



The cyberlocker gold rush: Tracking the rise of file-hosting sites as media distribution platforms

Ramon Lobato

Swinburne University of Technology, Australia

Leah Tang

Independent scholar, Australia

Abstract

This article examines the content distribution practices and regulatory anxieties generated by a particular cloud computing technology: the cyberlocker, or one-click file-hosting site. Cyberlockers, which offer an easy and free way to share media files, are widely used for content piracy. Over the last decade, usage of cyberlockers has increased rapidly; however, an intellectual property crackdown in 2012 has had far-reaching consequences for the industry. In this article we provide a short history of this ephemeral digital technology before considering some questions it presents for current media studies debates about sharing and reciprocity. We argue that the cyberlocker, as a non-reciprocal sharing technology, represents a limit case for liberal theories of informational freedom.

Keywords

copyright, cyberlocker, direct download, distribution, file-hosting, internet regulation, piracy

In the late 2000s, when social media platforms Facebook and Twitter were redefining the way many people communicate and collaborate online, a rudimentary web technology

Corresponding author:

Ramon Lobato, Swinburne Institute for Social Research, Swinburne University of Technology, Mail 53, PO Box 218, Hawthorn, Melbourne, VIC 3122, Australia.
Email: rlobato@swin.edu.au

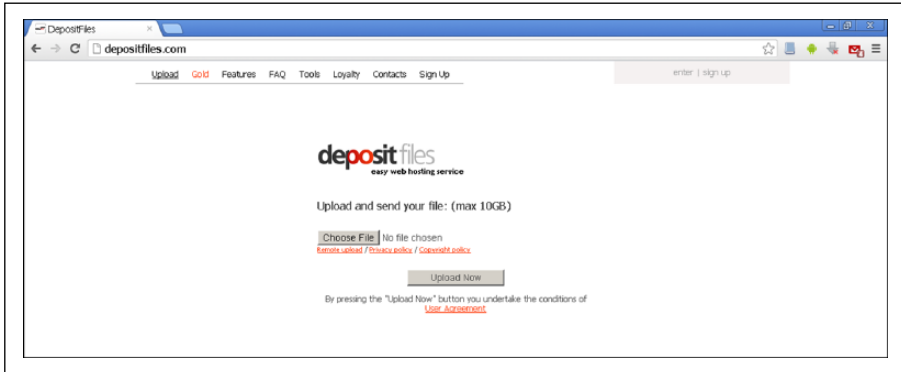


Figure 1. DepositFiles, a cyberlocker registered in the Seychelles.

was shaking things up in a very different way. The cyberlocker – otherwise known as a file locker, file-hosting site, one-click hoster or webhard – is a browser-based platform for sharing digital files (see Figure 1). Users select a file (an MP3, a movie in AVI format, an RAR archive of scanned books, and so on), upload it to a central server, and receive a unique URL from which the content can be downloaded. This URL can then be posted online, enabling the file in question to be accessed by other internet users.

Cyberlockers provide a free, private and easy-to-use system for media distribution. This makes them an ideal platform for content piracy. By 2011, cyberlockers like RapidShare and Megaupload were among the most visited sites on the internet, with millions of users and significant advertising revenue. However, in 2012, a concerted crackdown by rights-holders in various nations resulted in the closure of a number of cyberlockers, the disabling of sharing features on many more, and a fragmentation of the nascent industry. At the time of writing, this file-hosting ecology is extremely fragile. Now is a good time to revisit the curious case of the cyberlocker, which offers an instructive case study in the ‘politics of platforms’ (Gillespie, 2010).

This article seeks to document aspects of the cyberlocker’s history and popular uses – a story that has yet to be told in media scholarship.¹ This case study takes us through some of the more esoteric regions of the digital economy, and it raises questions that are relevant to ongoing debates about internet regulation. The cyberlocker moguls were fly-by-night entrepreneurs, often based in Europe, who worked outside the established IT industries. Over the course of a few years their geeky scene morphed into a profitable and ostensibly legal industry, with revenues based mostly on demand for copyrighted content. While it raised the ire of the publishing, entertainment and software industries, the cyberlocker also changed, for a brief moment, the organisation of the digital media ecology and provided an infrastructure through which a vast range of content could circulate. In what follows we reconstruct some of this history and consider its implications for current media studies debates.

