IJoC | Piracy & Social Change

You Are Not Welcome Among Us:
Pirates and the State

JESSICA L. BEYER
University of Washington, USA

FENWICK MCKELVEY[1]
Concordia University, Canada

In a historical review focused on digital piracy, we explore the relationship between hacker politics and the state. We distinguish between two core aspects of piracy—the challenge to property rights and the challenge to state power—and argue that digital piracy should be considered more broadly as a challenge to the authority of the state. We trace generations of peer-to-peer networking, showing that digital piracy is a key component in the development of a political platform that advocates for a set of ideals grounded in collaborative culture, nonhierarchical organization, and a reliance on the network. We assert that this politics expresses itself in a philosophy that was formed together with the development of the state-evading forms of communication that perpetuate unmanageable networks.

Keywords: pirates, information politics, intellectual property, state networks

Introduction

Digital piracy is most frequently framed as a challenge to property rights or as theft. This framing is not incorrect, but it overemphasizes intellectual property regimes and, in doing so, underemphasizes the broader political challenge posed by digital pirates. In fact, digital pirates and broader "hacker culture" are part of a political challenge to the state, as well as a challenge to property rights regimes. This challenge is articulated in terms of contributory culture, in contrast to the commodification and enclosures of capitalist culture; as nonhierarchical, in contrast to the strict hierarchies of the modern state; and as faith in the potential of a seemingly uncontrollable communication technology that makes all of this possible, in contrast to a fear of the potential chaos that unsurveilled spaces can bring.

Jessica L. Beyer: jlbeyer@uw.edu
Fenwick McKelvey: Fenwick.McKelvey@concordia.ca

[1] Both authors are equally responsible for the content of this article.

In his "Declaration of the Independence of Cyberspace," John Perry Barlow (1996, para. 1) names states—those "weary giants of flesh and steel"—as things of the past, which are "not welcome among us" (ibid.). By distinguishing between piracy's challenge to property rights and its challenge to state power, we argue that digital piracy should be considered more broadly as a challenge to the authority of the state. We describe the relationship between piracy and the state through a history of technological confrontations that span evasion to engagement. We illustrate how digital piracy is a key component in the development of a political platform that advocates for a set of ideals grounded in collaborative culture, nonhierarchical social organization, and a reliance on the network. We point to the creation of this political philosophy in tandem with the development of state-evading forms of communication.

These ensuing unmanageable networks would likely not be relevant to studies of popular communication if digital piracy were merely an elite or covert mode of state-resisting communication. However, digital pirates not only seek to create state-evading communication infrastructures, but their politics aspire to make these infrastructures as popular as possible. Particularly in the case of The Pirate Bay, mass piracy has been able to create state-free zones (Dyer-Witheford, 2002).

To understand this phenomenon, we bring two disparate strands of literature from media studies and political science into conversation. We begin by introducing relevant literature on the digital enclosure, the state, and hackers. We then discuss the idea of a CryptoNet or darknet as imagined by cypherpunks and others, before moving to a history of peer-to-peer (p2p) networking. Since the history of p2p networking as an alternative form of file distribution has been given significant attention, we focus on the interactions between pirate networks and the gaze of the state. We explicitly highlight MojoNation and BitTorrent as two crucial technical developments in the struggle between pirates and the state. We conclude by discussing how The Pirate Bay marks the most direct confrontation between pirates and the state—both in their support for a political party and in their state evasion.

Pirates and the State

Much of the literature about piracy has focused on the recording industry as a "microcosm of mass communication's past and harbinger of mass media's future" (Baym, 2011, p. 23). After the "Napster watershed" (Burkart & McCourt, 2006), small pockets of digital music piracy in the hacker underground gave way to an ongoing movement of mass piracy facilitated by decentralized or p2p file-sharing (Dyer-Witheford, 2002; Gillespie, 2007). These technologies—whose history has been discussed in depth (Allen-Robertson, 2013; Andersson Schwarz, 2014; Burkart, 2010; David, 2010; Johns, 2010)—have radically altered access to cultural products, inspiring some to label them a "digital commons" (Vaidhyanathan, 2004) or a "Celestial Jukebox" (Burkart & McCourt, 2006).

The debate rages about whether piracy is an alternative, is in opposition, or is auxiliary to the recording industry. Strangelove (2005) argues that pirate networks are an "empire of the mind" and explicitly anticapitalist, while Baym (2011) and Andersson Schwarz (2014) both regard piracy as part of the music industry and a catalyst for industry innovation. While the precise role of piracy in relation to the music industry remains disputed (Andersen & Frenz, 2007; Bhattacharjee, Gopal, & Sanders, 2006), the

past decade of recording industry lawsuits targeting anything associated with digital piracy demonstrates that it is seen as an unwanted influence to be purged from the Internet.

Drawing on the metaphor of an information commons, the struggle to prevent piracy on the Internet has been described as the construction of a "digital enclosure" (Bettig, 1997; Boyle, 2003; Schiller, 1999). The term *digital enclosure* references the enclosures of the commons that occurred in England as part of the Industrial Revolution. This framing of the Internet as a commons under threat of enclosure implicitly and explicitly argues that governments and corporations seek to erase the antagonistic history of the Internet, rewrite its rules to favor market and corporate activity, and marginalize public goods online in favor of private property and commercial interests. The process of enclosure is then the work of corporations and the state in copyright law, free trade agreements, and criminal prosecution— meant to enforce intellectual property through digital rights management, end user agreements, and content filtering. Within this logic, digital piracy, simply by existing, opposes this enclosure through the work of preserving an open Internet.

