UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Piracy Versus Privacy: An Analysis of Values Encoded in the PirateBrowser

Bodó, B.

Publication date
2015
Document Version
Final published version
Published in
International Journal of Communication : IJoC
License
CC BY-NC-ND

Link to publication

Citation for published version (APA):
Bodó, B. (2015). Piracy Versus Privacy: An Analysis of Values Encoded in the PirateBrowser. *International Journal of Communication : IJoC*, *9*, 818-838. http://ijoc.org/index.php/ijoc/article/view/3789

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:05 Sept 2026

International Journal of Communication 9(2015), 818–838 1932–8036/20150005

IJoC Piracy & Social Change

Piracy Versus Privacy: An Analysis of Values Encoded in the PirateBrowser

BALÁZS BODÓ
University of Amsterdam, Institute for Information Law
The Netherlands

The PirateBrowser is a Web browser that uses Tor privacy-enhancing technology to circumvent nationally implemented Internet filters blocking access to The Pirate Bay. This article analyzes the possible consequences of a mass influx of copyright pirates into the privacy domain. The article addresses the effects of the uptake of strong privacy technologies by pirates on copyright enforcement and on free speech and privacy technology domains. Also discussed are the norms and values reflected in the specific design choices taken by the developers of the PirateBrowser.

Keywords: piracy, privacy, Tor, privacy-enhancing technologies, policy

Introduction

Tor (The Onion Router), "endorsed by Egyptian activists, WikiLeaks, NSA, GCHQ, Chelsea Manning, Snowden" (Dingledine & Appelbaum, 2013), is a volunteer network of computers that relays Web traffic through itself to provide anonymous, unobserved, and uncensored access to the Internet. It has about 4,000 relays and about 1,000 exit nodes. Tor users connect to the network, and their Web traffic is channeled through the internal relays to reach its final destination through one of the exit nodes. This arrangement makes the identification and surveillance of Tor users difficult. Anonymity is promised by the difficulty of tracing the Web traffic that appears on the exit node back to the individual who initiated the traffic, as long as there is a sufficient number of internal hops in between. Protection from surveillance is granted by the fact that each link in the communication chain is encrypted. Tor anonymizes individuals and shields them from monitoring efforts. It also enables them to circumvent Internet blocks and filters if traffic exits the network through an exit node that is located in a country that does not IP-block (or filter) the Internet.

Work on Tor began in the mid-1990s, and its importance was recognized by a number of grants by the U.S. Defense Advanced Research Projects Agency and the U.S. State Department. Since 2002, a

Balázs Bodó: bodo@uva.nl
Date submitted: 2015–02–10

Copyright © 2015 (Balázs Bodó). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.

nongovernmental organization has coordinated the development of the open-source software project, but as of 2012, various U.S. government agencies still accounted for 60% of its budget. Tor and other privacy-enhancing technologies (PETs) are essential for governments to conduct sensitive communication.[1] They also have important civilian uses: Privacy-sensitive ordinary citizens (Maass, 2013), journalists, whistle-blowers, the business community, and dissidents in oppressive societies (Morozov, 2012) all have a legitimate reason (Marx, 1999) to rely on technological tools that provide strong anonymity and shield them from surveillance.

By 2012, Tor had developed into a technologically excellent but slightly marginal service, which was used by fewer than a million users daily. This number showed almost no growth during 2012 and most of 2013. However, in August 2013, the number of Tor users suddenly quintupled.

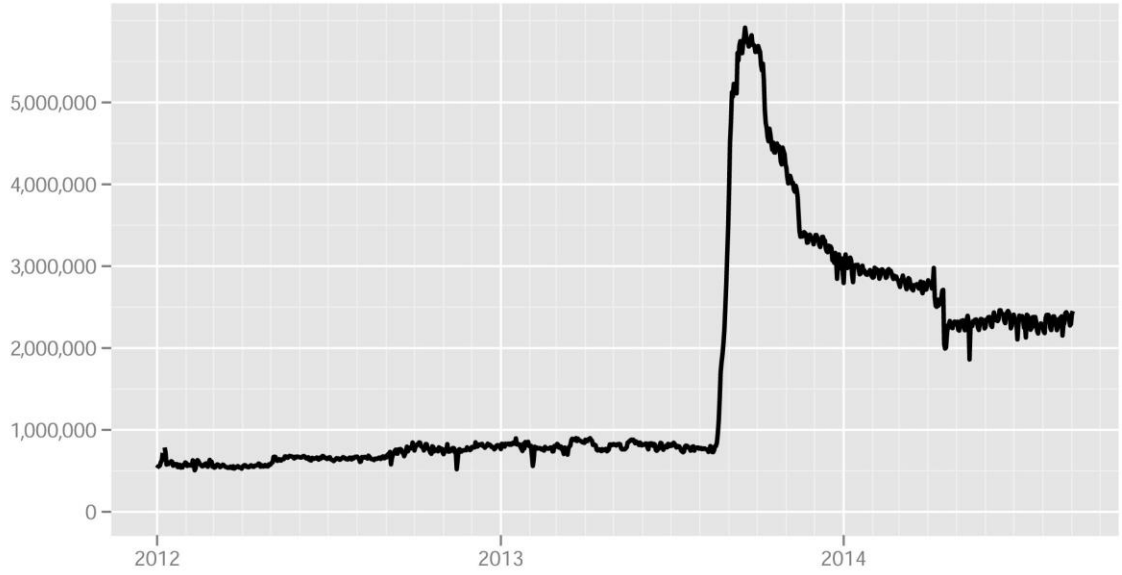

Figure 1. The number of users directly connecting to the Tor network between January 1, 2012, and September 2, 2014. Source: The Tor Project, Inc. (https://metrics.torproject.org)

This sudden rise in the number of users seemingly looking for privacy, anonymity, and uncensored Internet access coincided with several events: the "summer of Snowden," which included the revelations of whistle-blower Edward Snowden on the extent of governmental surveillance of online communications ("The NSA Files," 2013) and the subsequent debate over the legality of U.S. National Security Agency practices; an increased scrutiny of private data broker firms' data collection activities (Rockefeller, 2013); an FBI investigation that de-anonymized many Tor users who visited the hidden

[1] As Peter Dingledine, one of Tor's lead developers, puts it, even "censors need an anonymity system in order to censor their Internet" (Dingledine & Appelbaum, 2013).

services[2] hosted at Freedom Hosting (Poulsen, 2013); the bust of Silk Road, a drug marketplace, and one of the most prominent hidden services (Anderson & Farivar, 2013); and the appearance of a massive computer botnet that used the Tor network to control millions of infected machines (Dingledine, 2013).