Our analysis contributes to two areas of research. The first is the study of media distribution, incorporating both an emerging literature on the affordances of specific digital platforms (e.g. Burgess and Green, 2009; Snickars and Vonderau, 2012) and a longer

tradition of political-economic research (e.g. Garnham, 1990; Miller et al., 2001). As this body of work shows us, distribution technologies unevenly shape patterns of access to content, and hence to reservoirs of cultural experience and imagination. Digital platforms, including ephemeral ones like the cyberlocker, are useful sites of analysis because they construct new entry points into, and barriers around, media worlds. The second body of research is about the temporalities of popular internet technologies. In 2013, the cyberlocker gold rush appears to be in decline. The original possibility of cyberlockers becoming the internet's default pirate platform now seems remote. Like the compact disc, the QuickTime movie or Friendster, to name a few digital technologies currently attracting retrospective analysis by media scholars (boyd, 2007; Grainge, 2011; Rothenbuhler, 2012; Smith, 1999; Sobchack, 1999), the cyberlocker is part of our recent digital past and warrants cultural analysis and scrutiny on these grounds. We see the present article as forming part of a media-historiographical tradition, in the sense that it seeks to document ephemeral objects of internet culture and situate fast-moving technologies within a wider horizon of comparison and analysis.

An accidental technology

Looking back at its short history, we feel the cyberlocker can best be described as an *accidental* technology, in two distinct senses. On the one hand, it is a form of cloud storage that became a generative platform for cultural circulation by chance rather than design. Using cyberlockers to share proprietary media content, though a logical extension of their capabilities, was not a central feature of the early development of the technology. On the other hand, to borrow an idea from Paul Virilio, the cyberlocker has clearly produced its own 'accident' – namely, massive copyright infringement.

The cyberlocker has roots in earlier systems for file exchange, including FTP (file-transfer protocol), newsgroups and bulletin boards. One of the first web-based file-hosting systems was Apple's iTools, introduced in 2000. Around the same time, the South Korean technology giant LG introduced its 'webhard' (web-based hard drive) service, which became a very popular way for young Koreans to share files. This webhard scene was arguably the first mass-scale take-up of the cyberlocker concept.

A few years later, RapidShare – a Swiss business run by a German, Christian Schmid – adopted the web-based file-hosting model and popularised it in Europe and the English-speaking world. RapidShare started out offering free hosting for files up to 50MB in size. Its official function, to transmit files too large to send by email, was quickly eclipsed by other uses: sharing films, music, TV shows, software, ebooks and porn. By the mid to late 2000s, the cyberlocker was established as a viable business model for a new breed of tech entrepreneurs. RapidShare was joined by a number of other cyberlockers offering similarly user-friendly and anonymous downloads, including Hotfile and the now-infamous Megaupload.

Together these cyberlocker sites began to attract extraordinary amounts of traffic. Internet measurement is a notoriously imprecise science and no single metric can index overall usage patterns effectively, but all the available evidence points to a dramatic rise of cyberlocker downloads (relative to general web traffic as well as to other pirate platforms) in the second half of the 2000s. By the end of the decade the cyberlocker industry

Table 1. Examples of intermediary sites for pirated ebooks (2011–12).

| Type of intermediary | Representative site |
|-------------------------|-------------------------|
| Searchable aggregators | Filetube, Filetram |
| Searchable cyberlockers | 4shared |
| Linking site | Gigapedia, Library.nu |
| Curated archives | (various private sites) |
| User-driven forums | Kaskus, ShareTermPapers |
| Release logs | TehParadox, Warez-BB |

was responsible for a staggering proportion of global web traffic – around 16–22%, according to some studies (Maier et al., 2009: 8; Sanjuàs-Cuxart et al., 2012: 277) – with particularly high levels of use in South America (Ipoque, 2009: 12; cf. Envisional, 2011). Megaupload, with 50m users a day, reportedly accounted for 4% of total internet traffic (Pilling, 2013). The pattern was clear: cyberlockers, along with video streaming sites, were gaining ground on BitTorrent as the pirate platform of choice (Karaganis, 2011).² Millions of internet users around the world were regularly using them to access movies, books, music, anime, software, comics, porn and anything else that could be digitised.

The popularity of the cyberlocker as a file-sharing platform can be attributed to a number of factors. The first is ease of use. After arriving at a cyberlocker site, the user navigates through a series of advertisements to reach a download link. They then click the link and wait a certain amount of time, after which the requested file begins to download. There is generally no cost to uploader or downloader; although downloaders are typically encouraged to pay for a subscription entitling them to instant downloads and faster speeds. The whole procedure is anonymous, giving cyberlockers a distinct advantage over open peer-to-peer systems which can be easily monitored by rights-holders.

