The legal challenges of social media

Book section

Mapping the Rule of Law for the Internet

Andrew D. Murray

Abstract

Since its inception as a standalone topic of scholarship in the 1990s, the study of cyberlaw has been a study in regulatory theory. We have discussed systems of regulation and tools of regulatory enforcement. We have divided researchers into groups labelled as 'techno-deterministic' and 'libertarian/communitarian' and we have discussed regulatory effectiveness and legitimacy. The missing element of much cyberlaw study has been the law element. We have focused too extensively on the cyber and too little on the law. This chapter seeks to rebalance and refocus cyberlaw on the key element, the jurisprudential structure of cyberlaw, in particular to examine the question of the rule of law (or its absence) in cyberspace. In so doing it seeks to form the foundations of a cyberlaw jurisprudence by asking some difficult normative questions: Can a rule of law exist online? If so who is the legitimate lawmaker and what values are enshrined by cyberlaw?

Cyberlaw and Cyber-regulatory Theory

The title of this chapter may seem a little out of context for a book mapping the legal challenges of social media but hopefully over the course of the next few pages I can convince the reader of its utility and role in the wider context of the book as a whole. The challenge of social media regulation is a microcosm of the challenges of legal regulation of the internet as a whole, and lessons learned in the wider context can be applied in the narrower, and vice versa. Thus as one's

eyes are drawn down the list of chapters to be found in the book one sees clearly how the two are linked. Jacob Rowbottom's chapter on crime, communication and free expression is a chapter which can look inwardly at the regulation of social media platforms or outwardly at the normative question of values, culture and society in the global network context. The same is true of almost any chapter selected at random from the index such as Francois du Bois' chapter on reputation and dignity and Daithí Mac Síthigh's chapter on contempt. The macro becomes the micro and the micro the macro. It has become commonplace for the academic cyberlaw commentator to study the detail through micro-level analysis of a specific topic or challenge.[1] Arguably this represents a maturity of the subject. Just as the study of law involves the study of the application of developments and aspects of the law through specialist subjects of study: contract, torts, family law, corporate and commercial law, medical law and public law; the study of cyberlaw through the specialist aspects of cyberlaw: digital privacy and data protection law, protection of children, cybercrime, digital expression, and speech and jurisdiction, reflects the acceptance of cyberlaw as a distinct discipline of study within the wider field of legal study. This is despite the best efforts of early deniers such as Frank Easterbrook[2] and Joseph Sommer.[3]

[1] The list of such analyses is long and would include for example classic papers such as DR Sheridan's 'Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet' (1997-1998) 61 Alb L Rev 147 and Jacob Rowbottom's 'To rant, vent and converse: protecting low level digital speech' (2012) 71 CLJ 355 in the fields of defamation, speech and chilling effects, and Orin Kerr's 'Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't' (2003) 97 Northwestern University Law Review 607 or Daniel Solove's 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' (2002) 75 Southern California Law Review 1084 in digital privacy law.

[2] Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) University of Chicago Legal Forum 207.

[3] Joseph H. Sommer, 'Against Cyberlaw' (2000) 15 Berkeley Tech LJ 1145.

Arguably though what is missing from this contextual analysis of law in action in the cyberspace environment is the contribution of a jurisprudential analysis. Traditional legal analysis has the luxury of referring back to a rich jurisprudential framework and whereas cyberlaw, as the study of the application of legal normative principles in cyberspace, has access to that rich framework, we, that is scholars of cyberlaw, have as yet failed to make much in the way of meaningful contribution to the wider body of jurisprudence. That is not to say the contribution is not there. There is Chris Reed's excellent book *Making Laws for Cyberspace*,[4] and unique contributions from cyberlaw experts can be found in fields such as (digital) privacy rights[5] and digital expression.[6] However these contributions are uncommon, more commonly it is the micro analysis rather than the macro analysis that the academic cyberlawer engages in.

This is to be expected, it reflects the day-to-day work of the academic lawyer in 2016. We are detail oriented in a way a practicing lawyer cannot always be due to the pressure of work. The space afforded to the academic lawyer to look in detail at an application of the law to a specific cyberspace challenge has allowed for the production of a number of excellent books and papers in the last five years by academic cyberlawyers working in the UK.[7] The UK legal academic

[4] OUP, 2012.
[5] E.g. Julie Cohen, 'What Privacy is For' (2013) 126 Harvard Law Review 1904; Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.
[6] E.g. Jack M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 NYU Law Review 1; Cass Sunstein, *Republic.com 2.0* (Princeton University Press, 2007).
[7] E.g. Emily B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (CUP 2015); Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014); Jacob Rowbottom, 'In the Shadow of Big Media: Freedom of Expression, Participation and the Production of Knowledge Online' [2014] Public Law 491; Daithí Mac Síthigh, 'Virtual walls? The law of pseudo-public spaces' (2012) 8 International Journal of Law in

community is at the forefront of the analysis of the legal risks and responses to new media, especially social media, as this collection demonstrates. However the development of a distinct cyberspace jurisprudence remains stunted. Where we discuss theoretical aspects of cyberlaw (outwith the application of traditional jurisprudential theories to specific cyberlaw case studies) we tend to stray from the law to the wider fields of regulation and governance theory.

