Legal Studies (2018), **38**, 263–278
doi:10.1017/lst.2017.15

S·L·S
The Society of Legal Scholars

RESEARCH ARTICLE

Why judges need jurisprudence in cyberspace

Chris Reed*

Professor of Electronic Commerce Law, CCLS, School of Law, Queen Mary University of London, London, UK
*Author email: chris.reed@qmul.ac.uk

(Accepted 6 August 2017)

Abstract

Judges are increasingly asked to decide whether a rule of national law is applicable to a cyberspace actor who is not present in their jurisdiction, or whose activities do not clearly fall within the established understanding of the rule. They do this through interpreting the applicability and meaning of the law.

Every attempt to enforce a national law makes a claim that the law has authority over the cyberspace actor. By accepting that claim, the judge asserts that the law's claim is legitimate. This is a Hartian exercise, adopting the internal view of the national legal system as the test for legitimacy.

But in cyberspace the legitimacy of a national law claim is determined not by the internal perspective of the legal system but by the external perspective of cyberspace actors. A law will only have authority in cyberspace if it can convince cyberspace actors that its claim is legitimate. And a legal system which repeatedly makes illegitimate claims thereby weakens its status as a system which adheres to the rule of law.

Judges can help solve this problem by interpreting laws and applying public and private international law so as to reject applicability claims which are illegitimate. To do this successfully, they need to understand the jurisprudential foundations of any law's authority in cyberspace.

Keywords: cyberspace; jurisprudence; legitimate authority

Introduction

Cyberspace transcends territorial boundaries. This means that an activity undertaken in cyberspace has the potential to occur, in whole or in part, within multiple nation states. The activity's effects might be felt in every member state.

This state of affairs gives rise to the biggest and most intractable problem of cyberspace law. If multiple nation states claim that their law is applicable to a particular activity undertaken by a particular cyberspace actor, and that their courts have jurisdiction, then which of those claims to authority are legitimate and ought therefore to be obeyed? A related question, which can arise even where there is no cross-border element involved, is how laws originally designed to regulate offline activities should most appropriately be applied where the activities take place in cyberspace.

Judges are required to answer these questions if a case is brought in their national courts. To date, however, few judges have taken the issue of legitimacy into account when making their decisions. Instead they have focused on their own national rules of public and private international law, and of substantive law.

In such cases judges have in practice a wide scope of freedom to decide whether and how to apply their national law or to take jurisdiction over a case, which can be exercised in three dimensions.

First, the vagueness of localisation concepts in cyberspace[1] gives judges ample scope to decide where relevant matters occurred or were geographically located. As a simple example, in *Moberg v*

[1]See further C Reed *Internet Law: Text and Materials* (Cambridge: Cambridge University Press, 2nd edn, 2004) ch 7; U Kohl *Jurisdiction and the Internet* (Cambridge: Cambridge University Press 2007); J Hörnle 'The jurisdictional challenge of the internet' in L Edwards and C Waelde (eds) *Law and the Internet* (Oxford: Hart, 3rd edn, 2009) ch 3.

© The Author 2018. Published by The Society of Legal Scholars

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

33T LLC[2] where a copyright work had been uploaded to a German-located web server, the court had to decide the geographical location where the work had been first published. The court's decision was that it had occurred in Germany only, but the court might with apparently equal justice have decided that it took place simultaneously world-wide.[3]

Secondly, judges also have scope, through interpreting the meaning of the substantive law, to decide whether what *did* happen in the jurisdiction falls within the meaning of the law. In *Euromarket Designs Inc v Peters and Crate & Barrel*[4] an Irish company traded via its website using a trade name which was registered as a UK trade mark. The English court held that the relevant act, 'use' of the mark, was not committed merely by making the mark visible in the UK, but required some attempt to solicit custom from UK residents. Again, it could legitimately have decided some different meaning for 'use' in this context.[5]

Finally, judges have discretion whether to make mandatory orders against unsuccessful cyberspace actor defendants in addition to awarding damages or imposing fines. A mandatory order, such as an injunction, de facto asserts that the national law is universally applicable and should therefore be obeyed by the cyberspace actor in its dealings with persons from other countries as well.[6] Damages or a fine alone permits the cyberspace actor to continue its activities unchanged if it is prepared to pay the costs of doing so and thus asserts, implicitly, that the law applies to dealings with nationals but makes no claim to authority over other dealings.