In most cases, cyberlocker content is not directly searchable by users: there are no search boxes, and one cannot simply Google a desired track or movie and be taken directly to a cyberlocker download link. Instead, the cyberlocker – a ‘dumb’ storage-and-retrieval technology with limited and highly specific functions – depends on an array of intermediary sites that work to channel traffic through to the active URLs. The cyberlocker constitutes the backend of a larger infrastructure that includes release logs, bulletin boards and forums, where links to cyberlocker-hosted content can be found. Cyberlockers are the storage workhorses of this system; intermediary sites are where users navigate the potentially vast content available. Some of these intermediaries are captured in Table 1 below, which lists popular services for ebook sharing at the time of our research (some of these have subsequently disappeared).

The case of ebooks is particularly interesting, as they come in various open and proprietary formats (pdf, epub, lit, mobi, azw, etc.) and can be shared as single files or compressed archives, with small file sizes that make them well suited to cyberlocker storage. Searchable aggregators provide links to pirated ebooks by scouring the offerings of a subset of cyberlockers, usually the shadier operators, and packaging the results in a Google-like way for easy access, peppered liberally with banner and pop-up ads. Cyberlocker links proliferate on fan and special interest forums, where a more

communitarian atmosphere prevails, and on release logs that specialise in providing timely indexing of uploaded content. There are also many private websites and online communities, catering to particular niches (genre fiction, academic books and so on), where links are shared. While researching this article, we observed how demand for cyberlocker-hosted content can funnel massive amounts of web traffic to unlikely places. Consider the case of the now-defunct ShareTermPapers, a website originally devoted to sharing of plagiarised student essays and projects, with a distinct focus on disciplines like electronic engineering, computer science, IT and business (there remains a particularly large section of MBA-related material), and also covering interview techniques and CV preparation. Following the introduction of a new ShareTermPapers forum, Books and e-Books, in April 2010, ebook piracy well and truly overtook the site's original purpose, to the point where posts related to book uploads outnumbered all other posts by a factor of five to one.³

Having provided some context for the history of cyberlocker development and take-up, let us now turn to its legal status, and specifically to the 2012 Megaupload case that wiped out many of the sites and practices described above.

Countdown to the crackdown

The Wild West era of the cyberlocker came to a dramatic end in 2012. The US Digital Millennium Copyright Act (DMCA) had provided some protection for the online storage industry, which could claim to be unaware of the nature of the content transferred between users; however, the indifference to intellectual property that characterised most cyberlocker businesses did not endear them to rights-holder groups.

To understand cyberlocker regulation we must first consider the business model underpinning the sites. Cyberlockers have two main sources of income: banner advertising and subscriptions (many users choose to pay around US\$10 per month for faster download speeds and improved functionality). A number of cyberlockers, seeking to attract the high-volume uploaders who provide the most in-demand content, reward uploaders with points (convertible to cash) based on the number of downloads their content generated. Megaupload used to pay US\$1500 for a million downloads, while for Wupload the payment was US\$40 for 1000 downloads (Lauinger et al., 2012: 1). These points schemes are referred to euphemistically as affiliate programmes, and they enable users to profit from uploading popular content – in theory, at least. Jelveh and Ross (2012) estimate that a small group of semi-professional pirates were able to cobble together an income stream of above US\$40,000 per year this way; however other studies suggest most uploaders earned little or nothing from their activities (Lauinger et al., 2012; Roettgers, 2012).⁴

These affiliate payments enraged rights-holder groups and provided the silver bullet needed to shut down Megaupload, which was viewed as the most egregiously piratical of the cyberlockers. The Motion Picture Association of America began to apply pressure on law enforcement agencies as well as on the advertising companies (including Google's AdSense) that supplied banner ads to the site. This unwelcome attention culminated in the dramatic arrest, in January 2012, of flamboyant Megaupload founder, Kim Dotcom, on fraud and copyright infringement charges. The result was a media spectacle that

would make headlines around the world. New Zealand police, acting at the behest of the FBI, found Dotcom in the panic room of his multi-million dollar mansion. Early news reports claimed Dotcom had a shotgun by his side, though this turned out to be unloaded and locked in a nearby safe. This bizarre episode on the outskirts of Auckland marked the end of the cyberlocker boom years. While Dotcom's fate has yet to be decided, it was clear that cyberlocker operators would have to be much more careful about how they promoted their services and how they dealt with anti-piracy notifications. The regulatory pressure was so intense that many of the leading operators simply exited the business.

