THE ENFORCEMENT OF LAWS REGULATING DIGITAL CULTURAL CONTENT: A PROPOSAL

Law is becoming increasingly digital in nature, and the State is increasingly using digital technology for the purposes of physical legal enforcement. This paper argues that this poses unique issues for legal regulation of cultural content, changing the relationship between the individual and the State. The paper focuses on laws in the UK and China to demonstrate how these issues have arisen, and what the potential consequences of this change could be. The paper culminates in arguing that legislatures and courts should be required to explicitly consider how digital technology influences, in a given law or case, the enforcement of law.

Introduction

In the context of Internet communications, enforcement of legal regulations by the State and private actors can be increased utilising digital technology. This paper investigates how this has been occurring, what the possible ramifications of this are, and whether there is a need for legislatures to explicitly consider this change. The paper does so by focusing on two countries, the UK and China. It does so because both have been using digital technology to enforce laws concerning cultural content; in China this has been for the purpose of State censorship; in the UK, this has often been to enforce intellectual property laws. This paper will focus upon those laws – Internet censorship rules in China, and Internet copyright enforcement in the UK. There are striking similarities between the two systems – both utilise similar techniques to physically enforce the law through digital technology. Indeed, the underlying technologies that enable surveillance and enforcement are fundamentally the same. This paper will firstly argue that we should remember that digital technology is based in a physical world, and then analyse how the use of digital technology for physical enforcement is a natural progression of digital technology. It will then consider how digital technology strengthens legal enforcement and thus poses a challenge to the existing individual-State relationship. In the UK, the increasing use of censorship systems for the purposes of copyright infringement will be considered. There is then a proposal made in terms of requiring the legislature to perform a risk assessment of the impact of digital law upon physical enforcement, noting the difference between the previous analogue law and the newer digital law.

1. Physicality

Enforcement of laws by a State has always been subject to the ability of the individual to be able to be identified by the State for the transgression of the law. In the UK, for example, there is no provision allowing for the private copying of a copyright work.[1] However, in reality, the UK has permitted the sale of recording equipment,[2] and individuals have in all probability made unauthorised reproductions of copyright works without the knowledge of the right holder or the State. A similar situation exists throughout numerous aspects of our lives – for example, a motorist may often speed away from the eyes of speed cameras or the Police. As works become increasingly digital, and as digital devices become more prevalent, the reach of legal

[1] Helberger, N., and Hugenholtz, P., 'No place like home for making a copy: Private copying in European copyright law and consumer law', 22 *Berkeley Technology Law Journal* 1061 (2007). The reader should note that s.28B CDPA 1988, which was introduced in 2014 and which intended to allow for private copying, was quashed– see R (on the application of British Academy of Songwriters, Composers and Authors) v Secretary of State for Business, Innovation and Skills [2015] EWHC 2041 (Admin).

[2] Consider the outcome of CBS Songs v Amstrad Consumer Electronics [1988] AC 1013.

regulation is gradually expanding. There has often been a perception that the Internet is, or could be, a lawless place.[3] However, digital technology does not exist in a vacuum; it relies upon the technologies of the physical world for its very existence. Nowhere is the failure to recognise this clearer than in the 1993 *New Yorker* cartoon, which shows a dog looking at a computer, with a speech bubble containing the text "On the Internet, nobody knows you are a dog."[4] Never was anything more incorrect or wrong about the nature of digital technology. On the Internet everyone knows, and everyone has always known, who you are.[5] Knowledge is what the core of the Internet is based on; a linking of physical computers with physical wires, utilising the protocol of TCP/IP for the purpose of discoverability.[6] TCP/IP is for the purpose of providing the basis of enabling data transactions between different computers by making them discoverable, not by hiding their existence.[7] It is a system based in, and of, the physical world. It is not a system of ethereal existence, but a physical technology of wires and microchips. It is this rather critical overlooked point, coupled with the fact that the backbone of the Internet is one of discoverability, that meant that the ability to use digital technology for the purposes of greater law enforcement was, perhaps, inevitable.

As digital technology has developed into its own web of existence, that digital technology is influencing the existence of the physical world in unforeseen ways. This first notably occurred with Digital Rights Management (DRM) mechanisms, an attempt to limit what individuals could, and could not, do with digital video which nonetheless could be achieved with traditional analogue works, e.g. reproduction.[8] These were the first steps in the imposition of digital control back into the analogue world. However, those steps were restricted in that an individual could still step out of the digital controls e.g. simply by watching a DRM protected DVD in person, using a camera; or finding works that were broken into already and thus stripped of the DRM making the DRM issue irrelevant. With the rise of streaming services, however, our increasing reliance on digital technology in day to day activities[9] makes analogue physical circumvention more difficult to achieve.[10] For example, whilst an analogue video recording of a DVD may suffice for an analogue school project, DRMs will have a greater impact if they limit a similar project contained within the digital world, using interactive computer code – e.g. a mashup of video game code interactions, or editing of code in DRM protected (encrypted) video games.[11] Thus, this is the nascent beginning of the digital technologies having a direct

---

[3] See, for example, the implicit assertion in Barlow, J., 'Declaration of the Independence of Cyberspace' (1996) in Spiller, N., 'Cyber_Reader', Phaidon Press (2002); see also https://www.eff.org/cyberspace-independence; National Research Council, 'The Digital Dilemma', National Academy Press, Washington D.C., 2000 at p.50*ff*.