The second half of 2013 was a tumultuous period in the history of online privacy, and Tor played a central role in it. Despite the bust of several hidden services, Tor is a simple and effective technology to achieve reasonable levels of online anonymity, privacy, and uncensored access to the Internet. It fills the void left by inadequate legal instruments and the lack of will from private and governmental parties to provide the aforementioned freedoms.

On August 10, 2013, in the middle of the Snowden scandal, The Pirate Bay (TPB) released—for its 10th anniversary—a piece of software called the PirateBrowser, tagged with the headline: "No more censorship!" ("PirateBrowser," 2013). The PirateBrowser is a modified version of the official Tor Web browser, and it uses the Tor network to provide uncensored access to TPB and other piratical websites in countries where access to these sites is blocked.[3] The PirateBrowser soon became immensely successful: In the its first 10 months, it was downloaded more than 5 million times (Ernesto, 2014).

Copyright infringement may not be the most noble, justified, or relevant application of the Tor network. In fact, many Tor servers are configured to filter BitTorrent traffic as a precaution against the legal troubles caused by copyright violations and the technical difficulties caused by the BitTorrent protocol. The sheer number of PirateBrowser downloads, however, warrants special attention; the mass influx of copyright pirates may profoundly impact Tor—and, by extension, the future of digital freedoms.

Pirates framed their anticopyright-enforcement technology as an anticensorship tool, reanimating debates about the relationship between copyright protection and the freedom of expression. However, Tor is more than just an anticensorship technology. It is an essential tool in providing protection against private and governmental surveillance, and the arrival of millions of pirates into this technological domain may have long-lasting effects on Tor and on public perceptions of PETs.

In this article, we investigate how the future of digital freedoms may increasingly hinge upon a few technologies that are able to provide privacy effectively and stymie censorship efforts, even if other (legal and policy) approaches are unavailable or ineffective. Tor is engineered to perfection, but its public perception is hotly debated. The success of the PirateBrowser profoundly shapes the debates about who Tor users are, what Tor is used for, and whether Tor represents the right balance between security and freedom.

---

[2] Tor enables the setup of so-called hidden services, where neither the user nor the hidden service operator is able to learn the other's network identity. Many websites dealing in illegal wares use such hidden services to conduct business (Biryukov, Pustogarov, & Weinmann, 2013).

[3] Besides TPB, the PirateBrowser allows uncensored access of the following services: eztv.it, isohunt.com, kickass.to, bayimg.com, torrentcrazy.com, h33t.com, monova.org, bitsnoop.com, 1337x.org, fenopy.se, torrentz.eu, and proxy-ez.tv.

We begin with a discussion of the validity of pirates' censorship claims. Copyright enforcement and censorship have a long common history, in which copyright enforcement at the level of online intermediaries has opened a new chapter. Internet service providers (ISPs) and search engines are increasingly engaged in the filtering and blocking of piratical websites, and the PirateBrowser promises to circumvent those practices. We try to find the PirateBrowser's place in the current copyright enforcement landscape.

We also examine how the mass influx of pirates into Tor impacts the privacy debate. PETs, especially Tor, are in dire need of expanding their user bases, and the 5 million PirateBrowser downloads may help them to reach the tipping point and push these technologies into the mainstream. These potential users, however, come at a cost, because they may tilt the public understanding of the legitimacy of PETs in an unforeseen direction.

Finally, we discuss the default settings of the PirateBrowser, which are significantly different from the default settings of the official Tor Web browser. We discuss what these differences mean and how they may affect the long-term future of Tor.

Pirates and Censorship: A Long History in the Making

The latest move in copyright enforcement has been to enlist online intermediaries—ISPs and search engines—to help curb digital piracy. Conveniently situated between users and copyright infringing Web services, intermediaries are in the position to detect and block infringing acts. After long court battles in which intermediaries tried to fend off any legal liability for the copyright infringing actions of their customers, ISPs as well as search engines are now increasingly required to take steps to render infringement impossible (Angelopoulos, 2009, 2014). As a result, government-mandated or voluntary Internet filters block access to TPB and other piratical websites in countries such as Ireland, Belgium, Finland, Denmark, and Italy. The PirateBrowser uses the Tor network to circumvent these nationally implemented Web filters by relaying traffic to blocked websites via Tor exit nodes located in countries where no such filters exist.

The tagline of the PirateBrowser, which claims "no more censorship," suggests that copyright enforcement through website blocking is censorship, not substantially different from other forms of politically motivated censorship. The developers of the PirateBrowser clearly frame the PirateBrowser as the latest development in the long history of intellectual property enforcement and censorship.

The Conflict of Copyright and Free Speech in a Historical Context

The claim that copyright protection has adverse effects on the freedom of expression dates back to before the first copyright act, the 1709/10 Statute of Anne. Copyright pirates' claims that they are not just simple infringers but actually useful agents of freedom of expression date back to the 16th and 17th centuries, when censorship in Britain was partly enforced by the Stationers Company, which, in exchange for such censorship enforcement services, had the freedom to provide and enforce private copyrights (Feather, 1994; Pollard, 1916). The monopolies created by perpetual copyrights and the bans issued by

the censors severely limited the circulation of certain texts, and pirates were more than happy to step in and serve readers with counterfeit editions. Pirates also played a significant role as anticensorship agents in continental Europe, circumventing national economic and political controls over the production and distribution of texts, and disseminating the texts of the Reformation and the Enlightenment where they were banned (Darnton, 1982, 2003; Luther, 1545; Wittmann, 2004).

With the gradual development of modern copyright (Samuelson, 2002) and various free-speech guarantees, the link between the political and the economic control of the printing press was severed. In late-17th-century England, the arbitrary nature of both the print monopoly and of press censorship prompted intense debates over the freedom of the press and the ownership of texts (Rose, 1993, 2003). In these debates, the emerging intelligentsia fought simultaneously for its economic and political emancipation. The role of copyright reform was to secure control over the revenues generated by texts, while the abolishment of prior censorship could help political emancipation. The figure of the economically independent author, taking ex post responsibility for his printed words while having the chance to live by his pen, has served well for most of the last 300 years.