Earlier we discussed the South Korean webhard industry. Webhards were the object of an earlier crackdown, which prefigured the Megaupload incident. These storage sites had long been a headache for local rights-holders: as early as 2006, 53% of anti-piracy enforcement actions in South Korea were against webhards, and by 2007, the figure had risen to 70% (International Intellectual Property Association, 2007: 420, 2008: 337).⁵ In 2008, this came to a head when key staff from a number of popular webhards – Pdbox, Clubbox, Mfile, Endisk, Folderplus, and Wedisk – were arrested. This enforcement push was not uncontroversial. Pdbox and Clubbox parent company Nowcom was already unpopular with the government thanks to its video-sharing site Afreeca, which was used by dissenters to distribute footage of protests against President Lee Myung-Bak. Subsequent prosecutions had a resulting whiff of political interference (Noh, 2008). As in the Dotcom arrest, where flaws in the police process led to embarrassment for the New Zealand authorities (Edwards, 2012), cyberlocker regulation became linked in the minds of many internet users to wider political controversies.

After the Korean crackdown, a new, tougher licensing regime for webhards was brought into force, with steeper penalties for violation (Ahn, 2012). An uneasy truce between webhard operators and rights-holders now prevails. The same cannot be said of cyberlockers elsewhere. In the wake of the Dotcom indictment and the closure of Megaupload, panic gripped the industry. The more legitimate operators moved to introduce stronger anti-piracy measures, hoping that self-regulation would be enough to satisfy rights-holders. FileSonic disabled its public links, reducing itself to a back-up service, before disappearing in August 2012. RapidShare reduced download speeds to very low levels, changed its marketing slogan to 'Secure data logistics', issued anti-piracy manifestos, and attempted to shift the blame onto linking sites. MediaFire severed links with cyberlocker search engines and reinvented itself as a business service.

The more ephemeral sites used creative means to evade prosecution. In a reversal of the typical geoblocking scenario, Uploaded.to disabled access to all US-based ISP addresses, with the aim of reducing its vulnerability to US law enforcement. Oron, a Hong Kong-registered cyberlocker used widely for porn piracy, reportedly tried to cut a deal with one of its key litigants, adult producer Liberty Media, by offering to hand over details of offending uploaders; it also offered to replace pirated content with links to Liberty's pay-sites (Enigmax, 2012a). Across the internet, dozens of cyberlockers disappeared, changed names, or relocated their bases to jurisdictions unfavourable to copyright enforcement. The global cyberlocker industry, already highly dispersed, became even more fragmented, with many operators adopting border-crossing structures designed to deter prosecution: a shell company in the Caribbean, a bank account in Hong Kong, a multi-lingual website, servers in Germany or Austria, and so on.⁶

One consequence of these events is that petabytes of content have simply disappeared from the internet. Many intermediary linking sites now resemble ghost towns: dead links are everywhere. This is not just your average case of link rot but a mass-scale, if not unexpected, evacuation:

when [filehost name redacted on request] shut down sharing we were all but finished [...] 90% of our content was hosted there. Then they deleted all our files and closed the account. They won't even speak with us about it. A whole year's work gone. We shut at the end of the month. (cited in Enigmax, 2012b)

At the time of writing, RapidShare, Hotfile and MediaFire are still in operation but many of the other key cyberlockers – including Oron, Wupload and FileSonic – have disappeared. This underscores the structural instability of file-sharing communities. For all the cyberlocker's wild generativity, the community it brings together is as fragile as these links.

Kim Dotcom was not to be deterred, however. On 19 January 2013, one year after his arrest, he unveiled a new cyberlocker (Mega) with secure user-controlled encryption facilities. User encryption provides another layer of legal indemnity for operators, who can claim ignorance of any copyright violation because they cannot view or access the files. At the time of writing, Mega is up and running and is used widely for pirating content, though it has not reached the same level of popularity as its predecessor. Dotcom has abandoned the affiliate schemes and is marketing Mega on the basis of its privacy and security: its new slogan is 'The Privacy Company', foregrounding some of the curious overlaps that exist between internet libertarians, privacy advocates and pirates. Given the fate of the previous sites, Mega's future is by no means secure. Rights-holder groups have already convinced many subscription resellers, who funnel funds back to Mega, to cut ties with the venture.⁷ Meanwhile the cyberlocker industry remains under siege from every direction. Time will tell if the cyberlocker endures as a major pirate platform, but the industry's gold rush days, promising quick profits and minimal enforcement, have well and truly passed.

The institutional politics of the cyberlocker

Thus far we have documented aspects of the cyberlocker's rise and sudden fall. We have shown how this rudimentary form of web storage became a mainstream technology for content distribution, and have analysed the sharing practices that grew around it. As well as being a curiosity, the cyberlocker is a service that, because of its technological properties and the way it is used, occupies a complex ethical terrain. Of all the internet's sharing platforms, it is the most unloved and unsavoury: few people outside file-sharing circles openly mourn the passing of sites like Oron or Wupload. In this final section, we propose that the cyberlocker represents a limit case for advocates of informational freedom, and we explore the issues this raises for current debates about internet regulation.