[4] Steiner, P., 'On the Internet, nobody knows you're a dog' The New Yorker July 5, 1993. See also https://web.archive.org/web/20051029045942/http://www.unc.edu/depts/jomc/academics/dri/idog.html

[5] This is a point of logic but also see Rheingold, H., 'The Virtual Community: Homesteading on the Electronic Frontier', Harperperennial, New York (1994).

[6] See Scrimger, R., LaSalle, P., Parihar M., and Gupta, M., 'TCP/IP Bible', Hungry Minds, New York (2002).

[7] See e.g. Berners-Lee, T., 'Weaving the Web', Texere (1999).

[8] As evidenced by the mass of writings, see *inter alia*: Lessig, L., 'Code', Basic Books (1999). Lessig, L., 'The future of ideas', Random House (2001); Lessig, L., 'Free Culture', Penguin (2004); Rochester, J., and Gantz, J., 'Pirates of the Digital Millennium', Prentice Hall (2004); Litman, J., Digital Copyright, Prometheus Books (2001); Vaidhyanathan, S., 'Copyrights and Copywrongs,' NYU Press (2003); Vaidhyanathan, S., 'The Anarchist in the library,' Basic Books (2004).

[9] Note the use of tracking and tracing technologies in such services – see empirical evidence of pre-emptive licensing practices -notes on file with the author (RIVENTA/SLS), and notes in Griffin, J., A proposal for a bridge of licensing over a sea of IP uncertainty: Digital Watermarking of 3D Printed Content' in Chan, Choo, Griffin and Osuji (eds), Intellectual Property Rights and Emerging Technology: 3D printing in China (Routledge, 2018)

[10] See discussion in Griffin, J., State of Creativity, Edward Elgar (2019) Chapters 2-4.

[11] See Griffin J., "The rise of the digital technology 'meritocracy': legal rules and their impact" 15(3) *Information and Communications Technology Law* 211 (2006).

impact in the physical world.

Similarly, as digital technology becomes an increasingly central part of everyday life in the physical world, so digital technology will increasingly influence our expectations in the real-world context. This can be from our expectations of how artistic works should operate, to the legal sanctions we may expect if we commit a wrong. In short, digital technology will increasingly inform and alter our real-world conduct. Copyright Management Information (CMI) and watermarking systems can gather information about our use, not just of digital works but also of physical products.[12] Such watermarking systems could be used to assess whether the physical use of products is a potential copyright infringement, for instance with augmented reality cameras detecting those potential infringements. DRM and CMI can also be used in other technologies such as 3D printing, 4D printing and virtual realities, all of which can impact our day to day existence in the physical world. This is a far cry compared to the early days of DRM when individuals could simply turn off a computer. Like the Skynet in Terminator (without wishing to sound melodramatic),[13] we appear to be rapidly reaching a stage where turning off a computer to remove the impact of the digital upon our nature of being is becoming an impossibility. To turn off the machine is to turn off ourselves: we are becoming a symbiotic machine-being.

However, the inability to turn off the machine is not unique to the digital technologies developed within the last few years. Such developments have long been taking place in other countries,[14] who seek to combine certain characteristics of digital technologies with that of governance – in essence, the State becomes a symbiotic machine-State, unable to turn off the machine without also turning itself off, i.e. endangering its existence.[15] The country that has been most advanced in this symbiotic system is the People's Republic of China (PRC) in relation to its online censorship system, the Great Firewall.[16] The system acts to block access to selected foreign websites such as Facebook and Twitter, and possibly to slow down access to some overseas sites.[17] The PRC has a policy of identifying individual users with specific Internet access points. The system of Internet policing bears similarities to those used in DRM and CMI systems, in how it links physical world presence to penalties. The PRC has effectively taken those systems and placed them within the context of real-world national censorship. Instead of mostly civil sanctions under the UK copyright provisions relating to DRM and CMI,[18] the sanctions could become criminal for acting against the State.

Physical restrictions may be from physical force exerted or threatened directly by the State, or

---

[12] Griffin, J., We become what we think: Machine laws in machine minds', in Chan, Choo, Griffin and Osuji (eds), Intellectual Property Rights and Emerging Technology: 3D printing in China (Routledge, 2018).

[13] A reference to the various *Terminator* films; a familiar trope in science fiction works.

[14] First, a clarification. As Heidegger notes (Heidegger, M., The Question Concerning Technology and Other Essays (1954; Harper Perennial 2013)), technologies have many forms and technology as a phrase itself can include governance. Digital technology is a form of that governance. China remains, to the knowledge of the author, the foremost example of digital enforcement. See also Higgs, E., The Information State in England: The central collection of information on citizens since 1500, Palgrave (2003).

[15] Also see Licklider, JCR, Man-Computer Symbiosis, IRE Transactions on Human Factors in Electronics, March 1960, 4.

[16] Liang, C., 'Red light, green light: Has the PRC achieved its goals through the 2000 Internet regulations?' 34 *Vanderbilt Journal of Trans-national law* 1417 (2001); Fu K., Chan C., Chau, M., 'Assessing censorship on microblogs in China: Discriminatory keyword analysis and impact evaluation of the 'real name registration' policy', 17 *IEEE Internet Computing* 42 (2013). For details please see discussion below p**.

