that been rejected a year before as grossly insecure. You could hear the baby Jesus crying in Shanghai. (Ruffin 2004b)

In this he says-he says dispute, there is no arguing that a demanding coding project is vulnerable to disputes over relative contributions, as members disagree over different styles of coding, and to the value of coding versus other kinds of effort.

It is also clear that these internal disputes, and the ultimate Peekabooty split, have slowed down Hacktivismo’s progress in delivering usable software. “The last year and a half have gone slowly due to Peekabooty,” (Mixter 2002b) said Mixter, the primary coder on Hacktivismo’s Six/Four project. Four years after Hacktivismo was first announced, Peekabooty has only released a developer version[52] of its program; Hacktivismo’s new Peekabooty competitor, the Six/Four tool, has likewise only had a developer release.

Internal disagreements have only been part of the slow-down, however. Another obstacle in Hacktivismo’s development has been the legal hurdles that must be surmounted by software that challenges government authority. The release of the Six/Four developer version was delayed by US government restrictions on encryption

---

[52] A developer release is like a sneak preview of as-yet-unfinished software, intended for other programmers rather than for end users. By releasing a developer version open source software projects can engage other programmers in finding bugs, weaknesses, or areas for improvement, and allow other programmers to begin developing related software that will complement the program once it is released.

technology exports, which had to be negotiated before the software's release. (Mixter 2002b; Ruffin 2003) But encryption technology is not something that a project like Six/Four could easily forego. Precisely because of the high costs of failure, Six/Four needs to use very strong encryption technology in order to protect the identities of its users; and the export of strong encryption is regulated by the US government.

The high costs of failure have thus imposed two significant burdens on the Hacktivismo project. First, by imposing a rigorous standard of quality on the software code, it demands a significant commitment of time by Hacktivismo's programmers. As an all-volunteer project, Hacktivismo is vulnerable to disputes over how that time commitment in shared. Second, by requiring strong encryption to protect users' identities, it subjects Hacktivismo software to US government export regulations. Together, these obstacles have significantly slowed Hacktivismo's progress – although progress is still visible. But this is a game in which pacing matters: as Ruffin himself acknowledges, it is just a matter of time before government authorities figure out how to crack any code that programmers develop to protect people from Internet censorship.(Ruffin 2003) The more slowly Hacktivismo proceeds, the more quickly its target governments catch up.

If Hacktivismo has been slowed by facing high costs of failure, then those costs can be directly attributed to the lack of constraints on Hacktivismo's target governments. As the third variable in our model would predict, tackling non-liberal governments is a much tougher proposition for sponsors of policy circumvention. In the case of Hacktivismo, coders are taking on governments that face negligible political constraints on their ability to identify participants in policy circumvention, or to punish people for using circumvention software. By definition, any country that Hacktivismo targets – any

country that censors the Internet – has a government that is willing to use heavy-handed tactics in controlling information and information technologies.

International observers have amply documented the authoritarian tactics used to control Internet users in censoring regimes. A 2002 Amnesty International report on Chinese control of the Internet documented " prisoners of conscience who have been detained for using the Internet to circulate or download information."("State Control of the Internet in China" 2002) Those who are arrested are not necessarily radical challengers; "many have merely voided a politically sensitive opinion online." (Kalathil and Boas 2003) Online activities have become a central focus and weapon for Chinese state security:

> during searches of any political suspects' home or office, the first thing Chinese security agents seize these days is the computer, hoping to find on the hard drive incriminating evidence such as incoming or outgoing e-mail messages to co-conspirators…..It should also be noted that the authorities appear willing to charge dissidents with 'subversive' uses of the Internet that are inherently nonpolitical in nature, primarily as a tactic to silence them or smear their character…..The authorities searched [dissident writer Wang Yiliang's] home and found pictures of nude women downloaded from the Internet on his computer, which they subsequently used to sentence him to two years of reeducation through labor for 'possessing pornographic articles.'(Chase and Mulvenon 2002)

Using policy circumvention to challenge non-liberal regimes is thus much riskier than using policy circumvention to evade the policies or laws of politically constrained, liberal governments. While policy circumvention efforts may nonetheless emerge under these regimes, as in the case of Hacktivismo, they will be much less likely to succeed in nullifying their target policies.

The case of Hacktivismo shows how policy circumvention may fail, even when political entrepreneurs sponsor its emergence. Hacktivismo has a substantial and dedicated team of entrepreneurs, who together have fostered an ambitious program of

policy circumvention, but its efforts have often been stymied by the combination of high costs of failure and negligible constraints on repression. Despite almost four years of hard work, the project has yet to release end user software[53] that would fulfill its core mission: allowing Internet users in countries that censor the Internet to access the full range of online information and sites.

While Hacktivismo has yet to succeed in sponsoring policy circumvention, however, it has achieved some influence on policy change. Since the emergence of Hacktivismo, the US Congress has begun to consider legislation that would create an "Office of Global Internet Freedom", mandated to "develop and deploy technologies to defeat Internet jamming and censorship."("To develop and deploy technologies to defeat Internet jamming and censorship. 2003) The Congressional Committee considering the bill has contacted Hacktivismo as possible expert witnesses on the project.(metac0m 2002) The International Broadcasting Bureau, which runs the Voice of America, has already commissioned software that would allow people to tunnel through firewalls in Internet-censoring regimes (Festa 2003).

These developments suggest that Hacktivismo's goal, to enable circumvention of Internet censorship, may yet be achieved. But the history of the Hacktivsmo project itself strongly vindicates a model that posits political entrepreneurs, costs of failure and political constraints as crucial ingredients in the success of any given circumvention effort.

---

[53] The currently released version of Six/Four is a developers release.