The cyberlocker controversy is emblematic not only of the consumers vs. rights-holders logic of the copyright wars but also of a larger conflict between different models of media business. On one side of the fence are the content producers and intellectual

property groups, for whom the cyberlocker is clearly a problem and threat. The way the cyberlocker is imagined (as a cause of revenue leakage), and the strategies through which it is contained (private complaints of violation building up to official enforcement action), are in line with the 'IP maximalism' underlying the war on piracy and the international enforcement push (Drahos with Braithwaite, 2002; Sell, 2003; Vaidhyanathan, 2003). However, this rights-holder agenda, while still the centre of gravity for US trade policy, is not the only force in today's IP debate. Copyright maximalism increasingly comes into direct conflict with the views of 'new economy' tech giants, such as Google and Facebook, which are not content producers in the traditional sense and do not have the same kind of overriding commitment to the IP status quo. For Google in particular, the copyright protection demanded by the movie studios and record companies is a hindrance to its search business model, which relies upon visibility, indexability, easy access and other things that do not necessarily exist in harmony with rights protection. Likewise, social web companies have an investment in making the internet a space of easy sharing, linking and streaming; strong copyright is not the foundational logic of such a vision.⁸

One would expect the cyberlocker industry to have found some support among this new power bloc, given their apparent coincidence of interests. In terms of design and functionality, services like Megaupload, Google Drive and the business-oriented file-sharing and syncing platform Dropbox (a privately held business valued at US\$4b) are relatively similar. Around the time Megaupload went offline in 2012, Dropbox was actually introducing its own easy-linking capabilities designed to encourage its users to share more content, thus inevitably committing more intellectual property offences; yet Dropbox has largely been able to evade the wrath of rights-holders.

From a legal perspective, the difference between 'legit' file management services and cyberlockers may boil down to commercial practice rather than technology. As the 2000 California District Court Napster judgement confirmed, a platform's patterns of actual use (as opposed to intended or stated function) matter from a legal perspective, and website operators cannot get away with presenting widespread copyright infringements as exceptions to the rule when they are in fact the norm. In other words, the legality or illegality of a cyberlocker enterprise is not solely premised on the technology it uses, the transactions it enables, and the consumers it serves; its governance and business model, and the objectives this embodies, also matter. The failed SOPA (Stop Online Piracy Act) Bill sought to ramp up the liability of operators by reducing existing 'safe harbor' provisions.⁹ Following the failure of SOPA, this is off the table for now, but the future viability of cyberlockers that employ affiliate programmes and do not respond promptly to rights-holder complaints appears rather dim.

As Peter Jakobsson and Fredrik Stiernstedt (2012) have noted, the clash between the IP-protecting industries and the newer models, which are premised on aspects of the open internet, represents a significant area of conflict in current intellectual property policy.¹⁰ The cyberlocker is a paradoxical object in this respect, because it is *unpalatable to both sides of the debate*. For the content industries, the cyberlocker is a pirate technology; for the social networking and search giants, it is a reminder of the untamed frontiers of the web that frustrate legitimate internet companies' attempts to project themselves as good corporate citizens and harbingers of a shiny new economic future. This is why most copyright liberals are hesitant about leaping to the defence of Kim Dotcom in the same

Table 2. Structural characteristics of online distribution platforms.

| | Cyberlockers | Social media | Video streaming sites | Peer-to-peer |
|---------------------|--------------|--------------|-----------------------|--------------|
| <i>Reciprocity</i> | Low | Medium | Low | High |
| <i>Co-creation</i> | Low | High | High | Low |
| <i>Transparency</i> | Low | Medium | Medium | Medium |

way that they did for, say, Jammie Thomas, the Minnesota mother and Kazaa user who was famously sued by record companies in 2007 (although see Benkler, 2012). The usual arguments against intellectual property maximalism are not so simple to mount for the cyberlocker, which has a murkier and more explicitly commercial history than peer-to-peer.

Further examination of the cyberlocker case reveals other fault lines in the current copyright debate. One example is the tension around what constitutes ‘creativity’ in online content production and distribution, and its potentially mitigating role within rights disputes. Prominent copyright reformists, including Harvard law professor Lawrence Lessig, frequently make a distinction between ‘good’ sharing and ‘bad’ piracy, the former characterised by the generative, non-market passion of the fan and the latter by commercial intellectual property theft (optical disc piracy, product counterfeiting, and so on). Against this ethical matrix, a corresponding discourse about creativity emerges: user-to-user sharing and copyright-infringing collaboration is creative, and therefore redeemable, while commercial piracy is theft (Lessig, 2004: 62). Hence Lessig’s fundamental call for a more moderate IP regime that can tolerate everyday infringements is achieved by roping off another domain of copying – commercial piracy – and foregrounding its difference.