[17] Mozur, P., Baidu and CloudFlare Boost Users Over China's Great Firewall, NY Times, 13 September 2015 at https://www.nytimes.com/2015/09/14/business/partnership-boosts-users-over-chinas-great-firewall.html

[18] See s.296, s.296ZA-ZG CDPA 1988 and in the US, 17 USC §1201 and §1202.

the physical restrictions may be caused by the technology. Prior to the digital era, innumerable theories had been developed to assess how the State may regulate the ability of persons to do what they otherwise may want to do through the use of technologies more generally.[19] One of these was the concept of the Panopticon penitentiary put forward by Jeremy Bentham in 1791:

> *'.. An inspection tower atop the well, in conjunction with a method for lighting the cells and leaving the inspection tower dark, made it possible for one person to monitor the activity of many people, each of whom would know he or she was under surveillance, none of whom would know exactly when ... It was precisely this mental state of being seen without being able to see the watcher that Bentham meant to induce. When you can induce that state of mind in a population, you don't need whips and chains to restrain them from rebelling*[20].

The doctrine demonstrates that there are physical ways of creating a penitentiary so as to create discomfort among prisoners to make them always feel observed. However, the theory also concerns possible physical limitations in the construction the building;[21] these might inhibit the 'Panopticon' effect. The panopticon notion has been used in the context of the Internet.[22] An Internet panopticon is not limited by the existing physicalities of bricks. Internet users can never be sure whether their actions are being monitored or not. Nonetheless, individuals do retain the power to be able to try and circumvent the panopticon element, in the same way a prisoner could dig away at bricks. A computer user could use another person's login codes, they could use obscure operating systems, or run software that hides an IP address. However, they can never know for sure. Furthermore, the computer, as mentioned earlier, is reliant on the physical, real, world for its existence. If a computer cannot run any programs other than, say, Internet Explorer, then the computer user cannot use any other programs to limit the 'Panopticon fear'. This is why China has attempted to require computers sold in the PRC to have certain software installed upon them, e.g. 绿坝·花季护航.[23] That software was designed to control Internet access on computers, by having a black list of pornography websites which could not be circumvented.

If a State wants to have control over the users of a network, then the use of a closed style system is preferable. The open nature of the Internet poses an issue, in that users can interact with it reasonably freely. As noted at the start of this paper, the foundation stone of the Internet is TCP/IP, which is based around discoverability.[24] Attempts are made to try to limit the Internet and technology in a way to make it fit with the characteristics of a closed network (e.g. by using filtering to block certain websites), but the focus of the State needs to be on the issue of discoverability for enforcement. For States such as the PRC, the Internet represents an

---

[19] Space precludes a detailed footnote but examples could include Plato, The Republic (380BC); Aristotle (see Allan, The Philosophy of Aristotle, OUP (1970)), Cicero, De Officius (44 BC); Moore, T., Utopia (1516); more recently see Giddens, A., The Constitution of Society, Polity Press (1984); Deleuze and Guattari, A Thousand Plateaus, Continuum (2004); Deleuze and Guattari, Anti-Oedipus (1977; Continuum (2004)). For discussion see Griffin J., State of Creativity, infra n. 11 Chapters 2-3.

[20] Rheingold, H., 'The Virtual Community: Homesteading on the Electronic Frontier', Harperperennial, New York, 1994 at 289; Bentham, J., The Panopticon Writings, Verso (1995).

[21] Bentham, J., The Panopticon Writings, Verso (1995), ibid., Letter II onwards.

[22] Rheingold, H., 'The Virtual Community: Homesteading on the Electronic Frontier', supra n. 20.

[23] 'Green Dam Youth Escort.' For details see http://news.cctv.com/special/yangshiwangtan/01/03/index.shtml ; https://web.archive.org/web/20111117105716/http://www.lssw365.net:80/. Note that prior to the demise of the system, it became voluntary.

[24] See above p.**.

uncomfortable anarchy at odds with the relatively tight control of the traditional print press. [25] The PRC has a 'Great Firewall" system, governed by operation Golden Shield,[26] and users remain individually identifiable in a wide range of circumstances.[27] As a consequence, the State can take hold of the reigns of the physicalities of the networks, to utilise these to verify the existence and actions of individuals.

In contrast to the UK, a computer user in the PRC is explicitly made synonymous with the computer being used to access the Internet. It is necessary for the user to fill out a number of papers and provide an ID card and *rukou* document.[28] Included among these is the initial police file report form, which has to be filled out in triplicate. One copy is for the ISP, another is for the local PSB (Police Security Bureau), and the third for the provincial level PSB computer security and supervision office.[29] There is also a Net Access Responsibility Agreement that must be completed. Finally, there is the application form for the ISP itself. [30] The application form also requires a great deal of personal information to be provided. It is necessary for the user to state *inter alia* where they live and work, their profession, and their home and office telephone numbers. Details of the computer equipment must be provided, the connection type, and even the connecting device's serial number.[31] The ISP will therefore hold all these details about everyone who uses its service, and certain websites can gain details of who access their websites.

Physical content control in the PRC has been typically achieved in two ways. One is to place traditional censorship upon a website, requiring particular pages to be read by a human censor. The other method was to reduce the ease of publishing on the web, by reducing access to the DNS system.[32] This makes clear the threat of legal action if the user performs a 'wrong'. In the PRC the print media is very closely regulated, and the State makes clear that Internet users will be treated in the same way as traditional book publishers. In other words, if a user is seeking to create content on the Internet, there is no reason why they should be treated differently to those using traditional printing presses. Originally, the PRC system of censorship began to emerge in the Internet Cafes, [33] and the Chinese Firewall, although blocking has occasionally been arbitrary because of the volume of content that exists. In the PRC, there has been an increase in surveillance over the content that individuals decide to access.[34] In 2000, the Golden

---

[25] Liang, C., 'Red light, green light: Has the PRC achieved its goals through the 2000 Internet regulations?' 34 *Vanderbilt Journal of Trans-national law* 1417 (2001) at 1429.