The purpose of this paper is not to investigate in detail the ways in which judges resolve these questions by reference to national law. Instead it proposes that in doing so, judges should consider the legitimacy of their national law's claims to authority. Merely by deciding that national law applies, the judge is implicitly making an assertion that the law's claim to authority is legitimate. If the judge accepts jurisdiction, this amounts to an assertion that the court has a legitimate claim to decide the case. And the natural tendency of any judge, faced with a novel cyberspace issue, is to analogise it to known activities for which the law provides a well-understood solution. This ignores the fundamental technological and social changes which cyberspace has produced.[7]

It should be uncontroversial that judges ought not to make illegitimate decisions, and legitimacy of law is the province of jurisprudence. But because scholars of jurisprudence have largely based their work inside the frame of national law, it may not be obvious to judges how the concept of legitimacy changes when applying national law to cyberspace activities. This is why judges in cyberspace matters need jurisprudence.

1. Constitutional legitimacy

The starting point for any judge is to decide whether the law in question meets the national legal system's requirements for legitimacy. This is an application of Hart's rule of recognition,[8] and focuses on

[2]666 F Supp 2d 415 (D Del 2009).

[3]As was decided on similar facts in *Kernal Records Oy v Mosley* 694 F 3d 1294 (11th Cir 2012). See Section 3(a), below, for the author's explanation of the difference between these two judgments.

[4][2000] EWHC (Ch) 453.

[5]See the contradictory decision in the US, *Euromarket Designs Inc v Crate & Barrel Ltd* 96 F Supp 2d 824 (ND Ill 2000).

[6]The CJEU decision in Case C-131/12 26 *Google Spain v AEPD & Costeja González* November 2014 did not go quite so far as to state this expressly when holding that the display of personal data in search results was subject to Spanish data protection law when it occurred 'in the context of' the commercial relationship between Google Inc and its Spanish advertising subsidiary, and that the Spanish data protection authority thus had power to make orders against Google Inc, a US corporation (paras 54–60). However, the Article 29 Working Party's *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12*, WP255 26 November 2014 specifically assert that the law applies to protect all individuals, world-wide (para 19), and that Google Inc must comply in relation to searches via its US-based .com search service as well as in its EU-domain denominated services (para 20).

[7]For an analysis of the defects of this approach see M Gillen 'Lawyers and cyberspace: seeing the elephant?' (2012) 9 SCRIPTed 130 at 136–138.

[8]HLA Hart *The Concept of Law* (Oxford: Oxford University Press, 2nd edn, 1994) chs V–VII.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

the source of the alleged law and the processes by which it was produced. This is normally described as constitutional legitimacy.

From the internal perspective of a legal system, this is the only question which needs to be asked.[9] The existence of the legal system is a given fact, and the judge is a part of that system. From that perspective the system itself is by definition legitimate, and so all laws properly emanating from the legal sources of the system have legitimate authority and should be enforced by the judge. Thus Hart's discussion of the idea of obligation[10] refers throughout to the group or society which, from its internal point of view, accepts the rules as imposing an obligation to act in conformity with them.

But a cyberspace actor who is not a citizen or resident of that nation state is not necessarily obliged to recognise the legitimate authority of all, or any, of its laws. The mere fact that a law is recognised as legitimate *within* a national legal system, because it meets that system's constitutional requirements, does not confer on it any legitimacy *outside* the boundaries of that legal system. This is because the constitutional approach to legitimacy is based on a legal paradox, as Luhmann has noted.[11] The legality of a constitution can only be determined by the law system established by that constitution, which therefore has to presuppose the constitution's legality in order to give itself power to decide the question. This paradox makes legitimacy, at its base, a political rather than a legal construct, and a matter of fact:

> An institution is legitimate in the sociological sense when it is widely believed to have the right to rule.[12]

As a consequence, a cyberspace actor who is not a party to the political settlement which constitutes the nation state is not under an obligation to recognise the legitimacy of its legal system, and thus the rules of law emanating from that legal system.