The cyberlocker, while it forms part of the new social web, is clearly more aligned with this second, socially unacceptable brand of infringement. Cyberlockers are commercial services with a purely strategic investment in sharing rhetoric. They take an instrumental view of the content hosted on their sites: uploaded files are simply deleted when reduced traffic or external enforcement pressures make it attractive to do so. No attempt is made to curate, organise or archive the hosted content. There are few ‘creative’ aspects to cyberlocker usage that would redeem the technology in the eyes of copyright moderates. These characteristics are summed up in Table 2, in which we compare different distributive technologies based on our observation of their day-to-day uses and capabilities.

The lack of search functions and the inability to preview or index content contributes to the perception that cyberlockers are closed, secretive and shifty – a quality that contrasts with the purported (if phantasmatic) openness and transparency of the social web. Furthermore, cyberlockers are not reciprocal; users can download without uploading. They are fundamentally different from peer-to-peer, which has a structural openness built into its architecture. But arguably its most egregious feature, from the perspective of current Web 2.0 discourse, is the fact that the cyberlocker does not foster collaboration or co-creation; its storage-and-retrieval functionality means there is no possibility of textual change for the content hosted on its servers.

The cyberlocker business model has mostly been about professional content, not amateur home videos. While they can be used to host fan-made creations, the profit potential of cyberlockers is bound up with demand for Hollywood movies and Top 40 records. In this sense, cyberlockers cannot claim to have pioneered their own unique form of content creation in the same way that social networking sites can, rightly, claim to have opened up a new kind of commodity-form and medium (Facebook's status update, for example). As Steven Hetcher has recently argued:

Facebook has furthered the creation of content that is subjectively valuable to smaller groups who are interconnected. Thus, rather than replacing a traditional business model for content production, Facebook has created a new type of content all together. A similar claim can be made for YouTube. Increasingly, people create content specifically to upload it on YouTube. (Hetcher, 2012: 40)

This generative property can be located *in the platform itself*, which becomes a media-producing as well as media-distributing entity – allowing platform proprietors a defensible economic, if not moral, claim to the value thus generated.¹¹ Cyberlockers can make no such claim. Their basic functionality (store, retrieve) does not change the nature of the texts that move through its system. There is no space for creative modification or textual interaction on the platform. Like commercial DVD piracy or book photocopying, cyberlocker piracy would appear to be one of the most uncreative forms of sharing – even in the eyes of free culture advocates. An ethical gulf thus divides the cyberlocker industry from the reciprocal, participatory culture at the heart of liberal internet theory.

In this article we have provided a brief cultural and technological history of the cyberlocker, recounting its accidental emergence, its Wild West years, and its dramatic fall from grace. While the cyberlocker is among many technologies to have followed the pattern of mass take-up followed by crackdown and shake-out, in the current socio-legal climate its story is instructive. The cyberlocker figures as a remarkably 'bad' object of internet culture, one that resists assimilation into any progressive ideology. It cannot be romanticised: its brazen commercialism and its distinct technological properties make it impossible to redeem through a rubric of freedom or openness. As it enters its second decade, we will watch with interest to see how the remnants of the industry evolve and how future generations of media scholars will reconstruct the story of this unloved and unlovely technology.

Funding

The financial support of the Australian Research Council's Discovery program is gratefully acknowledged.

Notes

1. This article draws on and develops Lobato's previous discussion of cyberlocker usage in film piracy (Lobato, 2012: 104–6).
2. According to one study, in this period cyberlockers such as Megaupload and 4Shared received more hits than the iconic torrent website, the Pirate Bay (Envisional, 2011: 16, citing Comscore data).