We accept the conceptualization of the enclosure, but contend that scholars examining digital piracy have underemphasized the role of the state in this process. To understand the role of the state in this process of enclosure, we bring political science literature about the formation of the modern state and state-society relations into conversation with literature focused on the economic aspects of digital piracy. Drawing again on the metaphor of enclosure, when political scientists speak about the historical enclosure of the English commons, they highlight the role of the state. The literature about historical enclosure is part of political science theory about the formation of the modern state and state-society relations; in particular, we emphasize the role of the modern state as an actor that both reifies and enforces capitalist societal structures, as well as an actor that pursues unchallenged authority in all spheres. As such we draw on Migdal's definition of the state as:

> A field of power marked by the use and threat of violence and shaped by (1) the image of a coherent, controlling organization in a territory, which is a representation of the people bounded by that territory, and (2) the actual practice of its multiple parts. (2001, p. 16)

In such a conceptualization, the state projects a coherent image of an all-powerful, single actor, at the same time that its many parts engage in various and constant struggles with actors who are attempting to reshape societal rules. These daily struggles between the state, as it attempts to be the final definer of "the rules" in society, and the many factions within society that are attempting to reshape the rules, is the inner dynamic of state-in-society theory (Migdal, 2001). The work of the digital enclosure then is part of the everyday reassertion of state authority in the continuous state-building process.

We argue that the modern state's dependence on control of information as a mechanism to produce and reproduce power has been a feature of the modern state since its birth—and incorporate Braman's (2007) conception of the "informational state" into our study. She claims that an informational state "uses control over information to produce and reproduce loci of power and to carve out areas of autonomous influence within the network environment" (Braman, 2007, p. 36). The modern state has

improved its ability to use information as an integral part of its strategies of domination as technology has improved. Indeed, the use of information in the consolidation of power has been an essential component of every theory about the formation of the state (although sometimes implicitly). The modern state depends on an informational infrastructure that makes its territory and population legible. As Scott argues about this process, the early modern European state turned the "social hieroglyph" of society into a "legible and administratively more convenient format" (1999, p. 3). This practice of legibility, or what Scott calls "social simplification"—which included gathering and recording as much information about individuals as possible—allowed states to then intervene directly in the lives of citizens. Elsewhere, Scott also argues that this mastery over information, which has only increased over time, has given modern states in every era vast power to expand authority over the ungoverned (Scott, 2009).

The state-building project that manifested the modern state has been one in which the state systematically made itself the primary authority figure in society, in part through informational domination—making all other traditional authority figures, such as religious leaders, subservient to the state itself. This process has been well documented, and a frequent case to highlight this consolidation of authority has been the same process of enclosure in England that is used by media theory to understand controls over digital information. For instance, in his seminal work, Polanyi discusses enclosure as being part of the destructive process that ultimately led to the horrors of the 20th century. For Polanyi, enclosure serves as another case where classical economic liberal ideals were allowed to structure society, something so disruptive that the Crown had to step in and slow this process of economic improvement to protect the humans affected (Polanyi, 1944/2001). Similarly, Moore articulates the process of enclosure as driven by the newly emerging middle class and Parliament, also acknowledging that the enclosure's damaging nature was slowed by the Crown (Moore, 1966).

Using such an understanding of a never-ending state-building process, it is predictable that the state would view any unregulated digital commons as a threat to its power. The process of digital enclosure then involves the reassertion of state power to enforce property rights through the prevention of piracy—an action taken through cooperation between the state and the segments of society wanting to maintain and expand their understandings of intellectual property (Johns, 2009). Much as in the original English enclosures, contemporary states are not unitary actors, but rather, the aggregate actions of individuals and institutions that have created a movement toward digital enclosure. As part of this aggregate, digital piracy is most often framed as theft of property, but it is likewise a challenge to state power.

As Scott argues, the "modernizing" state works to create a particular type of relationship with its citizens—one that makes its citizens legible (1999). The same demands continue for the normalization of the Internet, and they require digital communication to be visible to the state so it is able to enforce property rights. As intellectual property concerns propel the state into closer surveillance of digital communication, the state's demand for visibility and its protection of intellectual property owners come into conflict with the emergent values from online spaces.

Relevant to this discussion is the emerging literature that considers the politics of piracy—and by extension the politics of hacking—to be a major social antagonism that takes place in and around

technology. *Hacking* acts as a catch-all term for the many alternative approaches to technology (Coleman, 2013; Kelty, 2008; Söderberg, 2010). Hacker cultures have developed with a sense that open information is natural to digital materiality. Some hackers only desire open code (Raymond, 2001); others desire free code (Stallman, 2002); and yet others desire even greater social transparency based on the free flow of information (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2012). These moral positions mean that hackers act as recursive publics (Kelty, 2008) whose historic sense of the Internet-as-open drives the development of new technology to actualize openness. Hacking the fixedness of technology offers a form of resistance against prescribed uses, particularly those focused on preserving digital scarcity and regulability (Lessig, 2006). This antagonism plays out both in use and in production (Spilker & Hoier, 2013).

Emphasizing the role of the state and resistances to the state-building process better recognizes the state-resisting agendas of pirate and hacker cultures. Piracy particularly undermines state power by creating communication that is difficult for the state's administrative gaze to observe and its judicial arms to control. As activists argue, piracy is about specific contestations over the circulatory capacities of communication technology—what can be said, transmitted, or distributed. The work of pirates then involves perfecting the art of not being governed online (Scott, 2009), and state evasion has motivated activists to work to create uncontrolled spaces where the coercive power and regulation of the state cannot intrude**.**

Data

We present data in support of our argument that digital piracy is a state-evading practice from two major research projects. First, much of the historical overview of p2p generations comes from a research project into infrastructural struggles over Internet routing (McKelvey, 2012; McKelvey, forthcoming). As part of this project, McKelvey analyzed the technical development of p2p algorithms and how iterations purposefully sought to avoid the technical management by network providers. Much of the theoretical understanding of piracy is also derived from the lessons learned from this larger project.

Second, additional data came from a comparative ethnography of online communities conducted between 2007 and 2011 (Beyer, 2014a; Beyer, 2014b). Some of the findings of this project, such as beliefs about piracy, the framing of piracy as political activism, and the impact of the Pirate parties, provide evidence for our argument. Further, much of the theoretical understanding of the relationships between online spaces and the state—in particular, the state-building project in relation to the online world—was taken from this larger research project.