This can be tracked to the rise of the cyberpaternalist movement in the late 1990s, first seen in Joel Reidenberg's conceptualization of *Lex Informatica*.[8] In setting out his new model, Reidenberg identified two novel regulatory modalities arising from new rule-making processes for the online environment. The first consisted of the contractual agreements among Internet Service Providers (ISPs) and between ISPs and their customers. The second was to be found in the network architecture. Reidenberg argued, with some degree of success, that technical standards could function in a regulatory capacity. Using the network architecture as a proxy for regulatory architecture Reidenberg suggested a new way of looking at control and regulation in the online environment, a conceptualization he called *Lex Informatica*. Drawing upon the principle of *Lex Mercatoria* and referring to the 'laws' imposed on network users by technological capabilities and system design choices, Reidenberg asserted that whereas political governance processes usually establish the substantive laws of nation states, in *Lex Informatica* the primary sources of default rule-making are

Context 394; Ian Brown, 'Keeping Our Secrets? Designing Internet Technologies for the Public Good' (2014) 4 European Human Rights Law Review 368.

[8] Joel Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory Law Journal 911; Joel Reidenberg, 'Lex Informatica: The Formation of Information Policy Rules Through Technology' (1998) 76 Texas Law Review 553.

the technology developer(s) and the social processes through which customary uses of the technology evolve. To this end, he argued that the internet is closely regulated by its architecture.

Reidenberg contended that in the light of *Lex Informatica*'s dependence on design choices the attributes of public oversight associated with regulatory regimes could be maintained by shifting the focus of government actions away from direct regulation of cyberspace, toward influencing changes to its architecture. Reidenberg's concept of regulatory control implemented through the control mechanisms already in place in the network architecture led to development of the new cyberpaternalist school. This new school viewed legal controls as merely part of the network of effective regulatory controls in the online environment and suggested that lawmakers seeking to control the online activities of their citizens would seek to control these activities indirectly by mandating changes to the network architecture, or by supporting self-regulatory activities of network designers. This idea was most fully developed and explained by Professor Lawrence Lessig in his classic text *Code and Other Laws of Cyberspace*.[9] As the title reveals Lessig was influenced by Reidenberg's *Lex Informatica*[10] into developing his 'code is law' thesis. This posits that while there are four modalities of regulation: law, norms, markets and architecture, in cyberspace the regulatory effectiveness of three of these, law, norms and

[9] Basic Books, 1999.

[10] In truth Lessig had been working on a similar idea himself and indeed he and Reidenberg had been corresponding about their ideas as they developed them independently of each other. Earlier iterations of Lessig's 'Code' argument may be seen in Lawrence Lessig, 'The New Chicago School' (1998) 27 The Journal of Legal Studies 661 and Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501.

markets are reduced due to the nature of the space.[11] One modality though, as Reidenberg had predicted, is strengthened in the digital environment: the modality of architecture, or to use the label given to it by Lessig in relation to the digital environment 'code'.

Lessig's 'code is law', perhaps more correctly 'code as law', thesis quickly became the focal point of cyber-governance and cyber-regulatory discourse.[12] The discussion quickly recentred from the vibrant debate on the legitimacy of legal controls in cyberspace, which had been active prior to the publication of Reidenberg's and Lessig's works,[13] to a wider engagement on the role of regulatory modalities, and in particular the role played by code.[14] This arguably was the right direction for the academic discourse to move to at that time. It

[11] Due to effects such as remoteness, geographical limitations, anonymity and pseudonymity.
[12] The distinction between regulation and governance is one which has proven perennially difficult for regulatory theorists. Here the distinction applied is that regulation is 'the intentional use of authority to affect behaviour of a different party according to set standards, involving instruments of information-gathering and behaviour modification.' (Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World', (2001) 54 Current Legal Problems 103). Governance is a broader term than regulation. While the term governance has been given a wide range of meanings from varied literatures in the social sciences (see Kees Van Kersbergen & Frans Van Waarden, '"Governance" as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy (2004) 43 European Journal of Political Research 143) governance is understood (alongside government) as concerned with the provision and distribution of goods and services, as well as their regulation. Hence regulation is conceived as that large subset of governance that is primarily concerned with the purposive steering of the flow of events and behaviour, as opposed to providing and distributing (see John Braithwaite, David Levi-Faur & Cary Coglianese, 'Can regulation and governance make a difference?', (2007) 1 Regulation & Governance 1).
[13] David R Johnson & David G Post, 'Law And Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367; Jane C Ginsburg, 'Global Use/Territorial Rights: Private International Law questions of the Global Information Infrastructure' (1995) 42 Journal of the Copyright Society of the USA. 318; Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65 The University of Chicago Law Review 1199; Christopher M Kelly, 'The Cyberspace Separatism Fallacy' (1999) 34 Texas International Law Journal 413.
[14] Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (OUP 2006); Jonathan Zittrain, *The Future of the Internet: And How to Stop it* (OUP 2008); Andrew Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge 2006); Ian Brown & Christopher T Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013); Roger Brownsword, 'Code, Control, and Choice: why East is East and West is West' (2005) Legal Studies 1.