3. When we checked in May 2012, the Books and e-Books forum had around 50,000 posts. Shortly afterwards it was taken offline. Until late November 2011, there was also a 'requests' forum but this was subsequently removed. (It is worth noting that users of ShareTermPapers would often share links to their own carefully curated archives of ebooks, organised according to individual taste. This is in contrast to many forum sites providing links to cyberlocker content, where uploads do not come from the general user community, but rather are provided by a small number of super-users, who often post links to a wide range of apparently unrelated titles.) Other community forums which became hubs for cyberlocker piracy in a similarly accidental way include the Indonesian culture portal Kaskus (kaskus.co.id)
4. In the case of Megaupload, the points system became a crucial plank in the felony charges brought by US courts against Kim Dotcom and his co-accused. The Grand Jury indictment singled out marketing slogans like 'The more popular your files the more you make' as evidence of Megaupload's piratical intent (US District Court, 2012).
5. One 2009 report claims that the two biggest webhards, Pdbox and Clubbox, had 17m users between them (Noh, 2008). For more on cyberlockers see Lee (2009), Ahn (2012) and International Intellectual Property Alliance (2007).
6. Most cyberlockers already have multi-language capability for speakers of most major languages and some minor languages, especially those spoken in nations seen to have strong file-sharing scenes. Take, for example, popular new-breed cyberlocker Ziddu's range of languages: Chinese, Bahasa Indonesia, Arabic, Thai, Vietnamese, Japanese, Spanish, Portuguese, Polish and Romanian.
7. One of the figures involved is the Australian porn producer Robert King, who operates the website www.stopfilelockers.com. He has been running a high-profile anti-Mega campaign, targeting payment-processing companies.
8. We are referring to protection of media content here; of course, these companies are fiercely protective of other IP rights, which may cover things like software code, proprietary search algorithms, and so on.
9. Dotcom was arrested the same week the SOPA bill was shelved – a connection his supporters were keen to promote.
10. This conflict is made quite clear in, for example, the landmark, government-commissioned Hargreaves report into IP reform in the UK (Hargreaves, 2011). Naturally, views differ markedly between and within the 'old' and 'new' media sectors, and the position on copyright described above does not of course carry through directly to other areas of IP law, such as patents, where the approach may be significantly more hardline.
11. See Terranova (2000) for a critique of the ethical stakes of this value-capture.

References

- Ahn J (2012) Broadband policy in South Korea: the effect of government regulation on internet proliferation. In: *PTC 12 (Pacific Telecommunications Council) Proceedings*, 20–23 January, Hawaii, available at: www.ptc.org/ptc12/?page_id=1287&pid=123 (accessed 1 November 2012).
- Benkler Y (2012) Seven lessons from SOPA/PIPA/Megaupload and four proposals on where we go from here. *TechPresident*, 25 January, available at: techpresident.com/news/21680/seven-lessons-sopapipamegaupload-and-four-proposals-where-we-go-here (accessed 10 February 2013).
- boyd d (2007) None of this is real: identity and participation in Friendster. In: Karaganis J (ed.) *Structures of Participation in Digital Culture*. New York: Social Science Research Council, pp. 132–157.

- Burgess J and Green J (2009) *YouTube: Online Video and Participatory Culture*. Cambridge: Polity Press.
- Drahos P with Braithwaite J (2002) *Information Feudalism: Who Controls the Knowledge Economy?* London: Earthscan.
- Edwards B (2012) Political round-up: growing anger over Dotcom fiasco. *New Zealand Herald*, 27 September, available at: www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10836888 (accessed 1 November 2012).
- Enigmax (2012a) Cyberlocker offered to help prosecute users to settle \$34.8m copyright suit. *Torrent Freak*, 6 July, available at: torrentfreak.com/cyberlocker-offered-to-help-prosecute-users-to-settle-34-8m-copyright-suit-120706/ (accessed 1 November 2012).
- Enigmax (2012b) Mega aftermath: upheaval in pirate warez land. *Torrent Freak*, 28 January, available at: torrentfreak.com/mega-aftermath-upheaval-in-pirate-warez-land-120128/ (accessed 1 November 2012).
- Envisional (2011) *An Estimate of Infringing Use of the Internet* (technical report). Cambridge: Envisional Ltd.
- Garnham N (1990) *Capitalism and Communication: Global Culture and the Economics of Information*. London: Sage.
- Gillespie T (2010) The politics of 'platforms'. *New Media & Society* 12(3): 347–364.
- Grainge P (2011) *Ephemeral Media: Transitory Screen Culture from Television to YouTube*. London: British Film Institute.
- Hargreaves I (2011) *Digital Opportunity: A Review of Intellectual Property and Growth*. Available at: www.ipo.gov.uk/ipreview-finalreport.pdf (accessed 11 July 2013).
- Hetcher S (2012) Amateur creative digital content and proportional commerce. In: Hunter D, Lobato R, Richardson M and Thomas J (eds) *Amateur Media: Social, Cultural and Legal Perspectives*. London: Routledge, pp. 35–52.
- International Intellectual Property Association (IIPA) (2007) *Special 301 Report* (excerpt). Washington: International Intellectual Property Association. Available at: www.iipa.com/rbc/2007/2007SPEC301SOUTHKOREA.pdf (accessed 1 November 2012).
- International Intellectual Property Association (IIPA) (2008) *Special 301 Report* (excerpt). Washington: International Intellectual Property Association. Available at: www.iipa.com/rbc/2008/2008SPEC301SOUTH_KOREA.pdf (accessed 1 November 2012).
- Ipoque (2009) *Internet Study 2008/2009*. Leipzig: Ipoque GmbH.
- Jakobsson P and Stiernstedt F (2012) Reinforcing property by strengthening the commons: a new media policy paradigm? *Triple C* 10(1): 49–55.
- Jelveh Z and Ross K (2012) Profiting from piracy: a preliminary analysis of the economics of the cyberlocker ecosystem. Paper presented at IEEE International Conference on Peer-to-Peer Computing, Universitat Rovira I Virgili, Tarragona, 3 September. Available at: cis.poly.edu/~ross/papers/Cyberlockers.pdf (accessed 1 November 2012).
- Karaganis J (ed.) (2011) *Media Piracy in Emerging Economies*. New York: Social Science Research Council.
- Lauinger T, Engin K and Michiardi P (2012) Paying for piracy? An analysis of one-click hosters' controversial reward schemes. Paper presented at 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Amsterdam, 13 September. Available at: www.iseclab.org/papers/uploader-income.pdf (accessed 1 November 2012).
- Lee JY (2009) Contesting the digital economy and culture: digital technologies and the transformation of popular music in Korea. *Inter-Asia Cultural Studies* 1(4): 489–506.
- Lessig L (2004) *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: Penguin.