Pirate Utopias, Hacker Culture, and CryptoNets

Activists, anarchists, and libertarians have tried to evade the state online. Hacker cultures associated with public cryptography (Zimmermann, 1999), cypherpunks (Hughes, 1993) and crypto-anarchists (May, 1992) have all been inspired to develop better privacy communications for citizens (see Ludlow, 2001). We separate these cultures in spite of their commonalities to highlight their various motivations in developing software for state evasion—similar to the great divide between Eric S. Raymond

and Richard Stallman in the free and open-source software moment. These disparate groups embraced the Internet and sought to repurpose the network.

Arguably, their first impact was more cultural then technical as cypherpunks appeared on the front cover of the second issue of *Wired* magazine (Levy, 1993). The cypherpunks became particularly articulate in expressing the link between state evasion and computer networks. This articulation happened on and around the cypherpunk mailing list where members developed the encryption tool Pretty Good Privacy (PGP) (Hoffman, 1995) and complained about *warez*, a play on the term software used to describe early online file-sharing (Tetzlaff, 2000), and other matters related to cryptography. As crypto-anarchist and former Intel engineer Timothy C. May (1992) explains in his manifesto, which he read at the first cypherpunk meeting in 1990 and later posted to the mailing list, "computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner." According to May, the CryptoNet would, among other things, "alter completely the nature of government regulation" and "the State will of course try to slow or halt the spread of this technology, citing national security concerns" (May, 1992, para. 4). (In light of this rhetoric, it should be no surprise that later, Julian Assange also participated in the group.)

Piracy proved an inspiration to these hacker communities to develop networks, or what May calls the CryptoNet, which could elude the power of the state with secure, anonymous communication (Greenberg, 2012; Levy, 2002; Ludlow, 2001). These groups reappropriated the image of a romanticized swashbuckling pirate after the recording industry began using the skull and crossbones to warn the public about "piracy" in an attempt to evoke violent sea pirates (Land, 2007; Leeson, 2007).

Further, the cypherpunk mailing list often discussed the writings of Hakim Bey, who also drew on piracy lore as a way to articulate a political agenda. Bey's article about Temporary Autonomous Zones cited pirate utopias as anarchist spaces that could inspire network designers and p2p developers. He argued that data havens could be the 21st century's equivalent of the Pirate Havens of the Barbary Coast and Libertatia (Bey, 2001; Wilson, 2003). For actors such as Bey, piracy in these hacker cultures meant the evasion of the state as well as the insecurity of intellectual property.

A challenge for the cypherpunks and others was that the technology to create these pirate networks did not yet exist. While the CryptoNet might have been fiction when May wrote his manifesto, darknets informed his vision of the future of computer networks. *Darknets* refer to networks sharing information with little regard for content, particularly as to whether that content infringes on digital property (Burkart & McCourt, 2006). Darknets existed since the beginnings of computer networks due to the work of various hacker cultures to create the often small, private computer networks, such as electronic Bulletin Board Systems (Biddle, Engl, Peinado, & Willman, 2002; Sterling, 1992). The type of disregard for content that darknets represent antagonizes the state (and intellectual property holders) because it purposefully ignores intellectual property regimes while drawing on the Internet's affordances to remain anonymous, making the individuals involved invisible to the state. While many of these hackers sought to develop PGP, encryption discussion on the list also saw p2p communication that avoided the surveillance of the state as another important way to create their pirate networks. Although the p2p concept might have been prefigured by the cypherpunks and the hacker underground, its development

was left to a few teenagers inspired by their own exchanges on #w00w00 (Allen-Robertson, 2013)—an elite hacker Internet Relay Chat (IRC) channel (O'Hear, 2014).

The Napster Watershed

While Napster was not part of an explicit activist project (Morris, 2015), it had an essential role in inspiring subsequent activists to challenge the state. Napster popularized the ambitions of the pirate underground by making a decentralized communication network accessible to most Internet users. Prior to Napster, would-be pirates had to deal with mp3 sites that "were fleeting, buried, dilapidated, and outdated" (Gillespie, 2007, p. 23).

Just as Napster use reached critical mass, the state stepped in on behalf of media industries to dismantle the file-sharing site. The Recording Industry Association of America (RIAA) filed suit against Napster in 1999. The trial was based on a ruling that drew heavily on the famous *Sony v. Universal* or "Betamax" trial as discussed elsewhere (Landes & Lichtman, 2003). In the Sony case, the judge found in favor of Sony, but in the Napster case, the judge decided against Napster because its users were overwhelmingly infringing copyright. The ruling pointed to Napster's central servers and its theoretical ability to filter infringing content—a capacity unavailable to Sony. The ruling did not shut down Napster; rather, it required Napster to remove infringing content from its search index and ban users who were sharing the infringing content. The court, in effect, ruled that Napster had to control the communication in its p2p network in order to obey copyright laws, and this requirement killed Napster.

Social Change through Better Code

Napster's closure did not end p2p file-sharing—as the recording industry and the state had hoped. Instead, visions of darknets and cryptonets inspired a nascent political movement intent on creating state-evading networks that were able to transmit any type of content. Napster helped popularizing the term "p2p" as synonymous with state-evading communication. Programmers of all types began to cluster around p2p development—attempting to develop a p2p network that could not be shut down by the state. For these programmers, hackers, and activists, the state response to Napster did not serve as a deterrent. Instead, Napster's susceptibility to the state was seen as a way to highlight a technical problem that could be fixed with better code (Oram, 2001). Dozens of solutions emerged to achieve varying degrees of success (Austin, 2005; Plambeck, 2010). Some, such as OpenNap, merely copied Napster. Others, such as Kazaa, Morpheus, and AudioGalaxy, attempted to create profitable companies distributing file-sharing software.