seemed that regulation was the key question for lawmakers and for the users of internet services. Early attempts at direct legal control, such as legal controls over Digital Rights Management (DRM) software found in the Digital Millennium Copyright Act[15] in the US and the Copyright and Related Rights in the Information Society Directive in the EU[16] had failed in their effectiveness, as had early content laws such as the Communications Decency Act.[17] It seemed that code controls such as AOL's strictly regulated online walled gardens were more likely to be effective.[18] In short Lessig's refocusing of the debate from questions of the legitimacy of legal controls in cyberspace to questions of the role and legitimacy of private regulators and the interface between East Coast Code (or law) and West Coast Code (or digital network and applications code) was important and timely. However arguably we, that is academic cyberlawyers, have remained entrenched in this analysis for too long. I count myself among the worst offenders having spent the bulk of the last fifteen years examining Lessig's models, but I am not the only offender. As the internet has matured it has evolved from a disruptive space into an established space. We see this in almost all aspects of the internet and its use today. The explosive development of disruptive e-business models so prevalent in the .com boom of the late 1990s has been displaced by a settled business environment with a relatively small number of key e-commerce providers (Amazon, Alibaba, JD, Ebay etc), the explosive growth of social media in the 2000s has settled into a few providers (Facebook, Twitter, Weibo, LinkedIn, tumblr) and the vast explosion in blogs and news

[15] Pub. L. 105–304.
[16] Dir. 2001/29/EC.
[17] Pub. L. 104-104.
[18] Lawrence Lessig, *Code Version 2.0* (Basic Books 2005) 88-94.

networks has mostly seen the accretion of a large number of personal blogs into more widespread and popular collective blogs. In essence the Internet has become less fractured and less chaotic as it has become more commercialized and commoditized. Counterintuitively this makes code less important and laws more important. As the network becomes what one may call a civilized space governments have become happier and more used to the idea of direct regulation through law, and as the parties providing the platform for activity are in many cases multi-million dollar, or even multi-billion dollar international corporations, they are used to legal controls and on the whole have been happy to help governments enforce legal controls. Thus recently we have seen a raft of legislative measures designed to legally control online activity. These include amendments to the Computer Misuse Act 1990 to regulate (distributed) denial of service attacks[19] and network attacks;[20] the introduction of specific legal controls on involuntary pornography;[21] and the promulgation of new provisions, and specific defences, in relation to online defamation.[22] In addition the courts have been busy and cases such as *Google Spain SL and Google Inc*. v *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[23] and *Maximillian Schrems* v *Data Protection Commissioner*[24] demonstrate a new form of judicial activism in dealing with online activity through the application of existing laws.

[19] As made by the Police and Justice Act 2006.
[20] As made by the Serious Crime Act 2015.
[21] Criminal Justice and Courts Act 2015, s33.
[22] Defamation Act 2013, s5.
[23] Case C-131/12 (2014).
[24] Case C-362/14 (2015).

There remains, though an elephant in the room, an assumption or supposition which we all make and which I ask the reader to consider. Are these legal orders, settlements and judgements, which we discuss in the assumption that they carry the full force of law, legitimate? We assume the legitimacy of the Defamation Act 2013, as applied specifically to online content, as it is an Act of the UK Parliament. This is not an unfair assumption but it is an assumption borne of the physical rather than digital world. The UK Parliament draws authority to regulate and control our acts from a number of sources depending on your flavour of legal positivism. If you are Austinian, something of a rarity these days, you point to the fact that Parliament is Sovereign (as the Queen in Parliament) and its acts are therefore laws.[25] If you are a Hartian, more likely today, you will apply the rule of recognition and find that the relevant officials such as Judges will recognize the Act as law, as will citizens.[26] You may not define yourself as a legal positivist – perhaps you prefer the interpretive approach of Ronald Dworkin, among others, and you may trust in Judge Hercules to interpret the body of law in such a way as to recognize the Act and apply its principles.[27] There are alternates to these competing tenets of law – there remains the vestiges of natural law found today in Fuller's Morality of Law,[28] the distinction between this and legal positivism being found, in Niki Lacey's words in 'the clear separation between our understanding of how to determine what the law is and

[25] John Austin, *Lectures on Jurisprudence: Or the Philosophy of Positive Law*, (1869, Reprint Forgotten Books 2015).
[26] HLA. Hart, *The Concept of Law* (Clarendon 1961).
[27] Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press 1977), Ronald Dworkin, *Law's Empire* (Harvard University Press 1986).
[28] Lon L Fuller, *The Morality of Law* (Yale University Press, 1964).

our criticisms or vision of what it ought to be'.[29] Then there is Polycentric Law perhaps for our purposes the most sophisticated modern jurisprudence the acceptance of private ordering (such as ADR) and the recognition of multiple overlapping sovereignties.[30] It is the one philosophical foundation of law which specifically acknowledges the internet.[31] At each turn though however you define your jurisprudential footing we are discussing a philosophy of legal order defined by reference to the "old world": the world of atoms, borders, sovereigns and lawmakers. Not the new world: the world of bits, pipes, networks and platforms. By turns we find ourselves, some twenty years on from the famous Chicago conference of 1996, returning to the questions that were active then. In the face of increasing legal interventions into online activity by both governments and judges: can a rule of law exist online? And if so who is the legitimate lawmaker and what values are enshrined by cyberlaws and cyberlawmaking?