Over time, important legal instruments were developed to ensure that the economic controls imposed on the ownership and circulation of texts did not limit free speech. Such instruments include the protection of expressions (rather than the ideas behind them); the limited term of protection; the exhaustion and first-sale doctrines; and the development of a series of exceptions or limitations where no rights holder permission is needed (Nimmer, 1969).[4] Because copyright provides financial incentives to produce texts, many regard it as the "engine of free expression."[5]

Postmodern Constraints on the Free Circulation of Knowledge and Culture

The growing economic and political clout of copyright-based industries and the emergence of the Internet reanimated the old debates on censorship and copyright. There are growing worries that the concentration of copyright industries, the fact that profit maximization has become the dominant value, excessive pricing, the continuous expansion of the term of protection and of exclusive rights, the erosion of fair use, and other limitations may result in new types of censorship (Samuelson, 2002).

Politically conscious digital pirate movements repeat the claims of legal scholarship (Atkins & Mintcheva, 2006; Benkler, 2003; Coombe, 1998; Lessig, 2004, 2006) that the current copyright order may be in conflict with fundamental free-speech rights. This argument is raised in several domains:

- Unclear and/or inadequate fair-use provisions and limitations and exceptions may have chilling effects on creativity.

[4] In cases such as parody, pastiche, commentary, and criticism or in certain educational settings, usually no rights holder permission is needed to use a text. In continental law, such cases are usually spelled out, and in the common-law countries, the general framework of fair use makes such uses permissible.

[5] The term was used by the U.S. Supreme Court in *Harper & Row Publishers, Inc. v. Nation Enterprises* (1985).

- Certain enforcement measures, such as Digital Millennium Copyright Act (DMCA) notices, and Internet filtering may result in collateral censorship.[6]

- Overbroad copyright protections may result in widespread market inaccessibility, effectively a form of economic censorship.

The legal scholarship of the last decade has focused on the chilling effects of copyright, where creative production by amateurs as well as professionals is hindered by legal limitations on building upon preexisting works (Lessig, 2004). Although such a practice is in theory legitimate and justified, in reality it is routinely contested by rights holders. Beyond the negative consequences on new cultural production (self-censorship), copyright enforcement may affect the circulation of already existing works. False copyright claims are used to silence critical voices, opposition, competition, and commentary (Electronic Frontier Foundation, 2013; Seltzer, 2010; Von Lohmann, 2010). Much content is suspected to be misidentified by the algorithmic "piracy surveillance" (Katyal, 2004) agents operating without human oversight, and censored erroneously.

Collateral censorship (Meyerson, 1995; Mulligan, 2013) is an unintended consequence of the legal liability of online intermediaries in the copyright domain. Because online intermediaries are only immune from being liable for the infringement of their users if they take steps to stop infringement upon notification from rights holders, they have an incentive to err on the side of caution. When the alternative is to review rights holders' claims individually, intermediaries minimize their costs and liability risks by removing content that otherwise would be covered by fair use and copyright exceptions.

Economic censorship, on the other hand, is the effect of certain market structures and the economics of information production on the market availability of copyrighted works. The classic definition of economic censorship covers cases where media companies and news organizations are pressured by their advertisers to drop certain topics (Richards & Murphy, 1996). Economic censorship in the copyright domain also has the effect of certain texts disappearing from the marketplace of ideas, but in this case the logics of cultural production and distribution and the way cultural markets are organized are to blame. The current catalog of publicly sold copyrighted works is shaped by several factors, including: (expected) demand; production and distribution costs; resources available to the rights holders; and the (geographic) density of the distribution network. Any of these factors can render a work commercially unavailable, creating gaps of varying sizes between supply and demand. Unmet market demand creates the perfect conditions for the emergence of gray and black markets, which illegally provide for what the legal alternatives cannot or would not (Bodó & Lakatos, 2012). There is ample evidence that the copyright

[6] The Digital Millennium Copyright Act in the United States and the E-commerce Directive in the European Union both introduced safe-harbor provisions for online intermediaries regarding the copyright infringements committed by their users. They are not liable for such acts if, upon the notification by rights holders, they promptly take the appropriate steps to stop the infringement.

system in its current form creates an immense number of orphan works (Covey, 2005; Mousner, 2007) and an even larger group of out-of-print works (Heald, 2007, 2013).[7]

There is a significant difference between politically motivated censorship of texts and the unfortunate logic of the markets, but the effects of these distinct forces are virtually indistinguishable: Some texts are only available through the black markets (if at all). In recent years, it also has become increasingly difficult to distinguish the technological tools that political censors and copyright enforcers rely on. The same software filters, firewalls, and technologies that enable the blockage of certain "objectionable" content, such as pornography, "extremist and terrorist related content," and "esoteric material" (Killock, 2013, para. 8) in the United Kingdom, are used to filter copyright infringing websites.

Courts' Assessment of the Balance of Copyright Protection and Free-Speech Rights

Despite the concerns of academics (Coombe, 1998; Karaganis, 2011), activists (La Quadrature du Net, 2011), and pirate parties, and despite the red flags raised by the mass phenomenon of piracy itself, courts that were asked to assess the current balance of free speech and copyright found no reason to interfere with the status quo.

In the United States, Lawrence Lessig has led a long legal fight against retroactive term extension. The case (*Golan v. Holder*, 2012*)* reached the U.S. Supreme Court. The question there was whether the retroactive extension of the term of copyright protection, and the removal of works from the public domain, would be a breach of First Amendment rights. While the Justices acknowledged that intellectual property protection has relevance in the free-speech domain, they found that, as long as the free speech safeguards (the fair use exceptions and the idea/expression dichotomy) are not changed by Congress, their current balance is satisfactory.

At the European Court of Human Rights (ECtHR), the administrators of TPB, who were convicted by the Swedish court on copyright infringement grounds, sought free-speech protection for sharing copyrighted works.[8] The ECtHR reaffirmed[9] that copyrights may have adverse effects on free-speech

[7] *Orphan works,* as defined by paragraph (3) of the 2012/28/EU Directive on Orphan Works, are "works and other subject matter which are protected by copyright or related rights and for which no rights holder is identified or for which the rights holder, even if identified, is not located." The European Commission's Memorandum of Understanding on Key Principles on the Digitization and Making Available of Out-of-Commerce Works (2011) defines *out-of-commerce works* as "works that are still protected by copyright but are no longer commercially available because the authors and publishers have decided neither to publish new editions nor to sell copies through the customary channels of commerce."

[8] *Fredrik NEIJ and Peter SUNDE KOLMISOPPI against Sweden* (2013).