[26] See above p.**.

[27] Barme, G., and Ye, S., 'The Great Firewall of China', Wired Issue 5.06 (June 1997) at https://www.wired.com/1997/06/china-3/

[28] Details of the requirements for .cn domains can also be found at: http://cnnic.com.cn/IS/CNym/cnymyhfaq/ ; see also Fu K., Chan C., Chau, M., 'Assessing censorship on microblogs in China: Discriminatory keyword analysis and impact evaluation of the 'real name registration' policy', 17 *IEEE Internet Computing* 42 (2013).

[29] Barme, G., and Ye, S., 'The Great Firewall of China', Wired Issue 5.06 (June 1997) *supra* n.27.

[30] *Ibid*.

[31] *Ibid*.

[32] 'While most western countries have an open and liberalised domain name registration system, the Chinese system represents the government's rigid and suspicious attitude towards the Internet, which always has been subject to public criticism' Wang, J., 'The Internet and e-commerce in China: Regulations, Judicial Views, and Government Policies' 18 *Computer and Internet Law* 12 (2001) Unlike the US where any individual or entity who has a valid credit card can apply for a top level domain name within a few minutes, the PRC's domain name registration is open only to entities and organisations that are incorporated or registered under Chinese law.

[33] The system has the potential to be most rigorously enforced in physical areas such as Internet Cafes. When visiting an Internet Café, it is necessary to fill in the Police File Report Form, the Net Access Responsibility Agreement, and an ISP contract. The contract states that 'if anything out of the ordinary is discovered … you will be fined accordingly'.

[34] Feir, S., 'Regulations restricting Internet access: Attempted repair of rupture in China's Great Wall restraining

Shield Project was initiated, which was designed to "strengthen central police control, responsiveness, and crime combating capability, so as to improve the efficiency and effectiveness of police work"[35]. It created a database driven surveillance system, offering immediate access to registration records of every citizen. It has been suggested that the system is largely based on one by a Canadian company.[36]

The important thing to realise is that the network is essentially a surveillance network that is "intended to be able to see, to hear, and to think";[37] to identify individual subscribers when they logon, matching names to IP addresses, and learning over time what interests the subscriber. To be able to do this it is heavily reliant on the co-operation of ISPs. In the PRC, these are much more closely tied to the Government than UK ISPs tend to be. The Golden Shield project fits in at the 'subscriber edge', namely the aggregation point in the service provider's network where the subscriber meets the network. It is the only point in the network where the service provider has complete knowledge, control and visibility of the subscriber and his or her traffic flows.[38]

The PRC has implemented a system of censorship that anticipates future uses. There is a very close parallel to this in certain CMI and DRM systems, but the methods used within these systems are currently more primitive. There are, for instance, DRM-CMI which prevent individuals from being able to photocopy or scan banknotes, e.g. in photocopiers or the computer program Photoshop.[39] In other words, there is an assumption that someone who scans in a banknote is likely to do so for the purpose of committing an illegal (or otherwise undesired) act.[40] The PRC Golden Shield system goes far beyond the sort of presumptive systems employed in photocopiers and Photoshop. Golden Shield can make an educated guess of an individual's movement, through CCTV cameras, reading car number plates, scanning hotel records, and so on. Those elements in isolation are not in themselves anything outstanding; but the system can combine all of these elements together to assess if an individual is a risk (or not) to the State. If this is put into the context of the computer user, then the implications are clear: Visiting certain websites, performing certain acts, may label the user as a State risk. The result might vary from a lack of access to certain content, to imprisonment; in contrast, in the UK, this be aimed at a) whether one is a threat to the lives of others as a terrorist under national security rules, or b) has committed infringement of a copyright property.

---

the free exchange of ideas', 6 *Pacific Rim Law and Policy Journal* 361 (1997) at 380.

[35] Walton, G., 'China's Golden Shield: Corporations and the Development of Surveillance Technology in the PRC' *Rights and Democracy (International Centre for Human Rights and Democratic Development)* at http://go.openflows.org/#

[36] www.nortelnetworks.com. This company were developing software advertised thus: "… imagine instead of finding your web content, it finds you. Sounds personal? Exactly" (from www.nortelnetworks.com, as accessed in 2004). See inter alia Leydon, J., 'Nortel helping China to overhaul state surveillance architecture' The IT Register at https://www.theregister.co.uk/2001/10/22/nortel_helping_china_to_overhaul/

[37] Walton, G., 'China's Golden Shield: Corporations and the Development of Surveillance Technology in the PRC' *supra* n.35.

[38] In the PRC, for instance, ICPs (Internet Content Providers) are required to maintain records of all the information that has been posted on their websites, and all the users who have dialled onto their servers for the last 60 days. Websites normally display a certificate to show that they have performed the appropriate registrations.

[39] See for example Naramiuk, C., 'The Secret Code of Banknotes' (BBC Future) at https://www.bbc.com/future/article/20150624-the-secret-codes-of-british-banknotes; for the software in Adobe Photoshop, see Anon, 'Photoshop and CDS' at https://helpx.adobe.com/photoshop/cds.html

[40] See Anon, *ibid*.