Rule of Law

The astute reader may now suppose that I risk pursuing the wrong line of enquiry: to use a valuable analogy there is a risk going off down the wrong rabbit hole. They may say I am heading off down the rabbit hole called what is law? Or perhaps how does one define and recognize law, in other words the rabbit hole marked jurisprudence when you should be heading off down the rabbit hole entitled what is the rule of law – in other words following Dicey rather than Hart or Dworkin.

---

[29] Nicola Lacey, 'H.L.A. Hart's rule of law: the limits of philosophy in historical perspective' (2007) 36 Quaderni Fiorentini, 1203.
[30] Tom W Bell, 'Polycentric Law' (1991/92) 7(1) Institute for Humane Studies Review; Gerard Casey, 'Reflections on Legal Polycentrism' (2010) 22 Journal of Libertarian Studies 22.
[31] Casey ibid.

Except I think that as with so many things when we venture outwith the world of atoms and into the world of bits both rabbit holes lead us to the same Wonderland. So in the remainder of this chapter I'm going to follow both paths and see if we emerge into the same place – in so doing I'm hoping to begin by sketching out a map of where we may find a rule of law for cyberspace.

First I have a difficult definitional problem – No one seems to agree on what the rule of law actually is. Let's start with the formal or thin definition: 'At its core the rule of law, requires that government officials and citizens are bound by and act consistent with the law. This basic requirement entails a set of minimal characteristics: law must be set forth in advance (be prospective), be made public, be general, be clear, be stable and certain, and be applied to everyone according to its terms. In the absence of these characteristics, the rule of law cannot be satisfied.'[32] To this we may add thickness through concepts such as TRS Allan's principles of institutional fairness – 'ideas about individual liberty and natural justice, and, more generally, ideas about the requirements of justice and fairness in the relations between government and governed'[33] or thicker still through the incorporation of formal legality, individual rights, democracy, and a further qualitative dimension that might be roughly categorized under the label 'social welfare rights.'[34] We are in danger though as we thicken out understanding of the rule of law to depart from the core legal message an examination of society and inequality. I do not believe this is a role of the rule of law and more to the point

[32] Brian Z Tamanaha, 'A Concise Guide to the Rule of Law' in Gianluggi Palombella & Neil Walker, *Relocating the Rule of Law* (Hart 2008), 3.
[33] TRS Allan, *Law, Liberty and Justice: The Legal Foundations of British Constitutionalism* (Clarendon 1993) 21.
[34] Brian Z Tamanaha, 'The Rule of Law for Everyone?' (2002) 55 Current Legal Problems 97.

this is not necessary or relevant for my argument. I am going to remain wedded to the thin definition throughout the remainder of this chapter not because I necessarily believe it is the best definition (I actually like the thicker definition) but because it is the minimal definition and if I can demonstrate a failure in the rule of law at its thinnest the findings therein may be applied equally to thicker definitions.

Do we find the thin definition rule of law in the Internet? The answer I believe is no and I believe I can demonstrate this on both a theoretical and empirical level. To begin with the theoretical: We must start by defining our space and our participants. This was the root of that now long forgotten debate in the 1990s between libertarians and Berkman School paternalists.[35] As we may remember David Johnson and David Post argued that the Internet was not susceptible to legal control due to the lack of physical borders online and limits in territorial legitimacy:

> The determined seeker of prohibited communications can simply reconfigure his connection so as to appear to reside in a different location, outside the particular locality, state, or country. Because the Net is engineered to work on the basis of "logical," not geographical, locations, any attempt to defeat the independence of messages from physical locations would be as futile as an effort to tie an atom and a bit together. And, moreover, assertions of law-making authority over Net activities on the ground that those activities constitute "entry into" the

[35] See n 13 above.

physical jurisdiction can just as easily be made by any territorially based authority. If Minnesota law applies to gambling operations conducted on the World Wide Web because such operations foreseeably affect Minnesota residents, so, too, must the law of any physical jurisdiction from which those operations can be accessed. By asserting a right to regulate whatever its citizens may access on the Net, these local authorities are laying the predicate for an argument that Singapore or Iraq or any other sovereign can regulate the activities of U.S. companies operating in cyberspace from a location physically within the United States. All such Web-based activity, in this view, must be subject simultaneously to the laws of all territorial sovereigns.