While social movements in liberal democracies often employ the legal system to further societal change, those involved in this new hacker activist culture instead sought to evade the state by developing better code. Justin Frankel, inventor of WinAmp, captured this nicely, when in an interview, he recalled his first impression of Napster as: "I thought, 'Wow, that's pretty cool, but how will they keep from getting sued?'" (quoted in Kushner, 2004, p. 45). He answered his own question by developing a new p2p network called Gnutella in 2000.

The combined efforts of p2p programmers proved successful. By 2002, p2p accounted for 60% of Internet traffic (Sandvine Inc., 2014). One of the innovations created through this activism was to address what Frankel and other developers regarded as Napster's critical weakness—that it was too fragile to withstand the power of the state because of its centralization. Thus, rather than operating within the system to change the law, decentralization became a deliberate strategy adopted by the next generation of p2p developers to avoid the law (Leyshon, 2003; Wu, 2003).

Decentralization partially occurred through the move from proprietary and commercial code to open code. While Napster was a closed-source application, Gnutella was an open-source protocol with corporate backing, thus limiting the targets of lawsuits (Kan, 2001). This evolution marked an important intersection of the free software values discussed by Coleman (2013) with regard to piracy. It also meant, in relation to state power, that whereas an instance of Gnutella could be shut down, the actual software had no connection to the content. Open sourcing detached the production of Gnutella from any one location or organization. There were subsequently 22 different versions developed, which distributed the Gnutella protocol across different organizations and jurisdictions.

MojoNation and BitTorrent

The rise and fall of these commercial p2p networks helped cypherpunks and hackers refine the challenge posed to state authority. In order to do this, not only did networks have to be decentralized and distributed, but they also had to address uneven sharing and free-riding. For example, the free-rider problem (taking without giving back) plagued Gnutella (Adar & Huberman, 2000). It not only degraded the flow of information, but also threatened to inadvertently centralize the network—thereby reproducing the vulnerabilities of Napster. For activists, this was not only an issue of selfish users, but also a possible limitation on the disruptive potential of the technology. Even though darknets and anonymous networking had existed longer than Napster, the hope had been that the popularization of p2p tools could universalize rule-breaking communication. However, it fell to the next generation of p2p developers to make state evasion viable on a larger scale.

Within this tradition an active member of the cypherpunks mailing list, Jim McCoy, created the MojoNation project. Although this project was fueled by venture capital, McCoy was clearly inspired by the ideas of pirate anarchists such as Bey (2001), and named his company Autonomous Zone Industries. The developers called themselves "Evil Geniuses for a Better Tomorrow"—a reference to a game by Steve Jackson Games (Cave, 2000) and also a reference to the founding of the advocacy group Electronic Frontier Foundation (Sterling, 1992). In line with its political roots, the MojoNation website reiterated its ambition for a sustainable digital commons. It argued that digital networks are an opportunity for people to "convey information, images, and ideas that others wished to censor, remove, or outlaw" (Mojo Nation, 2000, para. 5).

Autonomous Zone Industries launched MojoNation in 2000 at DefCon, a famed hacker conference, where they presented it as a way to increase the resources of a p2p network (McCullagh, 2000). MojoNation broke a file down into pieces and distributed the pieces across the network as a way to avoid censorship. Breaking the file down meant that no single node contained a whole file. In doing so,

the system avoided concentrating files in any one server. Importantly, MojoNation addressed the issue of free-riding-induced centralization by not being a gift economy; rather, it attempted to create an economy of sharing by rewarding people when they shared files using a virtual karma system called "Mojo." The ultimate, revolutionary, goal was "an open market [that would be] an ideal place for people to exercise individual liberties: to make their own choices about information use and availability rather than having these choices determined by national government or local regulation" (Mojo Nation, 2000, para. 10).

MojoNation's innovations resonated technologically and politically among antistatists, even after the company ceased commercial operation in 2002. A similar project, FreeNet, shared many of the same distributed design ideas of MojoNation. It aimed to create a "decentralized p2p architecture to create an uncensorable and secure global information storage system" because "governments around the world have undertaken efforts to force Internet service providers to block access to content deemed unsuitable or subversive, or to make them liable for such material hosted on their servers" (Clarke, Sandberg, Wiley, & Hong, 2001, pp. 40–41). While the open-source project continues in development, the popularization of these ideas would be accomplished elsewhere.

Bram Cohen, an ex-MojoNation employee and longtime member of the cypherpunks mailing list, pursued the quest to improve p2p protocols. Over the course of 2001, Cohen developed and released the BitTorrent protocol and client (Thompson, 2005). One of Cohen's central innovations was to build a protocol that decentralized the very network itself. While Gnutella and MojoNation both attempted to create singular p2p networks, BitTorrent proliferates networks. In fact, every file shared through BitTorrent has its own network of peers. This trick is made possible by inverting the logic of connection—where peers once logged into networks to share files, in contrast, torrent files provide the meta-data necessary for peers to participate in their own BitTorrent network. Similar to MojoNation, BitTorrent approaches data as the sum of smaller pieces of information. The metadata list the number of pieces and their sizes in a given file. Through reading the metadata and performing error checking on the pieces received, a BitTorrent client gradually assembles a complete copy of file through all the bits shared on the unique network.

Although BitTorrent represented a sea change in the potential to create state-evading communication networks, that technology alone was not sufficient to further the political goal. The nascent political movement, whose platform was developed through listservs and other collaborative technology while developing tools to evade the state, found a coherent expression in pirate politics. BitTorrent, taken alone, was simply an innovation in p2p networking, increasingly detached from the political projects of Gnutella or MojoNation, but its innovations became foundational for the Pirate Politics movement (Burkart, 2014).

Hacking the State: From The Pirate Bay to Pirate Parties

In 2003, a Swedish anticopyright group known as Piratbyrån (The Piracy Bureau) founded the popular file-sharing website The Pirate Bay—which came to be a powerful symbolic actor, framing file sharing as a political act. The activists involved in The Pirate Bay have been very vocal that the website must be part of a political agenda that includes the creation of a very public darknet where any

information can be shared without censorship.