- Lobato R (2012) *Shadow Economies of Cinema: Mapping Informal Film Distribution*. London: British Film Institute.
- Maier G, Feldmann A, Paxson V and Allman V. (2009) On dominant characteristics of residential broadband internet traffic. Paper presented at *IMC 09*, 4–6 Nov 2009, Chicago. Available at: www.icir.net/mallman/papers/residential-imc09.pdf (accessed 1 November 2012).
- Miller T, Govil N, McMurria J and Maxwell R (2001) *Global Hollywood*. London: British Film Institute.
- Noh J (2008) Five Korean webhards prosecuted for copyright infringement. *Screen Daily*, 18 June, available at: www.screendaily.com/4039447.article (accessed 1 November 2013).
- Pilling D (2013) Lunch with the FT: Kim Dotcom. *Financial Times*, 19 April. Available at: www.ft.com/cms/s/2/95c68080-a68b-11e2-885b-00144feabdc0.html (accessed 25 April 2013).
- Roettgers J (2012) MegaUpload and the end of a pirate cottage industry. *GigaOm*, 24 January, available at: gigaom.com/2012/01/24/megaupload-affiliate-programs/ (accessed 1 November 2012).
- Rothenbuhler EW (2012) The compact disc and its culture: notes on melancholia. In: Bolin G (ed.) *Cultural Technologies: The Shaping of Culture in Media and Society*. London: Routledge, pp. 36–50.
- Sanjuás-Cuxart J, Barlet-Ros P and Solé-Pareta J (2012) Measurement based analysis of one-click file hosting services. *Journal of Network and Systems Management* 20(2): 276–301.
- Sell S (2003) *Private Power, Public Law: The Globalization of Intellectual Property Rights*. Cambridge: Cambridge University Press.
- Smith GM (ed.) (1999) *On a Silver Platter: CD-ROMs and the Promises of a New Technology*. New York: New York University Press.
- Snickars P and Vonderau P (2012) *Moving Data: The iPhone and the Future of Media*. New York: Columbia University Press.
- Sobchack V (1999) Nostalgia for a digital object: regrets on the quickening of QuickTime. *Millennium Film Journal* 34, available at: mfj-online.org/journalPages/MFJ34/VivianSobchack.html (accessed 1 November 2012).
- Terranova T (2000) Free labor: producing culture for the digital economy. *Social Text* 18(2): 33–58.
- US District Court (2012) Indictment against Kim Dotcom, Megaupload Limited, Vestor Limited, Finn Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm, and Bram van der Kolk. US District Court for the Eastern District of Virginia, 5 January. Available at: www.nbr.co.nz/sites/default/files/images/78786408-Mega-Indictment.pdf (accessed 1 November 2012).
- Vaidhyanathan S (2003) *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity*. New York: New York University Press.

Author biographies

Ramon Lobato is a research fellow with the ARC Centre of Excellence for Creative Industries and Innovation at Swinburne University of Technology. He is the author of *Shadow Economies of Cinema* (British Film Institute, 2012).

Leah Tang is an economist and historian with a particular interest in ebooks.