From the judge's perspective, therefore, constitutional legitimacy should only be the starting point when deciding whether a law is applicable extraterritorially, and whether jurisdiction should be taken. Obviously the judge should refuse to apply a law which lacks constitutional legitimacy. But fairness and justice require that the judge should also consider the legitimacy of that law from the *external* perspective of the cyberspace actor as well.

2. Legitimacy from an external perspective

One of the main defects of the constitutional approach to legitimacy in cyberspace is that it only addresses the legitimacy of the lawmaker's legal system and its lawmaking processes, and thus ignores questions about the legitimacy of individual legal norms. From a constitutional perspective, almost every claim to authority made by all the world's multiple legal systems, irrespective of the location of the claim's addressee, is a legitimate claim. Constitutional legitimacy therefore tells the cyberspace actor nothing about which authority claims ought to be accepted.

Nor does Hart's external perspective, which is that of the dispassionate observer who is attempting to understand how the community operates by observing the statements which members make about the rules they claim to be following, and confirming or refuting those observations by reference to what they actually do.[13] This is a purely sociological enquiry, and the observer has no particular

[9]Although Hart recognises that there is a potential problem about the scope of a state's lawmaking authority: 'We may be doubtful in certain circumstances whether one legal system or another applies to a particular person' – he assumes that these are 'questions of law which arise *within* some system of law (municipal or international) and are settled by reference to the rules or principles of that system' and can therefore be resolved by those internal rules and principles (ibid, p 216).

[10]Ibid, pp 82–91.

[11]N Luhmann (K Hawkins, ed) *Law as a Social System* (Oxford: Oxford University Press, 2004) p 407 ff.

[12]A Buchanan and RO Keohane 'The Legitimacy of Global Governance Institutions' (2006) 20 Ethics & International Affairs 405.

[13]'Such an observer is content merely to record the regularities of observable behaviour in which conformity with the rules partly consists and those further regularities, in the form of the hostile reaction, reproofs, or punishments, with which

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

interest in the content of the rules nor any reason to frame his or her behaviour in accordance with them. Unlike the internal perspective, which is an attempt to discover which rules ought to be followed, the external observer is only interested in describing how the community appears to be governed.

For our purposes, though, there is a second and more important external perspective which Hart does not mention: that of the person to whom the law's authority claim is addressed. Cyberspace actors are faced with repeated claims by law systems that the actor should comply with their rules. Usually the cyberspace actor is not a resident or citizen of the nation state in question. What does validity mean when examined from the perspective of these actors? This is certainly an external perspective, but far from a dispassionate one. If the law system's claim is valid then the cyberspace actor ought to frame its behaviour in accordance with the rule. If not, not.

Once we switch to *this* external perspective we are forced to recognise that legitimate authority cannot be assessed at the level of the law system, but needs to be determined afresh for each individual authority claim of national law. We also need to accept that in cyberspace legitimacy is not an absolute value. Instead, cyberspace users assign different values for legitimacy to the competing authority claims with which they are faced, and by accepting the authority of one of those claims (and thus denying the authority of the others) they enhance the value of its legitimacy in the eyes of other cyberspace users. Thus the value of a particular law's claim to legitimate authority can rise or fall in comparison to other claims.

Cotterell expresses the necessary approach succinctly:

> It might be tempting, then, to think of authority as something primarily *claimed* in support of power by its holders, and legitimacy as something primarily *conferred* on power by those subject to it or who observe it; that is to say, legitimacy indicates an acceptance of the claim of authority as successfully made.[14]

It seems clear that non-constitutional legitimacy is necessarily decided by those to whom a law is addressed. This is inherent in the concept itself, variously defined as 'the right to rule and the recognition by the ruled of that right'[15] and as the reasons behind 'voluntary subjection to a claim to authority'.[16]

The search for legally normative sources of legitimacy beyond constitutions has focused on what Paiment describes as the input, throughput and output aspects of lawmaking.[17] Input legitimacy concentrates on the participatory nature and inclusiveness of the norm-creation process. Throughput legitimacy examines the rule-making processes for procedural fairness and impartiality. Output legitimacy is based on the quality of the rules themselves, particularly in terms of achieving their desired outcomes.

