Anonymity and the Law: "The Darknet Rises"

Felix Ralph examines the challenges that the anonymity of the "darknet" poses for the legal system, copyright holders, the community and human rights.*

The darknet

Completely anonymous and encrypted browsing has the capacity to change nearly *all* current communication, media and copyright law. By rendering the internet untraceable, the "darknet" makes the law, in its current form, virtually unenforceable.

The concept of the darknet is both revolutionary and simple. It can be thought of as a series of unsearchable networks ranging from the simple copying of hard-drives between friends, all the way to a complex eco-system of layered anonymous networks.[1] Due to its nature, the size of these networks is unknowable but the regular internet is usually described as the mere tip of the iceberg in comparison to the darknet(s). The biggest of which is The Onion Routing (the ***TOR***) program. It scrambles data through various nodes to protect the IP addresses and data packets from unwanted traffic analysis. Effectively, *no-one* but the user can identify where and what content is being consumed.

The digital dilemma then deepens, with the paradox for users being that the more they desire online privacy the less they are likely to get.

The uses for the anonymity provided by the darknet can be at once noble and sinister. Cyber-criminals have adopted the network as their own. It has become a haven for child pornography and ordering drugs online.[2] All this is supplemented by an anonymous currency system that is used to finance some of these operations.[3] Conversely, the TOR network has been vital to journalists in repressive regimes.[4] Any *legally* created content on the darknet has been anonymously leaked onto the network, blatantly breaching copyright law. The TOR network has been simply described as "similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints."[5] What users do with their anonymous road is as diverse as the human condition.

While it does not guarantee absolute anonymity, TOR makes traffic analysis virtually unfeasible. Combined with periodic wiping of the hard drive,[6] it is almost impossible to determine the identity and location of the end-user. This means the proposed data retention policies[7] become meaningless and untraceable. As early as 2002, a number of Microsoft engineers made the simple but bold prediction that, "ultimately the darknet-genie will not be put back into the bottle."[8] Website owners do not even know who is looking at their website. Because the data is scrambled, questions of intermediary liability[9] also become moot, as internet service providers (***ISPs***) cannot hold any meaningful data. If *Roadshow Films Pty Ltd v iiNet Ltd* (2012) AJLR 494 (***iiNet case***) shows us anything, it is that the current status quo for legal enforcement of internet law relies on the dubious co-operation of the ISPs.[10] If the darknet becomes popular, the main challenge posed by this disruptive technology is the denial of *all* identifying information to ISPs, or any third party, which makes the law even harder to enforce. As always, technology spurs and requires the law to adapt to rapid changes.

One of two paths

It is not often that we stand at the precipice of great change. Technology is forcing the hand of our society to consider something that we have not experienced before; the prospect of completely anonymous community interaction. Communications, media, copyright and even criminal law must be nimble enough to adapt to this anonymous future. Essentially there are two paths we can take. The first path is one of prohibition. However, suggestions that the darknet be taken down may be ineffective. Not even considering the practical difficulties,[11] laws of prohibition may also be *ultra*

1 Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" *Microsoft Corporation* (2002) 1, 3. < http://msl1.mit.edu/ESD10/docs/darknet5.pdf>.

2 Geoffrey A. Fowler 'Tor: An Anonymous, And Controversial, Way to Web-Surf', *The Wall Street Journal* (Online) 17 December 2012; < http://online.wsj.com/article/SB10001424127887324677204578185382377144280.html> Editorial, 'Anonymous marketplace: software a boon for criminals and the 'darknet', The Age, (Online) 9 March 2012 http://www.smh.com.au/technology/security/anonymous-marketplace-software-a-boon-for-criminals-and-the-darknet-20120309-1uo4d.html>.

3 Bitcoin, *About Bitcoin* <http://bitcoin.org/about.html> 19 January 2013.

4 Ian Shapira, 'U.S. funding tech firms that help Mideast dissidents evade government censors', *The Washington Post* (Online), 9 March 2011 < http://www.washingtonpost.com/wp-dyn/content /article/2011/03 /09/AR2011030905157.html>.

5 The TOR Project, *TOR Overview* <https://www.torproject.org/about/overview.html.en> 19 January 2013.

6 See generally, Tails: The Amnesic Icognition Live System *About,* <https://tails.boum.org/> 19 January 2013.

7 Attorney-General's Department, 'Carrier-Carriage Service Provider Data Set' (Consultation Paper No 1.0), 2010 Commonwealth of Australia. < http://images.smh.com.au/file/2010/07/23/1710367/Secret-Document.PDF> Note: Document is heavily redacted and undated.

8 Biddle, England, Peinado, and Willman, above n 1, 1.

9 See *generally,* Roadshow Films Pty Limited v iiNet Limited (2011) 194 FCR 285.

10 David Lindsay, 'Liability of ISPs for end-user copyright infringements: The first instance decision in Roadshow Films Pty Ltd v iiNet Ltd (No 3)' (2010) 60 *Telecommunications Journal of Australia 29.*

11 See the defeated Bill, US Congress House, *Stop Online Piracy* Act H.R. 3261, 112th cong., 1st sess. (October 26, 2011).