At the time of writing (February 2015), the longstanding popularity of the site has only very recently resumed, currently ranking it as the world's second most visited BitTorrent indexing site.[2] The dip in popularity between December and February was because the site went offline following a police raid at the location where the site was hosted in Stockholm, Sweden, on December 9, 2014. This was not the first time the site was raided, and it remains to be seen if this hiatus has helped cause a break with the near-monolithic status of the site, which has for the last decade been seen as more or less synonymous with BitTorrent. Before the raid, The Pirate Bay had more than a billion page views a month (Ernesto, 2014).

File-sharing insider news site *TorrentFreak* explains this shift, while hinting at the resilience of the overall BitTorrent ecosystem:

> [The Pirate Bay] has been crowned the most popular torrent site since 2008, but isn't serving any torrents at the beginning of this year. As a result, the top spot is now taken by KickassTorrents. The Pirate Bay hasn't gone away completely though. There are currently several popular clones and copies of the site that together can easily match the traffic of most other sites that are listed. (Ernesto, 2015, para. 5–6)

Prior to December 2014, The Pirate Bay had long remained the largest, most public BitTorrent search engine and tracker on the Internet, in spite of constant legal threats and a guilty verdict for the three men who were administrators of the website for a time—Peter Sunde Kolmisoppi, Fredrik Neij, and Gottfrid Svartholm Warg. These men have argued that the website is simply a search engine and have shut down the website's tracker to emphasize this function, a move aimed at legitimizing the site in relation to Swedish law (where its servers have been located).

The Pirate Bay activists describe their work as creating a kind of alternative commons—a place outside the law or regulation. Perhaps most apt given the roots of piracy in offshore radio, they half-jokingly suggested purchasing Sealand, a well-known data haven hosted on a retired sea fort in the North Sea. Due to its location in international waters, Sealand is considered to be a micro-nation, and The Pirate Bay promised to create its own Nation of Pirates upon it. While this move to physical sovereignty proved unsuccessful (Libbenga, 2007), the contents of its search indexes remain outside any control—even of the administrators, who have refused to remove any torrents. The Pirate Bay's attempts to create an open index of files shared on the Internet—a kind of mass index beyond state or corporate censorship—recodes the dreams of prior hackers and developers.

In spite of the administrators' belief in the legality of the site, their activism has put them in direct confrontation with the Swedish and U.S. governments. This confrontation has coincided with a new

---

[2] On February 17, 2015, The Pirate Bay's global Alexa ranking was 206 (Alexa, 2015b) while its competitor Kickass Torrents ranked at number 67 globally (Alexa, 2015a).

development in the piracy movement—one that is not about state evasion, but rather about direct engagement with state institutions. The new direction is at odds with crypto-anarchy but consistent with traditional activist confrontation with the state. As The Pirate Bay has repeatedly lost in Swedish court, first Swedish youth and subsequently young people across other democracies have become politically engaged with Pirate parties (Erlingsson & Persson, 2011).

Although not affiliated with The Pirate Bay, the Pirate parties owe much of their success to The Pirate Bay. The Swedish Pirate Party membership grew every time one of the Pirate Bay principals appeared in court and, as a result, has sent two representatives to the European Parliament. Pirate parties have sprung up in some 40 countries around the world and have had electoral successes. In 2009, around 13% of first-time German male voters gave the new German Pirate Party their votes (Allen, 2009). In Germany, the party has seen support in state and local elections, and as of mid-2012, 209 German Pirate Party members had been elected, with 45 of these seats being gained in state level elections (Ernesto, 2011). The Pirate parties in Switzerland, Croatia, the nationality of Cataluña, and Austria managed to win city-level seats between 2010 and 2013 (Falkvinge, 2012; Nordenfur, 2014; Voegt, 2013). The Icelandic Pirate Party gained three seats in the Icelandic Parliament in 2013 (BBC, 2013), and the Czech Pirate Party won a seat in the national parliament in 2012 (Jones, 2012). While the Pirate Party platform varies to some extent from country to country, all of the Pirate parties tend to agree that intellectual property law should be revised, and that the move by governments to increase surveillance, particularly using digital information, must be stopped.

Meanwhile, The Pirate Bay remains online and continues to frame its presence in political terms despite the concerted efforts of the U.S. government, the Swedish government, and many other governments to remove it. After Sweden ratified the Intellectual Property Rights Enforcement Directive (IPRED) in 2009 (Burkart, 2014), The Pirate Bay launched a virtual private network service designed to encrypt its users' communications. As Peter Sunde explained, its service helped its users "to hide from what the government does in the form of giving companies police powers" (quoted in Tay, 2009, paragraph 22). After The Pirate Bay's administrators' trial ended, those in control of The Pirate Bay began moving its domain regularly so it could not be seized (Ernesto, 2012). Each switch changes the national jurisdiction that antipirate organizations need to navigate in order to finally shutter the site. The Pirate Bay has also recently launched its own branded version of the open-source Firefox browser along with the TOR anonymity client to allow its users to circumvent state censorship (Dredge, 2013; see also Bodó in this Special Section).

While the successes of the various Pirate parties have been limited thus far (see Jääsaari & Hildén in this Special Section), engaging with political institutions in the era of Snowden and WikiLeaks' revelations about an overreaching surveillance state could produce fruit. In Sweden, following the growth of the Swedish Pirate Party in 2006, candidates from various other political parties said publicly that they did not think file-sharing should be illegal (Kudinoff, 2006). More recently, Pirate parties have begun collaborating on translating the ideas of p2p networks in their party organizations though delegative democracy—or "liquid democracy." The project has inspired the European Union–funded D-Cent (Decentralized Citizens ENgagement Technologies) project to create open direct democracy tools for political parties, which will support further development and experimentation with new forms of political

organization. (For more details, see its website: http://dcentproject.eu/.)

Conclusion: Weary Giants of Flesh and Steel?