Nor are the effects of online activities tied to geographically proximate locations. Information available on the World Wide Web is available simultaneously to anyone with a connection to the global network. The notion that the effects of an activity taking place on that Web site radiate from a physical location over a geographic map in concentric circles of decreasing intensity, however sensible that may be in the nonvirtual world, is incoherent when applied to Cyberspace. A Web site physically located in Brazil, to continue with that example, has no more of an effect on individuals in Brazil than does a Web site physically located in Belgium or Belize that is accessible in Brazil. Usenet discussion groups, to take another example, consist of continuously changing collections of messages that are routed from one network to another, with no

> centralized location at all; they exist, in effect, everywhere, nowhere in particular, and only on the Net.
>
> Territorial regulation of online activities serves neither the legitimacy nor the notice justifications. There is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group. The strongest claim to control comes from the participants themselves, and they could be anywhere.[36]

The paternalist response demonstrated the ability of regulators (lawmakers if you will) to leverage effective control.[37] Lessig's code argument remains a tour-de-force and illustrates that taking an external perspective, as outlined by Orin Kerr, allows us to treat the Internet like any other communications network: in Kerr's words 'the Internet is simply a network of computers located around the world and connected by wires and cables'.[38] Taking this approach Lessig and others demonstrated that Johnson and Post's argument was a simple enforcement argument not a normative one and it seems the entire debate moved on. From the point of the publication of *Code and Other Laws of Cyberspace* in 1999 the debate has been about accountability of regulators and legitimacy of the rule-making process, but there remained a part of the original Johnson and Post argument which was never fully answered by the external, paternalist, analysis. In his paper *What Larry Doesn't Get*, David Post argued that we should not be convinced by

[36] Johnson and Post, above n 13 at 1374-1375.
[37] See e.g. Reidenberg, above n 8 and Lessig, above n 9.
[38] Orin S. Kerr, 'The Problem of Perspective in Internet Law' (2003) 91 The Georgetown Law Journal 357 360.

Lessig's argument that without collective action the invisible hand of commerce will regulate.[39] In a section entitled 'the ought of it' he discussed the legitimacy of intervention into an organic community on the pretence of staving off the invisible hand. Here he returned to the earlier point made by himself and David Johnson – just because a government can regulate does not mean that they ought to regulate. If by making an intervention they act in an illegitimate manner they ought not to intervene. This is a basic tenet one may say of the most basic principle of the rule of law: government officials and citizens are bound by and act consistent with the law. An illegitimate act (assuming it is legally or procedurally inconstant not just morally inconsistent) is therefore a breach of the thin principle.

What Post and Johnson pointed out was that the acts of traditional state-based lawmakers will exceed their authority due to the borderless nature of the network. A decision by say a court in Sweden to close down The Pirate Bay affects not only citizens who are subject of the jurisdiction of that court but also citizens globally.[40] Thus if I am a UK based musician who distributes my content via The Pirate Bay, the decision of the Swedish court to close down the site affects me directly even though I am not subject to that jurisdiction or court. Similarly if say an English court orders that the identity of a philandering footballer must not be revealed and orders that a website upon which this may be found remove the

[39] David Post, 'What Larry Doesn't Get: A Libertarian Response to Code and Other Laws of Cyberspace' (2000) 52 Stanford Law Review 1439.
[40] Sweden v Neij et al. Case B 13301-06, Tingsrätt, Stockholm, 17 April 2009.

offending content or face an action in contempt this will affect individuals in Italy, Canada or even Scotland.[41]

Now you may say that the effects of the Swedish or English court decision are not strongly felt, the network will route itself around the legal intervention as if it were damage and everything will continue on as it were, UK citizens will still access The Pirate Bay and Scottish citizens will call the philandering footballer Ryan Giggs. This though is to miss the point that the act produced illegitimate, extra jurisdictional, effects: it was not in compliance with the rule of law. This though is only the start of our journey, for the response of the lawmaker faced with failure of their legal intervention is to create further and more restrictive legal interventions. We find that as a citizen subject to the courts of England and Wales offline we become subject to multiple overlapping legal controls online. Actions we complete, from Kerr's external viewpoint, in the comfort of our own homes *may* from the internal viewpoint be viewed as occurring elsewhere. Extradition for acts committed externally in the UK become possible from the internal viewpoint. This you may say is fanciful but let's look at a few individuals who have been caught up in this. In 2013 Yasir Afsar, a British Citizen, was subject to an extradition request from the United Arab Emirates.[42] He had threatened to place naked images of his ex-wife online unless she gave him money following their separation. He then allegedly sent a naked photograph of his ex-wife via

[41] The second example draws inspiration from the case of CTB v News Group Newspapers Limited [2011] EWHC 1326 (QB) and in particular the application CTB v Twitter, Inc. and Persons Unknown (Case No. HQ11X01814) which was withdrawn by the claimant.

[42] The Government of the United Arab Emirates v Yasir Afsar, Unrpt, Westminster Magistrates Court, 15 August 2013. Transcript available from: http://www.kaimtodner.com/news/2013/08/16/yasir_afsar_judgement.asp.