[9] The case—ECtHR (5th section) *Ashby Donald and Others v. France,* Appl. nr. 36769/08)—was the first to establish that "a conviction based on copyright law for illegally reproducing or publicly communicating copyright protected material can be regarded as an interference with the right of freedom of expression and information under Article 10 of the European Convention" (Voorhoof & Høedt-Rasmussen, 2013, para. 2).

rights. It also established that operating a site that facilitates file sharing is covered by the right to "receive and impart information" under Article 10 of the European Convention on Human Rights, even if those files being shared are copyright-protected and the facilitation takes place for profit-making purposes. In the judgment, however, it was stated that, because the protection of the right to share copyright-protected information "cannot reach the same level as that afforded to political expression and debate" (*Fredrik Neij and Peter Sunde Kolmisoppi Against Sweden*, 2013, para. 52) in this specific case, copyright holders' rights to the protection of their intellectual properties prevails. The conclusion that both Courts reached was that the current balance legislators and the judiciary struck between the two values does not justify intervention.

Pirates beg to disagree but so far have not been able to challenge the status quo directly. The release of the PirateBrowser is an attempt to change this situation.

Pirates and PETs

> In cyberspace, intellectual property and privacy are at an impasse. There is no way out—the enforcement of each area faces inherent conflicts with another. . . . The law has displayed a persistent failure to recognize that expansions of control of intellectual property cause tradeoffs in other areas of consumer protection—particularly where privacy is concerned. As a result, we have created a world in which the property rights of copyright owners are valued over the liberty, property, and privacy rights of others, suggesting that those principles are somehow less valuable than those involving commercial self-protection. (Katyal, 2004, p. 335)

The PirateBrowser demonstrates, in practice, this conflict.

Having exhausted every other option in the past decade, rights holders trying to curb digital piracy started to concentrate on Internet intermediaries: search engines and ISPs (Ginsburg, 2013). The ability to block infringing acts at the level of online intermediaries depends on their surveillance and filtering capacities. Infringing acts and users are detected, identified, and stopped through "piracy surveillance," and piratical websites are identified, located, and rendered inaccessible through "piracy filtering" (Katyal, 2004). PirateBrowser does not promise to defeat piracy surveillance, but it certainly hopes to defeat piracy filtering.

The PirateBrowser relies on the established Tor network to provide uncensored access to the Internet. This strategy of appropriating and repurposing networks and technologies that were designed with other, primarily nonpiratical goals in mind has had a curious side effect. The Tor network is used by a large number of people who rely on it to preserve their privacy, speak freely, and engage in practices that enjoy full legal and social support—at least in the West. Because it is impossible to single out pirates from all the others using the same Tor network, any copyright enforcement measure (such as a mandatory filtering of Tor exit nodes) will necessarily affect all Tor users.

Before the PirateBrowser, dedicated Web proxies made otherwise censored piratical websites accessible for users behind national Internet filters. By abandoning this strategy and releasing a tool that merges the copyright infringers with the privacy crowd, pirates raise and change the stakes of copyright enforcement. The consequence—which may not be altogether unintentional—of the PirateBrowser is that it effectively uses other, nonpiratical Tor users as human shields against copyright enforcement. The argument about whether copyright is a threat to free speech will become irrelevant if they manage to create a technological environment in which copyright enforcement is only possible through the surveillance and de-anonymization of others, who are assumed to be legitimately engaged in practicing their basic human rights to free speech and privacy.

The Debate on the Legitimacy of Tor

This shift in pirate tactics comes at a time when the future of privacy is intensely debated (Ball, Lyon, & Haggerty, 2012; Bauman & Lyon, 2013; Lyon, 2006). The pressure to reduce and eliminate obstacles to surveillance is enormous. Businesses need surveillance to extend their scientific management methods beyond production to consumption (Beniger, 1986). Media consumption has become a form of labor (Andrejevic, 2004) that can best be managed through the tight monitoring of consumers. Governments, operating in a permanent state of emergency, trying to fend off the constant and omnipresent threat of "terrorism," are incentivized to implement tools that enable the control of "time and space, present and future, here and there" (Bigo, 2006, p. 62). Moderating the massive impetus of these forces should be a task of laws that translate the abstract human rights enshrined in constitutions and universal declarations in a way that reflects upon the actual surveillance practices and trends of the 21st century. However, as established by the European Parliament resolution of March 12, 2014, on the U.S. NSA surveillance program, surveillance bodies in various member states, and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, this translation and the subsequent update of outdated privacy-protecting legal instruments entails enormous work yet to be done. Given the lack of effective legal instruments, the use of PETs became the most readily accessible and effective countersurveillance measure.

But PETs are clearly dual-use technologies. They are used to protect basic human rights *and* to commit hideous crimes. They are used by political dissidents *and* pirates, botnet operators *and* law enforcement agencies, ordinary citizens defending their constitutional right to privacy *and* child pornographers. PETs, such as Tor, either protect them all or protect no one. There is no middle ground, were one can single out the "bad" guys without compromising the "good" ones. In this context, the future of Tor and other dual-use PETs hinges upon the public's perception of what the primary use of these technologies is.

The developers and proponents of PETs understand this dilemma. As late as December 2013, the project leaders of Tor (Dingledine & Appelbaum, 2013) felt they needed to use their main-stage appearance at a prestigious hacker conference to counter the public perception that Tor is used by bad guys. The title *Online Anonymity Is Not Only for Trolls and Political Dissidents* and the defensive tone of the article published by the Electronic Frontier Foundation (Maass, 2013) on the legitimate uses of Tor

speak volumes about the challenges PET developers, proponents, and users face when the pros and cons of anonymity and privacy technologies are discussed.

Tor demonstrates the trade-off between freedom and security with brutal simplicity. It is designed to make law enforcement difficult, if not impossible. While it is easy to justify a tool that enables dissidents in oppressive societies to commit the unlawful but legitimate acts of political dissent, criticism, and self-expression, it is much harder to explain that this freedom comes at the cost of enabling more controversial practices, such as the free exchange of copyrighted works, leaking secrets to journalists, or the exchange of counterfeit goods (including drugs and weapons).