Our article argues that the act of piracy is not simply a matter of property theft, but rather, illustrates the development of a cohesive resistance to the power of the state. From the commercial ambitions of Napster and Kazaa to the crypto-anarchism of MojoNation to the overt activism of The Pirate Bay, these different forms of piracy have developed and popularized communication technologies that undermine the authority of the state. In other words, whether for profit or for political reasons, pirates have focused on undermining the legibility and regulability of networks.

Focusing on the relationship between piracy and the state helps answers the simple, but perplexing, question: What is piracy? It is a question at the center of studies of piracy and activism. For instance, the roundtable discussion in this volume's companion special issue of *Popular Communication* asked its participants to distinguish between hacker/tinker and pirate political formations (Andersson Schwarz et al., 2015). In the same roundtable discussion, Kelty suggested that piracy was primarily an economic practice that is "deflected into either hacking/activism or hacking/piracy" (Andersson Schwartz et al., 2015, p. 97). The familiar history in this article suggests that many of the p2p file-sharing applications and protocols—what Coleman called "weapons of the geek" at the roundtable and in other writing (e.g., Coleman, 2014)—have been inherently ambiguous in their distinction between piracy and activism.

Indeed, MojoNation and BitTorrent were designed to be illegible to the state (at least at the time) in that they simultaneously aimed to allow unaccountable sharing and to enact political resistance to the daily operations of the state. More so, the attention to the state as an invested actor also illuminates how certain practices become deflected into either activism or piracy. Certainly, the rhetoric of piracy allows for the state to both delegitimize some forms of communication as simply about theft, while also justifying its authority by quelling threats to intellectual property. In this way, the state is an important part of what Johns (2013) has called "the intellectual property defense industry," and, given the disclosures of U.S. lobbying in Sweden relating to The Pirate Bay (Burkart, 2014), perhaps the most important player in this industry of intellectual property defense. The state's legitimacy seems consummately tied to the protection of intellectual property.

The emphasis on the state also points to one of the most interesting developments of Pirate Politics, the application of p2p file-sharing practices to the administration of political parties. In the roundtable discussion, Burkart points to the German Pirate Party's experiments with the creation of a liquid democracy (Andersson Schwarz et al., 2015, p. 96). While that experiment might seem to be ending with the decline of the party's fortunes in Germany (see Jääsaari & Hildén in this Special Section), these experiments have led to the international EU-funded D-CENT project.

A project such as D-CENT might seem odd for pirates were it exclusively a concern over free copying. However, as a confrontation with the state, D-CENT remains an important manifestation of piracy's obsession with the state and is a trend to watch in the future. Certainly, endeavors such as D-

CENT may be more the future than what seems to be the lingering corpse of The Pirate Bay—shut down, copied, and now seemingly resurrected in hopes of recapturing its past popularity. (For a broader discussion of these issues, see McKelvey, forthcoming.)

If these projects prove unsuccessful in changing the relationship of the state to pirates, then the future of piracy remains in doubt. The state has largely been reluctant to exert its full power against pirate opponents, mostly convicting them of copyright evasion. However, the response by the U.S. government to major online activists—such as convicting army private Chelsea Manning (formerly Bradley) of espionage, government-sanctioned digital attacks on hacktivists, charging former National Security Agency employee Edward Snowden with treason, and the harsh prosecution of those believed to administer The Pirate Bay—indicates that these giants of flesh and steel may not yet be that weary after all.

References

Adar, E., & Huberman, B. A. (2000). Free riding on Gnutella. *First Monday*, *5*(10). Retrieved from http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/792/701

Alexa. (2015a, February 17). Site overview: kickass.so [Web listing]. Retrieved from http://www.alexa.com/siteinfo/kickass.so

Alexa. (2015b, February 17). Site overview: thepiratebay.se [Web listing]. Retrieved from http://www.alexa.com/siteinfo/thepiratebay.se

Allen, K. (2009, September 28). Pirate Party fires broadside at German political establishment. *The Local (de)*. Retrieved from http://www.thelocal.de/20090928/22209

Allen-Robertson, J. (2013). *Digital culture industry: A history of digital distribution*. New York: Palgrave Macmillan.

Andersen, B., & Frenz, M. (2007). *The impact of music downloads and p2p file-sharing on the purchase of music: A study for Industry Canada*. Retrieved from http://www.ic.gc.ca/epic/site/ippd-dppi.nsf/en/h_ip01456e.html

Andersson Schwarz, J. (2014). *Online file sharing: Innovations in media consumption*. New York, NY: Routledge.

Andersson Schwarz, J., Burkart, P., Aufderheide, P., Jaszi, P., Kelty, C., & Coleman, G. (2015). Piracy and social change: Roundtable discussion. *Popular Communication 13*(1), 87–99. doi:10.1080/15405702.2014.978003

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: Freedom and the future of the Internet*. New York, NY: OR Books.

Austin, G. W. (2005). Importing Kazaa—Exporting Grokster. *Santa Clara Computer and High Technology Law Journal*, *22*(3), 577–619. Retrieved from http://digitalcommons.law.scu.edu/chtlj/vol22/iss3/7

Barlow, J. P. (1996, February 8). A declaration of the independence of cyberspace [Online manifesto]. Davos, Switzerland. Retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

Baym, N. K. (2011). The Swedish model: Balancing markets and gifts in the music industry. *Popular Communication*, *9*(1), 22–38. doi:10.1080/15405702.2011.536680

BBC. (2013, April 28). Iceland opposition wins election. *BBC*. Retrieved from http://www.bbc.co.uk/news/world-europe-22320282

Bettig, R. (1997). The enclosure of cyberspace. *Critical Studies in Mass Communications*, *14*(2), 138–158. doi:10.1080/1529503970936700

Bey, H. (2001). The temporary autonomous zone. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 401–434). Cambridge, MA: MIT Press.

Beyer, J. L. (2014a). The emergence of a freedom of information movement: anonymous, WikiLeaks, the pirate party, and Iceland. *Journal of Computer-Mediated Communication 19*(2): 141–154. doi:10.1111/jcc4.12050

Beyer, J. L. (2014b). *Expect us: Online communities and political mobilization*. New York, NY: Oxford University Press.