2. Are we entering an era where digital technologies will increasingly be used for State enforcement?

The code system used in China's Golden Shield system is essentially making the State an integral element in the running and physical existence of digital technologies. The State is in effect becoming akin to computer code, taking on the characteristics and abilities of the computer coder, yet able to influence the experience of the individual, both through the digital and through physical sanctions. Digital technology is being used to enforce physical world conduct – a means to enhance already existing structures of physical control.

Where Golden Shield moves away from the traditional DRM or CMI systems is that it is enforcing policing methods that exist in the physical world. DRM and CMI mechanisms are invariably seeking to create enhanced methods of control *within* digital technology. When technology begins to shift towards Golden Shield type systems, we can see a replication of enhanced methods of control that find their way into physical policing methods, controlling the actions of the individual using digital technology.

2a. Digital systems developed in the UK for physical enforcement

In the UK, one would have believed that there was merely limited observation of the actions of users of the Internet - until the revelations of Edward Snowden and Bernard Manning. This revealed that the 'five eyes' surveillance systems of the US, UK, Canada, Australia and New Zealand had also been collecting vast amounts of information about individuals use of the Internet.[41] For instance, there was the ability to record emails from the majority of mainstream service providers, chat, videos, photos, stored data, VoIP, file transfers, logins and so forth.[42] The UK is regulated through the Investigatory Powers Act 2016[43] which requires ISPs to store data about websites visited amongst other data.[44] The more integrated system of the Internet with the State means that information can be more easily accessible to law enforcement agencies.[45] The computer connecting to the Internet is becoming not just a computer – but an identifiable individual who will be held responsible for his or her actions.

What is perhaps most pertinent to remember is that the UK systems of surveillance are, in day to day use, those that are used against individuals who infringe commercial copyrights rather than those who somehow are perceived to endanger the State. The above 'Five Eyes' system is therefore very limited in day to day use. It would be unlikely that UK surveillance controls would be utilised against someone who, for example, challenged the opinions of the ruling UK Conservative Party. It is more concerned with copyright infringement, and thus enforcement is more focused on protection of commercial interests than the State. This is consistent with the history of UK copyright law, based as it is upon the system of commercial regulation since the time of Henry VIII.[46] State symbiosis is thus arriving under that system of commercially based

---

[41] The Guardian, NSA files decoded, available at https://www.theguardian.com/us-news/the-nsa-files (accessed 30th December 2019); Snowden PPT available at https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[42] *Ibid*.

[43] Investigatory Powers Act 2016 c.25.

[44] See s.62 Investigatory Powers Act 2016 *ibid*.

[45] The nature of the State also means that an aggrieved copyright holder could, if he had enough *guanxi* with the relevant officials, be able to obtain details of potential copyright infringers.

[46] For discussion see Feather, J., 'The Book Trade in Politics' 8 *Publishing History* 19 (1980); Griffin, J.,

regulation rather than one of wider censorship. That does not mean that the regulation is any more 'nefarious' than that of the PRC– both concern access to information, and can restrict this to an equivalent degree. The subject matter is naturally different, but both systems have the ability to shape the thoughts of the individual through limiting access to content, particularly when this is linked to physical sanctions. In the PRC, this will be political thought; in the UK, this will be where the boundaries of IP are considered to be infringed under copyright laws. As is argued below, the system in the PRC is increasingly making the State an integral element of the day-to-day life of the digital user; the question this article poses is whether we are likely to see something similar occur in the UK, and whether or not we wish to take a different path.

As UK enforcement measures develop, they are increasingly resembling the PRC Golden Shield system of enforcement. In the PRC, the focus remains firmly on the 'gateways' of access under Golden Shield. In the UK, companies can utilise the Norwich Pharmacal Order system[47] for the sending of letters to individuals, which has been subsequently endorsed by Justice Arnold in the *Golden Eye* case.[48] This requires ISPs to reveal user details. There is very limited regulation of the making of copyright threats, since copyright is not regulated by Statute unlike other areas of Intellectual Property such as Trade Marks or Patents.[49] However, there are other methods to enforce copyrights, again aimed at the content gateways - right holders can threaten to utilise s.97A CDPA 1988 in order to obtain blocking orders against infringing websites; there is the possibility of requiring filtering under EU law;[50] there is the possibility to seek secondary infringement,[51] a breach of authorisation,[52] and potentially inducement proceedings.[53] There are also the filtering mechanisms referred to in the 2019 EU Copyright Directive,[54] and there are also the attempts to enable digital licensing through the Digital Copyright Exchange (or Copyright Hub as it is also known).[55]

Although suing individuals for infringement has been a popular pastime in the UK,[56] there is an issue in linking the user with an IP address. Unlike the PRC, where an IP address is clearly allocated to one individual, in the UK they are dynamically allocated by an ISP. Even when a user is identified through an IP address, because of the way an ISP allocates addresses, mistakes can be made.[57] Furthermore, an ISP is not under an obligation to reveal the identity of a user directly to the right holder; this remains so due to the failure to implement s.3 and s.4 of the

---

'The State of Creativity' Edward Elgar (2019) Chapters 2 - 4; Putnam, G., Books and Their Makers in the Middle Ages, Putnam and Sons (1897) Volumes I & II.

.

[47] *Norwich Pharmacal Co. & Others* v *Customs and Excise Commissioners* [1974] AC 133

[48] *Golden Eye* v *Ben Dover Productions* [2013] RPC 18

[49] s.21 Trade Marks Act 1994, s70 Patents Act 1977.

[50] C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v *Netlog NV* [2012] 2 CMLR 18; C-70/10 *Scarlet Extended SA* v *SABAM* [2012] ECDR 4

[51] See e.g. s.22-27 CDPA 1988.