Because it is virtually impossible to control what the technology is used for, the debate will unavoidably need to focus on the control of the technology itself. Similar to so many other technology debates in the past, the debate on PETs should be about whether there are enough "legitimate uses" of a technology to warrant its own legitimacy and its legally protected status.[10]

It is difficult to assess the legal future of Tor. It is already blocked in some countries such as Iran, China, and Syria, because it enables practices that are illegal by the law of the land but which, from a Western point of view, are perfectly legitimate and are generally protected by universal declarations of human rights. There are no restrictions of Tor in many other countries, despite the fact that many of the practices that it enables are not only illegal but—as is the case with child pornography—justly cause universal moral outrage. So far, the potential benefits PETs provide have seemed to be greater than the perceived costs. However, Western governments already display a schizophrenic attitude toward Tor. By funding its development, the United States regards Tor as an indispensable tool in its quest of spreading digital freedoms (Morozov, 2012). At the same time, the United States spends billions of dollars on trying to crack the very same encryption it helped to make impenetrable. It is hard to imagine in the long run that a society would waive its right to prosecute acts that it deems objectionable. As it stands now, however, Tor is engineered to force just that. It is a government-sponsored technology that severely and deliberately limits the sovereign powers of the state (Bodó, 2011).

Until Western courts and legislators take up the issue of Tor, the debate will focus on the legitimate uses of PETs. The Snowden revelations uncovered the existence of massive, and in some cases probably illegal, government surveillance programs, demonstrating the lack of privacy in the digital domain and the limits of public oversight of government surveillance. In the current situation, Tor and similar PETs offer a prompt and effective countermeasure to surveillance, and they will continue to do so even if the political process eventually fails to guarantee the privacy of the individual in the digital domain. The countersurveillance capability of Tor provides a strong claim of legitimacy to the technology, as long as there is a consensus on the right to digital privacy. However, Tor is also a hotbed of controversial practices (Biryukov et al., 2013), and thus a recurring target of law enforcement. Various moral entrepreneurs ("The disturbing world," 2013) and incumbents (Hern, 2014), who have vested stakes in

[10] Virtually all electronic copying technologies, starting with the videocassette recorder in the famous *Sony Corp. of America v. Universal City Studios, Inc.* (1984) Betamax case, have been measured against this test by U.S. courts (Giblin, 2011).

ineffective countersurveillance technologies, try to turn public sentiment against PETs and Tor (Kelion, 2014), just as others tried to turn public sentiment against peer-to-peer (P2P) technologies (Lindgren, 2013; Patry, 2009). Because Tor is peer-produced and depends on volunteers to have enough nodes in the network, it is very sensitive to the loss of people trusting the network and sharing the resources necessary to fulfill its mission. A more general loss of faith in PETs, in terms of either their effectiveness or their being legitimate technologies to be used by everyday citizens, could be devastating for the cause of online privacy and other human rights in the digital era.

The influx of pirates into the PETs domain happens at a crucial point in this quest for legitimacy. In the next section, we dissect the specifics of the PirateBrowser to assess its impact on Tor and on the overall privacy debate.

The Tor Browser Bundle Versus the PirateBrowser

Tor is a network of computers mostly run by volunteers. Rather than accessing a website directly, users channel their Web traffic through the Tor network. They connect to one of the public entry points or through one of the semipublic bridges,[11] go through a number of hops in the network, and reach their desired Web destination through one of the nearly 1,000 exit nodes that connect the Tor network to the rest of the Internet.

Any browser can connect to the Tor client running on the user's computer, but there are preconfigured software bundles that do all the necessary tasks with a single and straightforward click. The official Tor Browser Bundle (TBB) has two major components. It contains a preconfigured Tor client that automatically connects to the network. The TBB also contains a stand-alone version of the popular Firefox browser, configured to access the Internet via the connection established by the Tor client.

The whole system can be fine-tuned to the specific needs and resources of the user, but the default configuration is such that the use of the software is simple and straightforward for even a technically naïve user, and no further tweaking is necessary to enjoy a reasonable level of online privacy. Tor developers defined a number of constraints to ensure a reasonable level of privacy. One such constraint is the minimum number of relays through which traffic needs to pass before exiting the network. Three internal hops are thought to provide a reasonable level of protection without serious restrictions on the speed of Internet access. The developers also advise against using relays that reside in the same Internet subnetwork, since the chances of de-anonymization are higher if this happens. They also keep track of trustworthy and untrustworthy exit nodes: ones that comply with the minimum security settings recommended for exit nodes, and the rest, which deviate from these settings and/or were caught

[11] Because the entry points to Tor are public, it is easy to block access to them. To solve this problem, volunteers can set up so-called bridges, the list of which is not maintained centrally. Although these bridges serve as entry points to the Tor network, their addresses are not made public, so there is less chance that access to these computers, and thus to the whole Tor network, is blocked by the ISP or the government.

doing things that may compromise users' security. These recommendations along with other settings are reflected in the configuration file that is loaded every time the Tor client is started.

The browser in the TBB has additional default settings to reduce the browser-based vulnerabilities. By default, the TBB does not record browsing history or website data; it disables browser plug-ins such as Flash, restricts third-party cookies and other tracking data, and makes sure that the browser's signature is indistinguishable from other Tor users' browser details. Additional extensions add extra layers of security. The HTTPS-Everywhere extension forces secure connections whenever possible, and the NoScript extension prevents potentially harmful JavaScript code from running. The browser is configured to channel all browser traffic through the Tor network.

The PirateBrowser is a software bundle in many aspects very similar to the Tor Browser Bundle. It is a prepackaged and preconfigured mix of a stand-alone Firefox Web browser and a Tor client. The differences between TBB and the PirateBrowser are not in their composition but in their configuration: The two software bundles are substantially different in their default settings.

The most important difference relates to the PirateBrowser's stated aim. To avoid TPB-related Internet filters, it has to ensure that exit nodes situated in countries where such blocks are present are avoided. At the time of writing, Denmark, Ireland, the United Kingdom, Belgium, Italy, China, Iran, Finland, and Norway were limiting access to some of the major file-sharing sites. These countries also host about 17% of all the exit nodes in the Tor network. Since the exit nodes are normally chosen by chance (taking into account the exit node's bandwidth, uptime, trustworthiness, etc.), TBB users with the default settings may run into blocks if the randomly chosen exit node happens to be in any of these countries. To make sure that this does not happen, the default settings of the PirateBrowser forbid the use of exit nodes in these countries.

Since no other adjustment is necessary for the PirateBrowser to fulfill its mission, differences could end there. However, they do not. The use of the Tor network comes at the cost of speed. The relays between the entry and exit nodes add 1.2 seconds of waiting time on average for any page to load. The default settings of the PirateBrowser are designed to reduce this overhead, but this can only be done at the expense of privacy and security. The PirateBrowser allows the use of exit nodes that permit direct connection to them. Direct connections to exit nodes greatly increase the risk of de-anonymization. Also, Tor developers advise against exit nodes that accept direct connection from users, because "these relays might be at higher risk of being seized or observed" (Tor Project, 2014, para. 118). The PirateBrowser allows the use of relays that are in the same subnetwork, which may reduce waiting times but again reduce the level of attainable privacy. The Firefox browser packaged in the PirateBrowser bundle lacks the additional privacy-boosting browser extensions of the TBB. Finally, rather than channeling all browser traffic through the Tor network, the browser is configured to do so only when any of the preconfigured torrent trackers are accessed. In all other cases, the traffic flows unencrypted through the regular Internet.