email to a common acquaintance. Although this may legally be blackmail in the UK he was not investigated or charged in the UK, instead the UAE government sought to extradite him for breach of UAE Federal Law No. 2 of 2006 on the prevention of Information Technology Crimes, Article 16 which provides: 'Whoever violates any of the family principles or values, published news or pictures violating the privacy of the private or family lives -even if true- through the information network or any other means of information technology shall be sentenced to imprisonment to a period of one year at least and a fine amounting to AED 50,000 at least, or to other penalties.' The maximum sentence set out in the Extradition Request was five years imprisonment. In the event the extradition was not allowed, not because there is no corresponding criminal provision in UK Law (or at least there was not at that time, one may argue whether s.33 of the Criminal Justice and Courts Act 2015 would be a corresponding provision) but because he was 'likely to be denied a fair trial' and would 'suffer prejudice because of his ethnicity'.[43] A not dissimilar case is that of Sheffield student Richard O'Dwyer. In 2012 he was the subject of an extradition request from the United States with regard to the operation of the TVShack website. The extradition request followed a decision of the Southern District Court in New York to bring two charges against him for criminal copyright infringement.[44] The two charges, conspiracy to commit copyright infringement and criminal infringement of copyright, each carried a potential maximum sentence of five years in prison. It is arguable that O'Dwyer's actions in operating a so-called linking website, that is one which does not host infringing materials but which links to where they may be found, was in accordance with UK Law as it

[43] ibid.
[44] USA v. O'Dwyer, New York Southern District Court, Case No. 1:10-mj-02471.

was understood at the time. He may have been in breach of s.107(2A) CDPA but the application of the admittedly non-binding Crown Court *Oinks Pink Palace*[45] and *TV Links*[46] cases, as well as the guidance on linking in *Shetland Times v Wills*,[47] suggested his actions were at least arguably legal in the UK. In January 2012 District Judge Quentin Purdey ordered O'Dwyer's extradition to the United States. He is reported to have said: 'there are said to be direct consequences of criminal activity by Richard O'Dwyer in the USA, albeit by him never leaving the north of England. Such a state of affairs does not demand a trial here if the competent UK authorities decline to act, and does, in my judgment, permit one in the USA.'[48] The extradition order was approved by UK Home Secretary Theresa May in March, 2012, and O'Dwyer launched an appeal. Then in November 2012, it was announced that O'Dwyer had signed a deferred prosecution agreement to avoid extradition. He was ordered to pay a fine of £20,000 and remain in contact with a US correctional officer over the next six months. In return, the United States would drop all charges.[49] Ultimately therefore O'Dwyer never stood trial in the United States for actions he committed, in the internal perspective in England, and strictly applying the external perspective in the Netherlands as that is where his content was hosted. The United States claimed jurisdiction solely on the basis that he used a .net domain name and which they claimed gave them the right to assert US laws globally, because American companies such as Verisign manage these domains.

---

[45] R v Alan Ellis T20087573 (Middlesborough Crown Court).
[46] R v Rock and Overton T20097013 (Gloucester Crown Court).
[47] 1997 SC 316.
[48] Peter Walker, '"Piracy" student loses US extradition battle over copyright infringement', *The Guardian* (London, 13 January 2012) http://www.theguardian.com/law/2012/jan/13/piracy-student-loses-us-extradition.
[49] Adam Gabbatt & Owen Bowcott, 'Richard O'Dwyer's two-year extradition ordeal ends in New York' *The Guardian* (London, 7 December 2012) http://www.theguardian.com/uk/2012/dec/06/richard-o-dwyer-avoids-us-extradition.

This was enough it seemed to force O'Dwyer to submit to US Federal Law and to force him to enter a plea agreement which saw him forced to close a website that at the very least was in a legal grey area in the UK, submit to a fine of £20,000 and agree to six months probationary supervision.

This is potentially the tip of a very large iceberg. Are you certain nothing you have ever said online has breached s.204 of Nigeria's Criminal Code?[50] What about s.133 of the Thai Criminal Code?[51] What does this mean for the rule of law? Let's return to our principles. The first principle is that law must be set forth in advance (be prospective). This will usually be the case whatever law is being applied and from whichever part of the world so this would appear to be satisfied. The second principle is that the law be made public. This is not quite so simple. While many laws from around the world are made available online not all are and where they are available many are not available in translation. This is a challenge for the rule of law if we accept the principle of extra-territorial effect (as I am arguing). The third principle is that the law be general. This would appear to be satisfied, although I don't know all laws in all jurisdictions which I may be made subject to. The fourth principle is that the law must be clear. Again there are some problems with this. Language aside there may be cultural references or procedural ones, which are unclear. Even something simple such as do not distribute indecent images of a child require one to know the age of majority. The fifth principle is that

[50] Any person who does an act which any class of persons consider as a public insult on their religion, with the intention that they should consider the act such an insult, and any person who does an unlawful act with the knowledge that any class of persons will consider it such an insult, is guilty of a misdemeanour, and is liable to imprisonment for two years.

[51] Whoever, defaming, insulting or threatening the Sovereign, Queen, Consort, Heir-apparent or Head of Foreign State, shall be imprisoned as from one year to seven years or fined as from two thousand to fourteen thousand Baht, or both.

the law must be stable and certain. It is clearly the case that individually each state may have stable laws in terms of the rule of law but collectively the law is inherently unstable and uncertain given the high level of 'churn' across all jurisdictions. For example in December 2013 I asked a room full of British experts on internet law whether the French HADOPI law [52] was still in force. The overwhelming majority of those present were unaware that the French Government had revoked it on 8 July 2013 because the penalties contained therein were considered to be disproportionate. The final principle is that the law be applied to everyone according to its terms. This appears to be satisfied but this may in fact be the problem. Individually each jurisdiction may comply with the thin definition of the rule of law but when we get extra-territorial impact, as we see occurring more and more the thin definition is undermined and the rule of law breaks down.