[52] See s.16 CDPA 1988; *Century Fox Film Corp* v *Newzbin Ltd* [2010] EWHC 608 (Ch)

[53] Inducement has been used in the US not the UK: For the US see Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. 125 S.Ct. 2764 U.S., 200 (Sup. Ct., 2005) but note this was adapted from patent law – in the UK, there is the same doctrine in patent and there is no reason why it could not be similarly transposed -see Unilever Plc. v Gillette (U.K.) Limited [1989] R.P.C. 583 (CA).

[54] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC Article 17.

[55] http://www.copyrighthub.org/

[56] See inter alia Griffin, J., and Nair, A., 'Scientia potentia est: Making threats of copyright infringement', 27 *International Review of Computers, Law and Technology* 1 (2013)

[57] See, for example, http://www.theregister.co.uk/2003/09/24/riaa_withdraws_300m_lawsuit_against/

Digital Economy Act 2010.[58] This is why there has been more of a focus in recent years on website blocking and filtering, as mentioned above. Nonetheless, as time progresses, the overall means of enforcement are becoming increasingly digital in form, and ever more resembling the PRC Golden Shield system. Code is being used to reinforce physical action, e.g. a legal order to block a website is then enforced through the IP system and subsequent filtering technologies. Importantly, this is becoming increasingly precise and directed towards individuals for particular actions, e.g. as is the case with *Norwich Pharmacal* actions (above). There is a clear link, increasingly, between these enforcement actions and the systems used in the PRC.

In the UK, the State has generally not been directly involved in the prosecution of individuals, except for the notable areas of State security and criminal law enforcement.[59] As noted above, the focus has been more on private companies initiating lawsuits, not the State itself. However, this should not deflect focus from the rise of digital style methods of regulation, which can interact with the individual at a micro level. Let us not forget the history of the regulation concerning Digital Rights Management mechanisms, which ended up with the phrase "access" becoming the all-encompassing mechanism of protection rather than "copyright."[60] That came about because everything on a computer needs to be accessed, and consequently the references to "access" in the Statute became all encompassing, leading to a situation where protection may extend beyond copyright.[61] History could repeat itself with PRC Golden Shield style regulation, where technological *access* to content is controlled by companies utilising a breadth of enforcement mechanisms, rather than the more traditional UK passive style of *ex post* cultural control, such as copyright infringement.

2b. Does this represent a shift in the paradigm of physical control?

In the PRC, with strong State regulation, the State is keen to control the actual creation and receipt of content, whereas in the UK, we tend to focus more on seeking to control the receipt of information after its creation. Thus, in the PRC a user must sign up to various agreements and reveal their identity, whereas the UK model tends to suggest that identity will be revealed only after an event such as a copyright infringement action.

In the UK, an individual may indeed feel fear of legal prosecution for downloading an unauthorised copy of copyright content.[62] However, in the PRC, detection is more difficult - and certainly more awkward - to avoid; and the legal action is more likely to be brought by the Government, not a private party, and is for a different aim. As all Internet access points are monitored, the user only really has two options by which to avoid detection. Firstly, the user could open a new unauthorised access point to the Internet, but the user is likely to be detected by the monitoring systems employed by the Chinese telecommunication networks.[63] Secondly,

---

[58] Griffin, J., "The Digital Economy Act 2010 and the impact on semiotic certainty" 24 International Review of Law, Computers and Technology 251 (2010).
[59] *Infra* section 3. See also Lilley, P., 'Hacked ,Attacked, Abused: Digital Crime Exposed', Kogan Page (2002).
[60] Efroni, Z., 'Access Right,' OUP (2011); Rifkin, J., 'The Age of Access', Penguin Books (2000).
[61] Reese, Will merging access controls and rights controls undermine the structure of anticircumvention law? 18 Berkeley Technology Law Review 619 [2003]; also see *Universal City Studios* v *Reimerdes* 111 F.Supp.2d 294 S.D.N.Y., 2000; *Chamberlain Group, Inc* v *Skylink Technologies, Inc* 381 F.3d 1178 (Federal Circuit, 2004); *MDY Industries, LLC* v *Blizzard Entertainment, Inc* 629 F.3d 928 (9th Cir. 2010)
[62] Consider the notion of wriggle room – see Griffin, J. State of Creativity, Edward Elgar (2019) Chapter 9; with reference to Helberger, N., and Hugenholtz, P., 'No place like home for making a copy: Private copying in European copyright law and consumer law,' 22 *Berkeley Technology Law Journal* 1061 (2007).
[63] Note, though, the recent attempt to run a satellite based Internet access point: Greenburg, A., 'The Ingenious

the user could seek to use proxy servers to try to hide the IP address, but, again, this is also easily detectable and at the time of writing increasingly less likely to succeed. Other filtering mechanisms could also be used to detect 'forbidden' content that is being viewed or posted. The difference is that in the UK, it is possible to use such techniques more safely. This is because the ISP is not required to release the details of the user, and because IP addresses are not linked to an individual. Furthermore, if a proxy chain is being used, then the proxies are not likely to be blocked. This is because there is no central blocking mechanism led by the State. It may therefore be concluded that in the UK, a skilled user is more likely to be able to avoid detection. However, the net is closing, due to the increasing variety of enforcement mechanisms discussed in the previous section.