Because false assumptions about the safety may cost more than just annoyance, the developers of the PirateBrowser should communicate clearly about the limitations of their product. However, the

PirateBrowser website has been far from clear on this matter. On the censorship circumvention issue, they claim that

> PirateBrowser is a bundle package of the Tor client (Vidalia), Firefox Portable browser (with foxyproxy addon) and some custom configurations that allows you to circumvent censorship that certain countries such as Iran, North Korea, the United Kingdom, the Netherlands, Belgium, Finland, Denmark, Italy and Ireland impose onto their citizens. ("PirateBrowser," 2013, para. 1)

However, the differences between the nature of online censorship in Iran and in Denmark are quite substantial. Although it may be true that all of these countries block access to TPB, the promise that the PirateBrowser would beat Iranian Internet censorship is not just false, it is outright reckless.

The issue of anonymity and privacy is addressed in the brief FAQ section of the website:

> Does it make me surf the net anonymously? No, it's not intended to be a TOR Browser, while it uses the Tor network, which is designed for anonymous surfing, this browser is ONLY intended to circumvent censorship. The Tor network is used to help route around the censoring/blocking of websites your government doesn't want you to know about. ("PirateBrowser," 2013, para. 5)

Although this description reinforces the misleading universal anticensorship claim, it remains silent on the exact nature of the differences between the Tor browser and the PirateBrowser. These differences are only apparent to those who compare the configuration files, buried deep in the installation folders, line-by-line to one another and to the Tor software documentation.

The PirateBrowser, in short, is configured to serve a single goal: to enable its users to reach TPB as fast as possible in countries where it is blocked and stand out of the way in every other case. Despite using Tor, it sacrifices security and anonymity for speed to the extent that it is hardly more secure than a plain Internet connection. Despite the bold claim of defeating censorship, it only circumvents the censorship of certain piratical websites and is useless in the case of all other censored websites.

The Potential Effects of the PirateBrowser on Tor

It is clear what pirates can expect from Tor: It beats piracy surveillance and piracy filtering in the short term, and it raises the stakes of copyright enforcement by letting pirates hide behind those Tor users whose acts enjoy more support than their own. It is less straightforward how the influx of pirates affects Tor. Two distinct logics are at work here, both impacting Tor in a nonlinear fashion. The direct effect of the PirateBrowser users on Tor has to do with the number of Tor users, to which the PirateBrowser users may contribute at a critical moment. Indirectly, the influx of pirates into the PETs domain may adversely affect the legitimacy of the privacy technology.

The direct effect of the PirateBrowser has to do with the number of regular Tor users. Tor is in constant need of more users. The law of network effects applies to this network as well: Any new user increases the value of the service to every other member. This rule applies both on the level of technology and in terms of the diffusion of technology.

Users who access the Tor network via the PirateBrowser may not be as well protected as the TBB users, but they do add to the traffic within the Tor network. For Tor to be effective, it needs large amounts of heterogeneous users, so that no single user or specific use would stand out. Every Tor user needs the crowd of others in which to hide and to cover their tracks. The pirates may increase the size as well as heterogeneity of the Tor user base. Tor is yet to cross the threshold of critical mass and develop into a mainstream technology. Pirates–turned–Tor users may be the technologically advanced, politically engaged, Internet freedom–conscious user base that Tor needs to get into the mainstream.

On the other hand, Tor is at the beginning of a struggle to establish itself as a legitimate tool to achieve a legitimate goal. PET proponents still need to counter basic arguments that try to normalize surveillance, such as the argument that only those who have something to hide fear surveillance and use PETs. PET proponents constantly need to demonstrate that online privacy is not a luxury demanded by a marginal group of exquisite users, but something that each and every Internet user should have.

The PirateBrowser has the indirect effect of interfering with this struggle. If the PirateBrowser reinforces the image that Tor and other PETs are primarily used to infringe on copyrights, traffic drugs, distribute child pornography, and commit other unlawful acts in general, then it will be much harder to argue that Tor and other PETs should be used by ordinary users who have "nothing to hide," and the norms and values expressed through technology are worthy of social, political, and legal recognition.

At the time of writing, it was not yet clear to what extent the PirateBrowser would affect the future of Tor and, by extension, the privacy debate. Between August 2013 and May 2014, there were 5 million PirateBrowser downloads. Between May 2013 and May 2014, there is said to have been 120 million Tor downloads (which include stand-alone Tor clients as well as the TBB) (Lewman, 2014). It has been shown (Dingledine, 2013) that at least part of this massive recent growth was due to a botnet that used Tor to communicate with its command and control servers.[12] Nevertheless, 1.5 million new users joined between mid-2013 and mid-2014. It is impossible to know how many of them are privacy-conscious users reacting to the endless stream of Snowden revelations and how many of them are pirates using the

[12] Botnets are malware-infected computers that can run any code on the command of the botnet masters. The computers of a botnet are coordinated through command and control (C&C) servers that effectively tell infected computers what to do. Because a botnet can be shut down by disabling (the access to) its C&C servers, protecting the servers from detection and interference is essential. According to the study conducted by (Biryukov et al., 2013) at the beginning of 2013, 6 out of the 10 most popular Tor hidden services at the time were, most likely, C&C servers for a botnet. In the months following August 2013, Microsoft stepped in and removed Tor from the botnet-infected machines. The results of this intervention can be seen in the sudden decline in the number of users, coinciding with the monthly release of Microsoft's tool to remove malicious software.

PirateBrowser. However, even if there are only a few PirateBrowser users among this group of 1.5 million, their direct and indirect impact is certainly greater than their actual numbers.

Conclusion

There could have been many different configurations of the PirateBrowser. It could have been a version of the TBB focused on anticensorship and configured to defeat all kinds of censorship and provide strong anonymity. This could have helped both pirates and nonpirates behind restrictive local and national firewalls. It could also have been a strictly piracy-focused tool that does not sacrifice anonymity and that defeats both piracy filtering and piracy surveillance. However, the developers of the PirateBrowser chose a third path by severely limiting both the countercensorship scope and the privacy protection ability of the technology.