We are seeing this happen over and over in internet law terms. In the Kim DotCom (Megaupload) case we see a case similar to the O'Dwyer case but with greater publicity and higher stakes. The case which has now been on-going for four years saw an extradition request made in the New Zealand courts by the US Federal Government on grounds of racketeering, money laundering and criminal copyright infringement. The racketeering and money laundering charges stem from the alleged $175 million dollars generated by DotCom's Megaupload site from criminal copyright infringement. A series of cases have challenged the search

[52] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet.

and arrest warrants issued, the seizure of property and only recently has the extradition case begun.[53] Again the question of the relevance of the United States as a forum for this case is questionable. DotCom lives in New Zealand and the company is registered in Hong Kong. Megaupload would though lease server space and according to the extradition request some of the alleged pirated content was hosted in the US on leased servers in Ashburn, Virginia, which gave US authorities jurisdiction. This though was only a small part of the companies operation and although this clearly gave the US Federal authorities jurisdiction over that content, it is not the case this gives them jurisdiction over the entire global operation of the company. Surely that is better reserved to either New Zealand or Hong Kong? More recently the European Union has applied domestic EU law in an extraterritorial way which has attracted a lot of commentary, attention and even ire from the United States. In the case of *Google Spain SL v AEPD*,[54] the Court of Justice ruled the Google (and other similar Data Controllers) had to remove links to content relating to EU data subjects under Article 12(b) of the Data Protection Directive [55] which provides that 'Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive.' Although this is technically only of domestic effect, in that it only applies to those branches of the data controllers established in the EU, more recent decisions of domestic regulators are pushing this envelope with the Commission Nationale de l'Informatique et des Libertés

[53] AFP, 'Kim Dotcom case is "simple fraud", court told, *The Guardian* (London, 24 September 2015) http://www.theguardian.com/technology/2015/sep/24/kim-dotcom-case-is-simple-court-told.
[54] Case C-131/12, 13 May 2014.
[55] Dir. 95/46.

(CNIL) in France ordering Google to apply the so-called right to be forgotten principles not only to the company's European domains such as google.co.uk or google.fr, but to the their global domain google.com.[56] More recently the case of *Schrems v Data Protection Commissioner*[57] has had a more immediate direct effect. German Student Maximillian Schrems challenged the safe harbour agreement[58] agreed between the European Commission and the US Department of Commerce which allowed safe exportation of the data of EU citizens to the United States in compliance with Article 25 of the Data Protection Directive. He argued that data transfers from the EU to the United States by companies such as Facebook where such data could be accessed by national security agencies through programmes revealed by Edward Snowden such as PRISM demonstrated that the safe harbour could not adequately meet the principles set out in Article 25. The European Court of Justice agreed and finding that the protections afforded by the safe harbour were insufficient to provide protection to EU data subjects ruled the safe harbour agreement invalid. The result of this was to render illegal almost all data transfers from the EU to the US, a situation which has led to great concern from technology

[56] 'Right to delisting: Google informal appeal rejected' (*CNIL*, 21 September 2015) http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/.

[57] Case C-362/14, 6 October 2015.

[58] European Commission's Decision 2000/520/EC of 26 July 2000 'on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.'

companies[59] and the White House[60] and moves to negotiate a new safe harbour framework which is complaint with Data Protection Laws.[61]

These decisions all points to a fundamental flaw in the rule of law in the online environment. Online global is local and the application of domestic laws in a domestic environment can have a global impact as seen in the *Google Spain* and *Schrems* cases. Equally online local is global and the impacts of local activities can attract global attention as seen in the Afsar, O'Dwyer and DotCom cases. The rule of law is replaced by a rule of laws which at points overlap with and conflict with each other undermining the basic principles of the rule of law. The problem is the result of conflicting attempts to apply both the internal and external views of online content and activity.

Jurisprudence

Does our other rabbit hole lead, as I argued, to the same conclusion? Very bravely I'm going to attempt what I believe to be a foolhardy exercise. Ask whether or not the preceding analysis undermines Hart's Rule of Recognition on an individual state level? As we know the rule of recognition is a central part of Hart's Concept

---

[59] Robert Levine, 'Behind the European Privacy Ruling That's Confounding Silicon Valley' *The New York Times* (New York, 9 October 2015) http://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html?_r=0.

[60] Kieron McCarthy, 'White House "deeply disappointed" by Europe outlawing Silicon Valley' (*The Register*, 6 October 2015)http://www.theregister.co.uk/2015/10/06/white_house_safe_harbor_decision/.