If digital copyright owners are forced into adopting DRM systems, the role of the law should be to stand behind the rights of those owners without compromising the privacy of its citizens

vires. Like the internet the darknet is not used solely for nefarious purposes. It is also a forum for the free exchange of political, social and philosophical ideas. If legislatures attempt to impose a blanket ban on this new space it could fall afoul of the implied freedom of political communication found in the structure and text of the Constitution.[12] However, laws banning an entire medium of communication have never appeared before the High Court. The cases of *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1 and *Australian Capital Television Pty Ltd v Commonwealth (No. 2)* (1992) 177 CLR 106 only address what can be said *within* a medium, not the banning of the medium itself. Nevertheless, a law prohibiting the darknet may violate the test in *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 which rules unconstitutional any law that effectively burdens freedom of communication about government or political matters either in its terms, operation or effect. Furthermore, such a sweeping law may not be compatible with representative and responsible government and may not be appropriate or adapted.[13]

So we are left with the second path; accepting and adapting to the changes brought by technology. If anonymous browsing becomes the norm this poses enormous challenges to artists and copyright owners. Because anonymous browsing has the capacity to circumvent legal detection, it significantly undermines the twin foundational pillars of copyright law. The first pillar is the idea that the work of the author has attached to it certain rights in property and contract. The second pillar is the utilitarian idea that copyright law, by protecting authors' rights, provides an incentive for the creation of literary and artistic works.[14] Without the protection of copyright, the artistic health of our society weakens.[15] Exclusively legal solutions have so far proved ineffective. The boom in piracy comes despite every lawsuit against a P2P network entrepreneur being successful.[16] A perfect illustration is Pirate Bay, one of the largest torrent sites, which proudly publishes expletive-riddled replies to the numerous legal threats they receive. In riposte to the multinational law firms they end with a statistic: "… 0 torrents has [*sic*] been removed, and 0 torrents will ever be removed."[17]

Despite large fines to users, legal threats are barely having an impact on the boom.[18] Any response to the problem of online pirating must take into account the old lessons taught by the P2P lawsuits when responding to new frontiers like the darknet.

The hidden dilemma

The piracy boom has created a dilemma for copyright holders. Charles Clark broadly formulated a solution to this "digital dilemma"[19] by finding that the "answer to the machine is the machine."[20] Technological innovation makes it possible to create an encrypted-lockbox embedded within content that only opens for an authorised user. This self-enforcing technology is a form of digital rights management (***DRM***) which can "directly impose technological controls on what users may, or may not, do with digital content."[21] There are multiple ways to achieve this; either through encryption, or watermarking and tracking technologies. One example is Cinavia, which embeds code into the audio of a Blu-Ray file and then limits copy and use on certain machines.[22] A stronger version of such a technology would solve the problem of anonymous browsing because copyright holders are not monitoring the traffic data of users but instead the *use* of their products. An anonymous browser still needs to download the content to use it.

It is time that we step away from the legal fiction that copyright owners are going to always be able to pursue illegal users of their content

This approach is not without its problems. Lindsay and Ricketson warn that there could a "technological arms race" between copyright owners and creators of circumvention techniques.[23] They also explore a more disturbing possibility that

> "…unconstrained implementation of technological forms of protection, such as encryption, may result in inefficiencies in the form of rent-seeking behaviour by copyright owners pursuing more returns than are available under copyright law."[24]

While TOR may protect *browsing,* it does not protect the end-users from content on their machines. The business models of compa-

12 Commonwealth of Australia Constitution Act 1900 (Imp) ss. 7, 24, 68 and 128.

13 cf: Coleman v Power (2004) 220 CLR 1.

14 Andrew Kenyon & Megan Richardson, New Dimensions in Privacy Law: International and Comparative Perspectives (Cambridge University Press, 1st ed, 2006) 125.

15 William Uzgalis, "John Locke", The Stanford Encyclopedia of Philosophy (Fall 2012 Edition), Edward N. Zalta (ed.) <http://plato.stanford.edu/archives/fall2012/entries/locke/> 20 January 2013.

16 Rebecca Giblin, *The Code Wars: 10 Years of P2P Software Litigation* (Edward Elgar Publishing Inc, 2011) 1.

17 The Pirate Bay, <http://thepiratebay.se/legal> 21 January 2013.

18 *Sony BMG Music Entertainment v Tenenbaum,* 93 USPQ 2d 1867 (D Mass, 2009); *Sony BMG Music Entertainment v Tenenbaum,* 2010 WL 2705499, at 3 (D Mass, 2010) cited in Giblin, above n 16, 2 -3.

19 United States, Committee on Intellectual Property Rights and the Emerging Information Infrastructure, *The Digital Dilemma* (Washington, DC: National Academy Press, 2000) cited in David Lindsay and Sam Ricketson 'Copyright, Privacy and DRM' in Andrew Kenyon & Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 1st ed, 2006) 128.