Rather than fusing the copyright domain with the free-speech and privacy domains, the PirateBrowser separates the two. The way the software is configured and communicated sends the message that pirates are willing to appropriate the rich tradition of the anticensorship struggle and a highly complex technological system in an abusive manner to achieve the single goal of keeping TPB accessible.

The PirateBrowser is published under the misleading tagline "no more censorship!" The PirateBrowser is not a general anticensorship tool, and it only works under very specific conditions, in countries where access to TPB is blocked. Although such blocks are evidently ineffective for curbing piracy in the long run (Poort, Leenheer, van der Ham, & Dumitru, 2014), intermediary liability may reach a point where more effective and pervasive filters will be put in place, effectively blocking access not just to TPB but to other, non-copyright-infringing websites as well. Although collateral and economic censorship are real dangers, the PirateBrowser, as it stands now, is not the right tool to address these issues.

On the other hand, PETs like Tor are technologies that are already being used to circumvent sophisticated online surveillance and censorship mechanisms. There is, however, little use in creating a simplified version of this technology that offers less functionality and exposes its users to substantial risks. One of the main factors that contributed to copyright piracy's successful transformation into popular social movements enjoying considerable social (and political) support was the pirates' technological invincibility and the power that came with this invincibility. Through successive steps, they developed technologies that provided them with enough autonomy to challenge the status quo constantly (Giblin, 2011). The inability to enforce copyrights effectively put unbearable stress on the incumbents and slowly forced the change they were at first reluctant to embrace. As rights holders realized that the changes brought by piracy could not be stamped out, they had few options other than to embrace many of the ideas put forward by pirates on how culture should be made accessible.

The PirateBrowser is designated to keep up the pressure. Enforcement moved onto the online intermediaries, who are, in theory, well positioned to detect and filter infringing online acts. In response, the PirateBrowser was designed to render these latest enforcement efforts ineffective. However, the vision

behind the PirateBrowser does not manage to match its claims, nor the context in which it has placed itself.

When it comes to defeating online censorship, the PirateBrowser offers a short-term and rather rigid solution that becomes quickly outdated as the piracy filtering landscape changes. By aligning themselves with the privacy domain, pirates also need to understand their role in the privacy debate. As popular and legally immune P2P file-sharing technologies appear to have compelled copyright industry business practices to change (Andersson Schwarz, 2013), popular and legally immune PETs may force the recognition of the privacy standards expressed through technology. The PirateBrowser directly affects not just the technology but the diffusion and the public perception of PETs and, as a result, the discourses around privacy. Yet it seems that the developers of the PirateBrowser have yet to realize how their actions feed into this process.

References

Anderson, N., & Farivar, C. (2013, October 3). How the feds took down the Dread Pirate Roberts. *Ars Technica.* Retrieved from http://tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts

Andersson Schwarz, J. (2013). *Online file sharing: Innovations in media consumption*. New York, NY: Routledge.

Andrejevic, M. (2004). *Reality TV: The work of being watched*. Lanham, MD: Rowman & Littlefield Publishers.

Angelopoulos, C. (2009). Filtering the Internet for copyrighted content in Europe. *IRIS Plus*, *4,* 1–12.

Angelopoulos, C. (2014, April 3). CJEU in UPC Telekabel Wien: A totally legal court order . . . to do the impossible. *Kluwer Copyright Blog*. Retrieved from http://kluwercopyrightblog.com/2014/04/03/upc-telekabel-wien

Atkins, R., & Mintcheva, S. (2006). *Censoring culture: Contemporary threats to free expression*. New York, NY: New Press.

Ball, K., Lyon, D., & Haggerty, K. (Eds.). (2012). *Routledge handbook of surveillance studies*. New York, NY: Routledge.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Cambridge, UK; Malden, MA: Polity.

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge, MA: Harvard University Press.

Benkler, Y. (2003). Through the looking glass: Alice and the constitutional foundations of the public domain. *Law and Contemporary Problems*, *66*(1), 173–224.

Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 46–68). Cullompton, UK: Willan.

Biryukov, A., Pustogarov, I., & Weinmann, R. P. (2013). Content and popularity analysis of Tor hidden services. *CoRR*. Retrieved from http://arxiv.org/abs/1308.6768

Bodó, B. (2011). You have no sovereignty where we gather—Wikileaks and freedom, autonomy and sovereignty in the cloud. *SSRN Electronic Journal*. doi:10.2139/ssrn.1780519

Bodó, B., & Lakatos, Z. (2012). P2P and cinematographic movie distribution in Hungary. *International Journal of Communication*, *6*, 413–445.

Coombe, R. J. (1998). *The cultural life of intellectual properties: Authorship, appropriation, and the law*. Durham, NC: Duke University Press.

Covey, D. T. (2005). Re: Response to notice of inquiry about Orphan Works [Letter]. Washington, DC: U.S. Copyright Office. Retrieved from http://www.copyright.gov/orphan/comments/OW0537-CarnegieMellon.pdf

Darnton, R. (1982). *The literary underground of the old regime*. Cambridge, MA: Harvard University Press.

Darnton, R. (2003). The science of piracy: A crucial ingredient in eighteenth-century publishing. *Studies on Voltaire and the Eighteenth Century*, *12*, 3–29.

Dingledine, R. (2013, September 5). How to handle millions of new Tor clients [Web log post]. *Tor*. Retrieved from https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients

Dingledine, R., & Appelbaum, J. (2013, December). *The Tor network—We're living in interesting times*. Presentation at the 30C3 conference, Hamburg, Germany.

The disturbing world of the deep Web, where contract killers and drug dealers ply their trade on the Internet. (2013, October 11). *Daily Mail.* Retrieved from http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html

Electronic Frontier Foundation. (2013, March). *Unintended consequences: Fifteen years under the DMCA.* Retrieved from https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca

Ernesto. (2014, May 16). Pirate Bay's anti-censorship browser clocks 5,000,000 downloads. *TorrentFreak*. Retrieved from http://torrentfreak.com//pirate-bays-anti-censorship-browser-clocks-5000000-downloads-140516

European Commission. (2011). *Memorandum of understanding on key principles on the digitisation and making available of out-of-commerce works.* Retrieved from http://ec.europa.eu/internal_market/copyright/docs/copyright-infso/20110920-mou_en.pdf

European Parliament. (2014). *European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various member states and their impact on EU citizens' fundamental rights and on transatlantic cooperation in justice and home affairs, A7-0139/2014.* Brussels, Belgium.