Conclusion

The cases of DeCSS distribution and Hacktivismo support several facets of the policy circumvention argument. First, they establish that policy circumvention is a distinct and recognizable phenomenon, characterized by the three criteria I have identified: it is a strategic political response to a specific policy, law, regulation or court decision; it focuses on nullifying the effect of a policy, law, regulation or court decision; and it offers at least some non-excludable benefits. Second, these cases support the three-variable model as a predictor of the emergence and relative success of policy circumvention efforts. In both cases, political entrepreneurs played a major role in the emergence of the policy circumvention challenge; but where DeCSS distribution faced low costs of failure, and liberal states constrained in their ability to repress the challenge, Hacktivismo faced the opposite situation. As a result, DeCSS distribution has thrived, while Hacktivismo so far remains stalled at the starting gates.

Most important, however, is that both cases support the larger claim made at the start of this chapter: that policy circumvention, as much as policy change, poses a significant transnational challenge to the authority of the nation-state. In the case of DeCSS, a scrap of code that began its life in Germany and Norway was able to thwart the intellectual property rights of US-based companies, and US law was unable to stem the challenge. In the case of Hacktivismo, a coalition of hackers based primarily in Canada, Germany, and the US has launched a campaign that, while not yet successful in defeating Chinese firewalls, has added to international pressure against censorship practices in China and elsewhere. Together, these cases support the claim made earlier in this chapter: that policy circumvention is itself a major pressure on state autonomy, and one

that must be comprehended by research into the transnational pressures on the nation-state.

These cases also support my other two arguments about the theoretical significance of the policy circumvention phenomenon. First, policy circumvention is itself an additional pressure for policy change. In the case of DeCSS distribution, policy circumvention drew widespread attention to issues around intellectual property law in the digital era, and to the Digital Millennium Copyright Act in particular. While the D.M.C.A. was already law by the time the DeCSS phenomenon emerged, its interpretation in the case of Universal Studios et al. vs. Eric Corley et al. lent fresh credence to the arguments that were earlier voiced by D.M.C.A. opponents. In the ongoing struggle over digital-era revisions to intellectual property laws, the DeCSS case stands as a prominent example of what is at stake in those revisions, and of the difficulty in enforcing their provisions.

Hacktivismo has played an even larger role in promoting debate over Internet censorship. While it has had only limited effectiveness in circumventing firewalls, Hacktivismo has been remarkably effective in drawing attention to the firewall issue. The US government has launched its own Hacktivismo-like initiatives against Internet censorship; and each successive announcement of impending Hacktivismo software draws a major wave of media coverage on the issue of Internet filtering and censorship. While policy change is not the explicit focus of either Hacktivismo or DeCSS, it is nonetheless a potential by-product.

Finally, DeCSS and Hacktivismo illustrate the way in which policy circumvention changes norms about policy compliance. In the case of DeCSS, that takes the form of

widespread law-breaking by individual users of DeCSS, whose contravention of copy protection has been normalized by the widespread availability of contravention tools. In the case of Hacktivismo, the shift in norms is even more institutionalized: the fact that the US government is now adopting Hacktivismo-like tools suggests that even governments may be susceptible to the lure of policy circumvention as a tool of international diplomacy. Rather than pressuring China, Cuba, and other regimes to eliminate their censorship practices, the US will simply throw its resources behind making that censorship ineffective. State-sanctioned policy circumvention represents a significant shift in the norm of respect for the internal jurisdiction of one's fellow nation-states.

Alongside these theoretical issues, the phenomenon of hacktivist policy circumvention raises some crucial problems for policy makers. The first is that in an information economy, policy circumvention will be an expanding sphere of political activity. The domains that are most vulnerable to policy circumvention are domains that are dependent on information: information distribution, and information control. In an information age, more and more economic and social activity unfolds in these domains. That means that more and more of the state's activity, and its policy responsibilities, will unfold in domains that are vulnerable to policy circumvention by hacktivists.

This leads to a second implication for policy-makers: policies must be robust in the face of measurable defection. Policy is about setting rules that *most* people will follow. But policy-makers cannot ensure total compliance – particularly when it comes to policies that affect, or depend on, digital technologies. We can expect that a sizable chunk of the population will have the technological means to "defect" from many policies pertaining to the digital realm; how big a chunk depends on both the risks

associated with defection, and the state's ability to use heavy-handed enforcement. Any digital policy has to be robust in the face of non-compliance; if its fundamental justice or utility would be compromised by a measurable rate of non-compliance – whether 5%, 10%, or 20 – then it's not viable.

Finally, we should note that the threat of policy circumvention is not just a political threat – it's an economic one. States and corporations are partners in the causes and consequences of hacktivist policy circumvention. In the digital era, the infrastructure for policy enforcement is often digital – and the creators of that infrastructure are generally private companies. That makes state security inseparable from corporate security; the ability to enforce policy compliance extends only to the extent that your technology is hack-proof. This creates a complicated relationship of policy interdependence among countries: consider, for example, the fact that China's firewalls – the infrastructure for its information controls, and the target of much hacktivism – run on routers from US-based Cisco. The US is thus in the paradoxical position of fostering technology exports, on the one hand, and fostering circumvention of that technology on the other.

The other side of this coin is that corporations cannot insulate themselves by or from state policy. A court ruling provides no protection from the challenge of hacktivism. So a corporation like Lufthansa may find its web site under attack, as a proxy for a broader challenge to German deportation policy.

Or a company like eToys could find that a court ruling is far from the last word. Etoys certainly learned that policy circumvention can be a powerful counterweight to

state authority. Despite its favorable court ruling, eToys filed for bankruptcy two years ago(Shabelman 2002)[54]. etoy is right where it was: live and online.

[54] The eToys web store has since re-opened, as a division of KB Toys, which purchased the online assets of eToys after its bankruptcy.