20 Ibid citing Charles Clark, 'The Answer to the Machine is the Machine' in Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium* (The Hague: Kluwer Law International, 1996).

21 Ibid 148.

22 Cinavia, *What is Cinavia Technology and What does it Do?* <http://www.cinavia.com/languages/english/pages/technology.html> 21 January 2013.

23 Lindsay and Ricketson above n 19, 131.

24 Ibid.

nies like Facebook and Google rely on how much private data they can collect. In the digitised epoch, data is money. Users may turn to the darknet in droves if and when they realise the moral hazards from multinational corporations who collect their private information.[25] If this happens and users flock to the darknet, if the current trend toward pirated films continues, it would result in intolerable conditions for copyright owners. They would have no means of enforcing their rights and would be unable to pursue intermediary liability against ISP providers. The defence in the *iiNet* case becomes even stronger in the context of widespread anonymity. Thus copyright owners may be forced to implement DRM systems that increase the "use of surveillance systems by both public and private sector entities, with possibly worrying consequences for ever more rationalisation and normalisation, and the threat of increased social conformity."[26] The digital dilemma then deepens, with the paradox for users being that the more they desire online privacy the less they are likely to get.

The new role for the law is to protect the digital environment for both copyright owners and internet citizens

The new role of the law

If digital copyright owners are forced into adopting DRM systems, the role of the law should be to stand behind the rights of those owners without compromising the privacy of its citizens. This requires consideration of both copyright owners and the privacy of end-users. To protect copyright owners, liability should be incurred for the possession of software or code, which has the dominant purpose of circumventing DRM-protected products. It then falls within the responsibility of copyright owners to create digital strong boxes to protect against modern day internet banditry. Copyright owners could then request or pursue ISPs that host content that circumvents DRM systems. While this may seem like an ineffective measure for the darknet, ISPs that run illegal websites can always be contacted to shutdown those sites. It is up to the legal system to create the regulatory eco-system that protects the rights of copyright-holders. It is time that we step away from the legal fiction that copyright owners are going to always be able to pursue illegal users of their content. The key to fighting online privacy is to layer protection after protection on the content *itself,* with the law providing the regulatory framework to protect that security.

To ensure the end-users privacy, laws should be enacted that prevent DRM protected products from exceeding their original purpose of protecting the product. That is, the "rent-seeking behaviour" [27] that Lindsay and Ricketson warned against should be regulated. Such a law should allow digital *protection* of the product but not the *tracking* or *collecting* of any data received. Any tracking of data should require the clear and informed consent of the end-user. This would allow for the creation digital eco-systems that allow users to pay subscription fees for access to content. It is perfectly possible to have an eco-system that protects the rights of copyright owners and the privacy of end-users. This makes sense both from privacy *and* economic standpoints because copyright industries are most profitable "when their primary focus [i]s not to minimize unauthorized uses but rather to maximize authorized use."[28] The legal system should remove the temptation to use DRM systems to collect, survey and retain personal information and data.

To supplement these laws the definition of "personal information" in the *Privacy Act 1988* (Cth) must be broadened. Personal information is currently defined as information, "…about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."[29]

Under this definition information that reveals the location of a user falls outside the statutory definition of personal information, but it certainly falls within a common sense definition of privacy. Such gaps need to be closed in order for citizens to have a reasonable expectation of privacy, and for governments to comply with human rights legislation.[30]

Essentially, the "machine" will correct itself. If copyright industries protect the *product* then the economics of supply and demand will take over. The new role for the law is to protect the digital environment for both copyright owners and internet citizens.

Where law and anonymity meet

It is naïve to assume that the darknet will remain a reserve for hard-core tech-heads *ad infinitum*. All parties need to begin thinking towards ways of adapting to our anonymous future. Our legal system is robust enough to change with this future *without* sacrificing the ideals that underpin it. If the law can strengthen the protection of content while broadening the privacy of users, both the interests of corporations and the rights of individuals become protected.

The darknet is not synonymous with crypto-anarchy. This paper has attempted to show that it is possible to have a thriving copyright industry, freedom of speech and communication and online anonymity at the same time. An anonymous future does not have to be an immoral one.

Felix Ralph is currently studying under full scholarship at the Victorian College of Law. He has a particular interest in criminal law and the challenges posed by new trends and technologies to the rule of law.

* This paper was awarded third prize in the CAMLA Essay competition.

25 Rana Foorahar, 'Learning to Hate Big Tech', *Time Magazine,* (New York), 4 May 2012.

26 Lindsay and Ricketson, above n 19, 147.

27 Ibid 131.

28 Daniel J. Gervais, *Collective Management of Copyright and Related Rights* (The Hague: Kluwer Law International, 2010) 17, cited in Giblin above n 16, 182.

29 Privacy Act 1988 (Cth) s 6.

30 E.g. *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.