Feather, J. (1994). *Publishing, piracy, and politics: A historical study of copyright in Britain*. New York, NY: Mansell.

Fredrik Neij and Peter Sunde Kolmisoppi against Sweden. Application no. 40397/12, ECHR Decision of the ECtHR (5th section). (2013).

Giblin, R. (2011). *Code wars: 10 Years of P2P software litigation*. Cheltenham, UK: Edward Elgar.

Ginsburg, J. C. (2013, December 30). Copyright enforcement in the EU: The return of website blocking. *The Media Institute*. Retrieved from http://www.mediainstitute.org/IPI/2013/123013.php

Golan v. Holder, 132 S.Ct. 873. (2012).

Harper & Row Publishers, Inc. v. Nation Enterprises, SCotUS Case No. 83-1632. (1985).

Heald, P. J. (2007). Property rights and the efficient exploitation of copyrighted works: An empirical analysis of public domain and copyrighted fiction best sellers. *UGA Legal Studies Research Paper,* no. 07-003.

Heald, P. J. (2013). How copyright makes books and music disappear (and how secondary liability rules help resurrect old songs). *Illinois Program in Law, Behavior and Social Science Research Papers*, no. 13.

Hern, A. (2014, August 21). Tor can handle Aphex Twin—but could it deal with Taylor Swift, like, ever? *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/aug/21/tor-aphex-twin-taylor-swift

Karaganis, J. (Ed.). (2011). *Media piracy in emerging economies*. New York, NY: SSRC Books.

Katyal, S. (2004). Privacy vs. piracy. *Yale Journal of Law and Technology*, *7*(1), 222–345.

Kelion, L. (2014, August 21). Tor Project's struggle to keep the "dark net" in the shadows. *BBC News*. Retrieved from http://www.bbc.com/news/technology-28886465

Killock, J. (2013, July 25). Sleepwalking into censorship [Web log post]. *Open Rights Group.* Retrieved from https://www.openrightsgroup.org/blog/2013/sleepwalking-into-censorship

La Quadrature du Net. (2011, March 11). French Constitutional Council Validates Internet Censorship. *La Quadrature du Net*. Retrieved from https://www.laquadrature.net/fr/node/4269

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. New York, NY: Penguin Press.

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

Lewman, A. (2014, May 26). *Sida.* Presentation for the 2014 Sida ICT Day, Stockholm, Sweden. Retrieved from https://svn.torproject.org/svn/projects/presentations/2014-05-26-Sida-Presentation.pdf

Lindgren, S. (2013). Pirate panics. *Information, Communication and Society*, *16*(8), 1–24.

Luther, M. (1545). "Warning to the printers," Wittenberg (1545). In L. Bently & M. Kretschmer (Eds.), *Primary sources on copyright (1450–1900)*. Cambridge, UK: University of Cambridge. Retrieved from http://copy.law.cam.ac.uk/record/d_1541

Lyon, D. (Ed.). (2006). *Theorizing surveillance*. Cullompton, UK: Willan.

Maass, D. (2013, October 29). Online anonymity is not only for trolls and political dissidents. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2013/10/online-anonymity-not-only-trolls-and-political-dissidents

Marx, G. T. (1999). What's in a name? Some reflections on the sociology of anonymity. *Information Society*, *15*(2), 99–112.

Meyerson, M. I. (1995). Authors, editors, and uncommon carriers: Identifying the speaker within the new media. *Notre Dame Law Review*, *71*(1), 79–125.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs.

Mousner, J. O. (2007). Copyright orphan works: A multi-pronged solution to solve a harmful market inefficiency. *Journal of Technology Law and Policy*, *12*, 395.

Mulligan, C. (2013). Technological intermediaries and freedom of the press. *SMU Law Review*, *66*, 157–277.

Nimmer, M. B. (1969). Does copyright abridge the first amendment guarantees of free speech and press. *UCLA Law Review*, *17*, 1180.

The NSA files. (2013). *The Guardian*. Retrieved from http://www.theguardian.com/world/the-nsa-files

Patry, W. F. (2009). *Moral panics and the copyright wars.* New York, NY: Oxford University Press.

PirateBrowser—No more censorship! (2013). Retrieved from http://piratebrowser.com/

Pollard, A. W. (1916). The regulation of the book trade in the sixteenth century. *Library*, *3rd Ser., 7*, 18–43.

Poort, J., Leenheer, J., van der Ham, J., & Dumitru, C. (2014). Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay. *Telecommunications Policy*, *38*(4), 383–392.

Poulsen, K. (2013, September 13). FBI admits it controlled for servers behind mass malware attack. *Wired*. Retrieved from http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi

Richards, J. I., & Murphy, J. H. (1996). Economic censorship and free speech: The circle of communication between advertisers, media, and consumers. *Journal of Current Issues and Research in Advertising*, *18*(1), 21–34.

Rockefeller, J. D. (2013, December 18). What information do data brokers have on consumers, and how do they use it? *U.S. Senate Committee on Commerce, Science, and Transportation: Hearings*. Retrieved from http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=a47c081a-d653-4272-8d12-d6edc1e04dc6&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=12&YearDisplay=2013

Rose, M. (1993). *Authors and owners: The invention of copyright*. Cambridge, MA: Harvard University Press.

Rose, M. (2003). Nine-tenths of the law: The English copyright debates and the rhetoric of the public domain. *Law and Contemporary Problems*, *66,* 75–88.

Samuelson, P. (2002). Copyright and freedom of expression in historical perspective. *Journal of Intellectual Property Law*, *10*, 319–344.

Seltzer, W. (2010). Free speech unmoored in copyright's safe harbor: Chilling effects of the DMCA on the First Amendment. *Harvard Journal of Law and Technology*, *24*, 171.

Sony Corp. of America v. Universal City Studios, Inc. 464 U.S. 417. (1984).

Tor Project. (2014). *Tor project manual.* Retrieved from https://www.torproject.org/docs/tor-manual.html.en

Von Lohmann, F. (2010, March 3). Unintended consequences: Twelve years under the DMCA. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/wp/unintended-consequences-under-dmca

Voorhoof, D., & Høedt-Rasmussen, I. (2013, January 25). ECHR: Copyright vs. freedom of expression. *Kluwer Copyright Blog*. Retrieved from http://kluwercopyrightblog.com/2013/01/25/echr-copyright-vs-freedom-of-expression

Wittmann, R. (2004, December). *Highwaymen or heroes of enlightenment? Viennese and South German pirates and the German market.* Paper presented at the History of Books and Intellectual History Conference, Princeton, NJ.