3. Physical feedback: the use of physical control being fed back into digital code

So far the focus of discussion has been on the development of Golden Shield style systems that revolve around the use of physical force through existing technology. However, it is important to consider the other side of the coin, namely the development of the technological mechanisms that allow for closer control and monitoring of the user within the content itself. These can then enable a content provider to have considerably closer control of the user than even the Golden Shield style systems. Furthermore, it is argued, these systems will become more prevalent with the rise in bleeding edge technologies such as 3D printing and augmented reality.[64]

The initial steps in the development of private user focused technology in the UK begins with the use of 'cookies' in Internet browsers for the purpose of targeted advertising;[65] this has now become a similarly important integral element in social media sites and streaming services.[66] With these services a user must identify themselves, rather than simply identifying their computer. The verification points for obtaining 'premium' content are becoming increasingly synonymous with traditional credit card verification procedures.[67] This creates the impression that to break into a verification point is as morally reprehensible as stealing someone's credit card details. Indeed, one cannot fail to notice that many of the mechanisms for seeking to restrict the reproduction of copyright content closely mirror bank protection mechanisms, and likewise, State enforcement mechanisms such as Golden Shield. Indeed, research previously undertaken by the author revealed that some of the technologies utilised by States for the purpose of State enforcement have found their way into some of the surveillance systems used by private companies, such as those running streaming services.[68]

It is increasingly the case that goods provided through these sites may only be accessed one at a time, and that the goods may reside only within a controlled environment allowing no (or

---

Way Iranians are using satellite TV to beam in banned Internet' at https://www.wired.com/2016/04/ingenious-way-iranians-using-satellite-tv-beam-banned-data/ (15 Jan 2020); Koetsier, J., 'Elon Musk's 42,000 StarLink satellites could just save the world' at https://www.forbes.com/sites/johnkoetsier/2020/01/09/elon-musks-42000-starlink-satellites-could-just-save-the-world/#165eb45e4c2c (9th January 2020).

[64] Griffin, J., 'A proposal for a bridge of licensing over a sea of IP uncertainty: Digital Watermarking of 3D Printed Content' in Chan, H., Choo, Griffin J., and Osuji O., (eds), 'Intellectual Property Rights and Emerging Technology: 3D printing in China', Routledge (2018).

[65] Whalen, D., 'The unofficial Cookie FAQ' available at http://www.cookiecentral.com/faq/

[66] Consider e.g. Facebook – Consumer Report – St John, A., How Facebook Tracks You, Even When You're Not on Facebook, at https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/

[67] Efroni, Z., 'Access Right,'; Rifkin, J., Age of Access, infra n.60 and the orange book Rifkin Age of access.

[68] From empirical interviews, evidence on file with the author (SLS and RIVENTA funded research, see https://socialsciences.exeter.ac.uk/law/research/projects/project/?id=249 and https://socialsciences.exeter.ac.uk/law/research/projects/project/?id=237)

few) copies. If any content is reproduced, it is often possible for the content provider to ascertain from where the content originated. Watermarks can enable a right holder to track the use of their works.[69] Such tracking may be done through the use of digital watermarks or serial codes, which can be traced or reported back to the content originator. This is essentially the system that was proposed by Shawn Fanning within his Snocap project, whereby content providers can trace (and charge for) the distribution of their content across P2P networks.[70]

Those in charge of these access points have a high level of control over users. They will have user accounts on record (often with information on record to identify the user in person), and have the potential to reveal these records to other parties, or to suspend user accounts. They know exactly what content they distrubute. It will be recalled that Golden Shield could predict the actions of users. The mechanisms for this are gradually appearing in the context of access-controlled content websites. For instance, websites may predict the sort of content that a user may prefer to view. It is a small step from such a system to using systems to detect the uses made of the works used from the website – especially if the website aids such use. As such, users may be graded on the potential risk that they pose to a particular site because of unauthorised acts.[71] The consequence of this could be a reinstatement of real-world norms. If digital technology is increasingly used to enforce policing in the real world, then real-world policing can influence digital technologies and their operation. When this power is placed in the hands of the State, the implications are enormous. As noted above, individuals cannot simply 'turn off' the State in the same way that they may 'turn off' a computer.[72]

4. A proposal

To summarise, there are therefore three key scenarios that arise in the consideration of how digital technology and physical enforcement interact. The first is where digital technology is used to control other digital technology; the second is where digital technology is used to enhance physical real world enforcement of law, and the third is a situation of bleed back from the second scenario to the first, where physical real world enforcement is used to control digital code. All scenarios present a situation where the physical enforcement of law can be enhanced through the use of digital technology. This poses a challenge to the traditional boundaries of State enforcement. Whereas in the past the eyes of the State were greatly limited by the technology available to it, especially with regard to acts in the home, digital technology can place the eyes of the state into the private sphere to a greater degree than before.

It should be reiterated that the systems in the UK and those in the PRC have a different purpose; namely, the UK systems being utilised in situations of potential criminal conduct but principally for investigations of copyright infringement, whereas the PRC system is principally used for censorship purposes. Nonetheless, as has been identified above, the technologies are extremely similar in their nature, and the consequences similar in terms of the relationship of the State with the individual. The State and the activities of the individual become merged over both the intangible and tangible physical worlds, with digital technology having a direct impact upon the actions of individuals in the physical world.

---

[69] See e.g. Anderson, R., Petitcolas, F., 'On the limits of steganography', 16(4) IEEE Journal of Selected Areas in Communications 474 (1998); Griffin, J., 'A proposal for a bridge of licensing over a sea of IP uncertainty: Digital Watermarking of 3D Printed Content' *supra* n. 64.