Bhattacharjee, S., Gopal, R. D., & Sanders, G. L. (2006). Digital music and online sharing: software piracy 2.0? *Communications of the ACM*, *46*(7), 107–111. doi:10.1145/792704.792707

Biddle, P., Engl, P., Peinado, M., & Willman, B. (2002). *The darknet and the future of content distribution*. Retrieved from http://msl1.mit.edu/ESD10/docs/darknet5.pdf

Boyle, J. (2003). The second enclosure movement and the construction of the public domain. *Law and contemporary problems*, *66* (Winter–Spring), 33–74.

Braman, S. (2007). *Change of state: Information, policy, and power*. Cambridge, MA: MIT Press.

Burkart, P. (2010). *Music and cyberliberties*. Middletown, CT: Wesleyan University Press.

Burkart, P. (2014). *Pirate politics: The new information policy contests*. Cambridge, MA: MIT Press.

Burkart, P., & McCourt, T. (2006). *Digital music wars: Ownership and control of the celestial jukebox*. Lanham, MD: Rowman & Littlefield.

Cave, D. (2000, October 9). The mojo solution. *Salon*. Retrieved from http://www.salon.com/technology/view/2000/10/09/mojo_nation/index.html

Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). Freenet: A distributed anonymous information storage and retrieval system. In H. Federrath (Ed)., *International workshop on designing privacy enhancing technologies: Design issues in anonymity and unobservability* (pp. 46–66). New York, NY: Springer-Verlag.

Coleman, G. (2013). *Coding freedom: The ethics and aesthetics of hacking*. Princeton, NJ: Princeton University Press.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso Press.

David, M. (2010). *Peer to peer and the music industry: The criminalization of sharing*. Thousand Oaks, CA: SAGE Publications.

Dredge, S. (2013, October 21). Pirate Bay's piratebrowser Web browser reaches 1m downloads. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2013/oct/21/pirate-bay-piratebrowser-1m-downloads

Dyer-Witheford, N. (2002). E-capital and the many-headed hydra. In G. Elmer (Ed.), *Critical perspectives on the Internet* (pp. 129–164). Lanham, MD: Rowman & Littlefield.

Erlingsson, G. Ó., & Persson, M. (2011). The Swedish Pirate Party and the 2009 European parliament election: Protest or issue voting? *Politics*, *31*(3), 121–128. doi:10.1111/j.1467-9256.2011.01411.x

Ernesto. (2011, September 18). Pirate Party enters Berlin parliament after historic election win. *TorrentFreak*. Retrieved from http://torrentfreak.com/pirate-party-enters-berlin-parliament-after-historical-election-win-110918

Ernesto. (2012, February 1). The Pirate Bay moves to .se domain to prevent domain seizure. *TorrentFreak*. Retrieved from http://torrentfreak.com/the-pirate-bay-moves-to-se-domain-prevent-domain-seizure-120201

Ernesto. (2014, January 4) Top 10 most popular torrent sites of 2014. *TorrentFreak*. Retrieved from

http://torrentfreak.com/top-10-popular-torrent-sites-2014-140104

Ernesto. (2015, January 4) Top 10 most popular torrent sites of 2015. *TorrentFreak*. Retrieved from
       https://torrentfreak.com/top-popular-torrent-sites-2015-150104

Falkvinge, R. (2012, April 17). Austrian Pirate Party wins first seat, makes frontpage news [Web log
       message]. Retrieved from http://falkvinge.net/2012/04/17/austrian-pirate-party-wins-first-seat-
       makes-frontpage-news/

Gillespie, T. (2007). *Wired shut: copyright and the shape of digital culture*. Cambridge, MA: MIT Press.

Greenberg, A. (2012). *This machine kills secrets: How WikiLeakers, cypherpunks and hacktivists aim to
       free the world's information*. New York, NY: Dutton.

Hoffman, L. J. (1995). *Building in big brother: the cryptographic policy debate*. New York, NY: Springer.

Hughes, E. (1993, March 9). A cypherpunk's manifesto [Web log message]. Retrieved from
       http://www.activism.net/cypherpunk/manifesto.html

Johns, A. (2009). Piracy as a business force. *Culture Machine*, 10, 44–63. Retrieved from
       http://www.culturemachine.net/index.php/cm/article/view/345/348

Johns, A. (2010). *Piracy: The intellectual property wars from Gutenberg to Gates*. Chicago, IL: University
       of Chicago Press.

Johns, A. (2013). The information defense industry and the culture of networks. *Amodern*, 2. Retrieved
       from http://amodern.net/article/the-information-defense-industry-and-the-culture-of-networks/

Jones, B. (2012, October 22). First pirate party senator elected in the Czech Republic. *TorrentFreak*.
       Retrieved from http://torrentfreak.com/first-pirate-party-senator-elected-in-the-czech-republic-
       121022/

Kan, G. (2001). Gnutella. In A. Oram (Ed.), *Peer-to-peer: Harnessing the power of disruptive technologies*
       (pp. 94–122). Sebastopol, CA: O'Reilly.

Kelty, C. (2008). *Two bits: The cultural significance of free software*. Durham, NC: Duke University Press.

Kudinoff, T. (2006, June 7). Nu vänder v och m i piratfrågan [Now V and M parties change their opinions
       on piracy]. *Expressen*. Retrieved from http://www.expressen.se/nyheter/nu-vander-v-och-m-i-
       piratfragan/

Kushner, D. (2004, February 5). The world's most dangerous geek. *Rolling Stone*, *941*, 44–46.

Land, C. (2007). Flying the black flag: Revolt, revolution and the social organization of piracy in the "golden age." *Management and organizational history*, *2*(2), 169–192. doi:10.1177/1744935907078726

Landes, W., & Lichtman, D. (2003). Indirect liability for copyright infringement: Napster and beyond. *Journal of economic perspectives*, *17*(2)*,* 113–124. Retrieved from http://www.jstor.org/stable/3216860

Leeson, P. T. (2007). An-arrgh-chy: The law and economics of pirate organization. *Journal of Political Economy*, *115*(6), 1049–1094. doi:10.1086/526403

Lessig, L. (2006). *Code: Version 2.0*. New York, NY: Basic Books.