[61] Ginger Hervey, 'EU hopes for new "safe harbor" deal with US by January' (*Politico*, 30 November 2015) http://www.politico.eu/article/eu-hopes-for-new-safe-harbor-deal-with-us-next-month-vera-us-reuters/.

of Law.[62] It is the fundamental rule by which all other rules are identified and understood. According to Hart, a legal system is primitive if it consists of just a series of primary rules that assign duties and obligations to the citizenry. This is because a society that issues only primary rules suffers from several deficiencies. To make up for those deficiencies, the society must issue secondary rules. These are of three types: rules of change, which allow primary rules to be extinguished or modified; rules of adjudication, which empower individuals to determine whether a primary rule has been broken; and, most importantly, the rule of recognition, which serves as an authoritative acknowledgment that the primary rules are the proper way of doing things. A legal system that contains these three types of secondary rules is, in Hart's view, fully developed.[63] In a gross simplification of Hart's position a rule or order becomes a law when it is recognized as such by the relevant officers of society. Of course the rule is much more sophisticated than this and learning to recognize laws (as opposed to other forms of rules) is complexified by the nature of modern complex legal systems. In modern systems with multiple sources of law, rules of recognition can be quite complex and require a hierarchy where some types rules overrule others. But, by far the most important function of the rule of recognition is that it allows us to determine the validity of a rule. Validity is what allows us to determine which rules should be considered laws, and therefore, which rules should create obligations for citizens with an internal perspective to the law. According to Hart, validity is not determined by whether a rule is obeyed, its morality, or its efficiency, but by whether it fits the criteria set forth by the rule of recognition. In more complex

[62] Above n 26.
[63] Ibid 91-99.

legal systems we may have to trace the origin of a rule back a few steps to the source of its authority.[64] In the context of Hart's definition of validity (whether the law is derived from a source and in a manner approved by other rules) it simply does not make sense to ask about the validity of the rule of recognition in its supreme form. Once we have reached the rule of recognition, there is no higher level of rules to provide us with the criteria with which to judge its validity.

What does this mean for our examples? One approach is to take the external view and to say that the rule is functioning perfectly well. Yasir Afsar was not extradited (in accordance with UK and Private Internal Law), Kim DotCom fights his day in court and Richard O'Dwyer reached a settlement (albeit one that cost him £20,000). Google may choose not to comply with the ruling of CNIL at which point should CNIL seek enforcement of the order it will become a question for the French, EU and potentially US courts in a manner not dissimilar to the classic Yahoo! France case of 2000. [65]Finally the European Commission and the United States Federal Government negotiate a new Safe Harbour with (hopefully) none of the shortcomings of the original. At each turn the participants in the legal system were dealt with in accordance with the law, the law as recognized by the participants in that system (themselves included). But on an internal level Richard O'Dwyer was regulated in his actions by a law alien to the English and Welsh legal system (admittedly with the compliance of the courts – I hold my hand up here this is a weak argument). We in the UK would not recognize the US Laws as valid

[64] Ibid 80-82.
[65] UEJF & LICRA v. Yahoo!, Inc. & Yahoo! France, Tribunal de Grande Instance de Paris, May 22, 2000.

within this jurisdiction so does this fail Hart's rule of recognition? Perhaps to borrow from another line of inquiry we are looking for Judge Hercules to protect us but instead we have to make do with Judge Achilles who seeks refuge in the rule of adjudication in determining the question of validity of external laws. This is because when viewed from Kerr's internal perspective the question is overwhelming and the only practical approach is therefore to rely on procedural rules and institutional values.

I believe that although we can rationalize the application of laws external to our jurisdiction in these internal internet cases through institutional value, doing so fails to acknowledge the elephant in the room (we have gone from Rabbits to Elephants) which is that Hart's rule of recognition expects commonality of experience, culture and political values; similarly Dworkin's Judge Hercules is someone who attains this role through common values, experience and culture, surely Dworkin does not expect Judge Hercules to be able to interpret English Law, US Federal and State Law and Burundian Law equally? More so than positivists, natural lawyers such as Fuller require commonality of experience, culture and society in asking the question – what is moral? Although some things may appear easy: murder, rape and theft are always immoral – is blasphemy always immoral? What about standards of taste and decency? Once one internalizes the concept of 'going to' or 'socializing' in the network our traditional legal foundations are under challenge and as international legal institutions and orders draw authority from the sovereign states which construct them so too do orders of international public and private law. I believe (in a less clear cut way) this rabbit hole leads to the same Wonderland. We have rules, laws even, for online actions, we can interpret how

the law applies to these actions but we need urgently to address the key question – are they legitimate.

Conclusion

I promised a map of where we could go to identify a rule of law for the internet. I'm afraid this chapter falls somewhat short of that. I can though tell you where the map is to be found. It is in Orin Kerr's divide between the internal and the external view of the network. For as long as lawmakers, courts and other adjudicatory bodies attempt to use both perspectives we will never have an effective rule of law for the internet. Too often authorities cherry pick whichever view they want to fit the situation they have before them so as Kerr notes when the US legal system allows prosecutors to choose to enforce either the external view (as in *United States v. Kammersell*[66] (bomb threat interstate)) and the internal view (as in *United States v. Thomas*[67] (obscenity distribution)) depending upon which is better for their case we can never have an effective rule of law for the internet. This is true on the micro level and truer on the macro (interjurisdictional) level. Hence I have my map, as now do you. We now just need to see where the road takes us.

[66] 196 F.3d 1137 (10th Cir. 1999).
[67] 74 F.3d 701 (6th Cir. 1996).