[70] http://www.theregister.co.uk/2004/12/03/snocap_launch/

[71] For instance, some message boards require users to have a certain number of posts before the can access particular sections of the boards. On one website, it was only possible to obtain lists of servers hosting pirated software if 500 posts by the user had been made. Also see *supra* n.9.

[72] Infra p.**.

To simply revert back to pre-digital days is self-evidently a non-starter, wed as we are to our digital devices. With that in mind, regulators should be made mindful of overstepping the boundaries of State regulation. One way to achieve this would be to require State legislatures – and courts - to explicitly acknowledge and question how the use of digital technology in legal enforcement influences individual autonomy. The example of that given at the start of the paper, private copying, is a good example. Whilst private copying in the UK is not permitted under copyright law, right holders would have been extremely unlikely to have known about private copies being made. However, if a work is digital, and a copy is made on a device connected to the Internet, then there is always the possibility of a right holder being able to find out about the infringement. In that particular example, the reader might suggest that perhaps privacy rights would help to provide an answer. Indeed, requiring privacy assessments may be part of the plan to acknowledge how the use of digital technology influences enforcement, but it does not cover all scenarios where digital technology and physical enforcement combine. For example, would an otherwise general law on digital watermarking result in the ability to quickly identify individuals for infringing copyright files?[73] Privacy by itself might be ineffectual, since the results might be anonymised but still be used to adversely impact certain groups (e.g the results might be anonymous but it could limit Internet access to certain groups). Any consideration of the impact of digital technology on enforcement therefore needs to be flexible in terms of balancing; the core aspect is to consider whether or not the fundamental balance between individual and State is being considerably affected by the use of digital technology when it leads to physical enforcement. Perhaps the solution is for States and courts to consider whether or not the digital enforcement of law– rather than privacy - is being diminished by the use of digital technology in enforcement? There have been many suggestions made that certain subject matter should be kept outside of IP protection – e.g. public domain – but this paper suggests that perhaps focus should be more on the notion of how the method of enforcement has changed. This could take the form of a simple consideration of whether or not the ability of the individual to otherwise act freely has become diminished (e.g. in reproducing non-copyright elements from a copyright work); and if it has been, then should steps be taken to preserve that act? For instance, should the public in the UK still be able to make private copies? Does not doing so imperil the rationality of copyright law? Does it significantly alter the copyright balance? Will it limit the ability of some individuals to engage with society? Is that a considerable change from the current position? The proposal does not seek to merely reinforce the status quo – though that may well be an effect of it. What it wants to do is to provide a means for their to be debate, and a realisation, of how it is that digital technology influences the enforcement and therefore the relationship of the individual and the State.

5. Conclusion – the future

There is a need for legal regulatory processes to explicitly recognise the ability of digital technology to enhance the physical enforcement of law. There has been no legislative attempt, at the time of writing, to consider in depth the means by which such control could be achieved or the consequences thereof. Whilst there have been attempts through non-digital technology to control individuals, this has not previously provided such a level of control – for example, the printing press could not control the way in which readers used the work. The physical control of the user is the most powerful aspect of digital technology. This has become clear in the PRC, where the traditional press regulation would concern only the creation of works,

[73] Griffin, J., 'Biotech 3DP Digital Watermarking: An 'uncanny valley' in the Prosthetic State' in Chan, H., Choo, H., Griffin J., and Osuji, o., (eds), Intellectual Property Rights and Emerging Technology: 3D printing in China, Routledge (2018).

rather than the private use of those works. This was because it was not physically possible to control how works were used. However, that level of control now exists within the context of digital technology. This means that regulation of the media now does extend to how individuals use works, and not merely the creation of them. That has been made possible with the PRCs Great Firewall and the Golden Shield systems.

Digital technology feeds back into the real world. Countries such as the PRC have been able to take full advantage of the control aspect by restricting physical access points to the Internet as much as they can, whilst using other physical bottlenecks to restrict access to certain content. Thus, in the PRC, Internet content has been restricted to the nature of information that is reflective of those that are permitted to be sold in retail outlets. In the UK, physical access points are not so easy to control, so there is greater reliance on controlling the actions of Internet users by creating the threat of private copyright prosecution when they, for instance, infringe a copyright on the Internet. It is, indeed, reflective of the history of copyright in the UK, which was largely a system of censorship stemming from the time of Henry VIII that gradually became enforced by right holders;[74] the PRC system is similarly reflective of the history of the Chinese Communist Party and is still based around censorship.[75] Whilst the UK has a strong system of potential censorship control through the Investigatory Powers Act 2016, this is only invoked in exceptional circumstances and is not the usually invoked means of regulation. By contrast, in the PRC, the equivalent system is invoked on a daily basis for all Internet communications.

This article proposes that there should be an explicit realisation, by all States, of the wider physical nature of the consequences of their digital regulatory systems upon the end user, the citizen. By requiring States to explicitly consider the impact of the enforcement of legal regulations upon the individual, the State itself and citizens - in theory - will have the ability to at least potentially understand the broader consequences of the digital enforcement. In an era where we are increasingly moving towards ever closer integration with digital technologies, this enhanced scrutiny is critical.

[74] See Griffin, J., State of Creativity, Edward Elgar (2019) Chapters 1-4; Feather, J., 'The Book Trade in Politics' 8 *Publishing History* 19 (1980)

[75] Barme, G., and Ye, S., 'The Great Firewall of China', Wired Issue 5.06 (June 1997) *supra* n.27 at https://www.wired.com/1997/06/china-3/