Levy, S. (1993). Crypto rebels. *Wired*. Retrieved from http://archive.wired.com/wired/archive/1.02/crypto.rebels_pr.html

Levy, S. (2002). *Crypto: Secrecy and privacy in the new code war*. London: Penguin.

Leyshon, A. (2003). Scary monsters? Software formats, peer-to-peer networks, and the spectre of the gift. *Society and Space*, *21*(5), 533–558. doi:10.1068/d48j

Libbenga, J. (2007, January 12). The pirate bay plans to buy Sealand. *The Register*. Retrieved from http://www.theregister.co.uk/2007/01/12/pirate_bay_buys_island/

Ludlow, P. (Ed.). (2001). *Crypto anarchy, cyberstates, and pirate utopias*. Cambridge, MA: MIT Press.

May, T. C. (1992, November 22). The crypto anarchist manifesto [Electronic mailing list message]. Retrieved from http://www.activism.net/cypherpunk/crypto-anarchy.html

McCullagh, D. (2000, July 29). Get your music mojo working. *Wired.* Retrieved from http://www.wired.com/science/discoveries/news/2000/07/37892

McKelvey, F. (2012). *Internet routing algorithms, transmission and time: toward a concept of transmissive control* (Unpublished doctoral dissertation). Ryerson University, Toronto.

McKelvey, F. (forthcoming). We like copies, just don't let the others fool you. *Television and New Media.* doi:10.1177/1527476414542880

Migdal, J. S. (2001). *State in society: Studying how states and societies transform and constitute one another*. New York, NY: Cambridge University Press.

Mojo Nation. (2000, August 15). *What it is*. Retrieved from http://web.archive.org/web/20000815205054/http://www.mojonation.net/whatitis.html

Moore, B. (1966). *Social origins of dictatorship and democracy: lord and peasant in the making of the modern world*. Boston, MA: Beacon Press.

Morris, J. W. (2015). Anti-market research: Piracy, new media metrics, and commodity communities. *Popular Communication. 13*(1), 32-44. doi:10.1080/15405702.2014.977998

Nordenfur, A. (2014, September 24). Alex Arnold becomes the first elected pirate mayor. *Pirate Times*. Retrieved from http://piratetimes.net/alex-arnold-becomes-the-first-elected-pirate-mayor/

O'Hear, S. (2014, March 2). Inside the billion-dollar hacker club. *TechCrunch*. Retrieved from http://techcrunch.com/2014/03/02/w00w00/

Oram, A. (Ed.). (2001). Peer-to-peer: Harnessing the benefits of a disruptive technology. Sebastopol, CA: O'Reilly.

Plambeck, J. (2010, May 12). Court rules that Limewire infringed on copyrights. *New York Times*. Retrieved from http://www.nytimes.com/2010/05/13/technology/13lime.html

Polanyi, K. (2001). *The great transformation: The political and economic origins of our time.* Boston, MA: Beacon Press. (Original work published 1944)

Raymond, E. S. (2001). *The cathedral and the bazaar: Musings on Linux and open source by an accidental revolutionary*. Sebastopol, CA: O'Reilly.

Sandvine Inc. (2014). *A proud history of innovation*. Retrieved from https://www.sandvine.com/downloads/general/company/sandvine-a-proud-history-of-innovation.pdf

Schiller, D. (1999). *Digital capitalism: Networking the global market system*. Cambridge, MA: MIT Press.

Scott, J. C. (1999). *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.

Scott, J. C. (2009). *The art of not being governed: An anarchist history of upland Southeast Asia*. New Haven, CT: Yale University Press.

Söderberg, J. (2010). Misuser inventions and the invention of the misuser: Hackers, crackers and filesharers. *Science as Culture*, *19*(2), 151–179. doi:10.1080/09505430903168177

Spilker, H. S., & Hoier, S. (2013). Technologies of piracy? Exploring the interplay between commercialism and idealism in the development of mp3 and divx. *International Journal of Communication*, *7*, 2067–2086. doi:1932–8036/20130005

Stallman, R. (2002). *Free software, free society: Selected essays of Richard M. Stallman*. Boston, MA: GNU Press.

Sterling, B. (1992). *The hacker crackdown: Law and disorder on the electronic frontier*. New York, NY: Bantam Books.

Strangelove, M. (2005). *The empire of mind: Digital piracy and the anti-capitalist movement*. Toronto, Canada: University of Toronto Press.

Tay, L. (2009, August 4). Pirate Bay's IPREDator not a place to hide. *ITNews for Australia*. Retrieved from http://www.itnews.com.au/News/151988,pirate-bays-ipredator-not-a-place-to-hide.aspx

Tetzlaff, D. (2000). Yo-ho-ho and a server of warez: Internet software piracy and the new global information economy. In A. Herman & T. Swiss (Eds.), *The World Wide Web and contemporary cultural theory* (pp. 99–126). New York, NY: Routledge.

Thompson, C. (2005, January). The BitTorrent effect. *Wired*. Retrieved from http://www.wired.com/wired/archive/13.01/bittorrent.html

Vaidhyanathan, S. (2004). *The anarchist in the library: How the clash between freedom and control is hacking the real world and crashing the system*. New York, NY: Basic Books.

Voegt, K. D. (2013, May 22). PP Croatia reaches 21% in city district, winning two out of nine board seats. *PirateTimes*. Retrieved from http://piratetimes.net/croatia-election-success

Wilson, P. L. (2003). *Pirate utopias: Moorish corsairs and European renegadoes*. Brooklyn, NY: Autonomedia.

Wu, T. (2003). When code isn't law. *Virginia Law Review*, *89*(4), 103–170. doi:10.2307/3202374

Zimmermann, P. (1999). Why I wrote pgp [Web log message]. Retrieved from https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html