If legitimacy is what tells a law's addressee in cyberspace that the law's authority claims ought at least to be considered, then it should be apparent that only output legitimacy is clearly visible to that addressee. Constitutional legitimacy might in theory be visible, or more likely assumed to exist if the lawmaker is part of a national legal system. However, few if any cyberspace users will have

deviations from the rules are met. After a time the external observer may … be able to predict with a fair measure of success, and to assess the chances that a deviation from the group's normal behaviour will meet with hostile reaction or punishment': Hart, above n 8, p 89.

[14]R Cotterell 'Legal authority in a transnational world/ Autotytet prawa w świecie transnarodym' The Leon Petrazycki Lecture, University of Warsaw, 22 May 2014 (Warsaw: University of Warsaw Faculty of Law and Administration, 2014) 43.

[15]J Jackson et al 'Why do people comply with the law? Legitimacy and the influence of legal institutions' (2012) 52 British Journal of Criminology 1051 at 1051.

[16]C Devaux 'The role of experts in the elaboration of the Cape Town Convention: between authority and legitimacy' (2103) 19 European Law Journal 843 at 845.

[17]P Paiement 'Paradox and legitimacy in transnational legal pluralism' (2013) 4 Transnational Legal Theory 197 at 213–215.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

the time or resources to investigate input or throughput legitimacy, so these are likely to have almost no influence on the user's attitude to a law's authority claim. Output legitimacy will surely have the greatest influence, and is therefore what should most strongly influence judges when making their decisions about applicable law and jurisdiction.

Judges ought also to be interested in output legitimacy because it affects the external perception of their own legal system, of which they are in part custodians. Because the value of a particular law's claim to legitimate authority can rise or fall in comparison to other claims, a perfect lawmaker would aim to increase the perceived legitimacy of its claim through the ways in which it makes that claim, and through the normative content of the law. But lawmakers are not all perfect, and some (doubtless unintentionally) make authority claims in a way which reduces the likelihood of their acceptance by cyberspace users. Cumulatively, this can reduce overall respect for that legal system. If a judge has the ability to interpret the law so as to mitigate these ill-effects, that is a strong argument for doing so.

There is a clear link between this external perspective on legitimacy and Fuller's minimum internal morality of law.[18] His parable of Rex the King describes eight ways in which Rex attempted, but in Fuller's view failed, to make law. Rex's pronouncements came in the form of individually-addressed directives rather than general rules, were kept secret, were retroactive, were impossible to understand, were contradictory, required the impossible, were changed with excessive frequency, and there was no congruence between official action, particularly enforcement action, and the declared rules.[19]

The paradox this created was that Rex's subjects were forced, because of their membership of Rex's law system, to attempt to treat these pronouncements as law even though, in Fuller's estimation, Rex had been completely ineffective in achieving any law:

> A mere respect for constituted authority must not be confused with fidelity to law. Rex's subjects … remained faithful to him as king throughout his long and inept reign. They were not faithful to his law, for he never made any.[20]

Fuller describes this failure in terms of the effectiveness of the law system in 'the enterprise of subjecting human conduct to the governance of rules'.[21] But he might equally have phrased his argument in terms of the legitimacy of the claims Rex makes for obedience. From Fuller's perspective as an observer it is clear that Rex's own subjects had no reason to accept claims that his 'law' should be obeyed, and an external actor in cyberspace would even more strongly deny that those claims made any legitimate assertion of authority.

3. Output legitimacy

Output legitimacy is about the quality of the normative content of a law. But because it is assessed from an external perspective, it would be more accurate to say that it is about the *perceived* quality of that content. Three factors are particularly likely to affect that perception:

(i) the extent to which the law is perceived as being addressed to the cyberspace user, rather than to some other person;
(ii) how far the law's provisions are congruent with the rest of the environment in which the cyberspace user acts; and
(iii) the perceived fairness and justice of the law's likely outcomes.

[18] L Fuller *The Morality of Law* (New Haven: Yale University Press, Revised edn, 1969). The application of Fuller's argument to cyberspace is explored more fully in C Reed 'How to make bad law: lessons from cyberspace' (2010) 73 MLR 903 at 914–919 and C Reed *Making Laws for Cyberspace* (Oxford University Press: Oxford, 2012) ch 10.

[19] Ibid, pp 33–38, under the heading 'Eight ways to fail to make law'.

[20] Ibid, p 41.

[21] Ibid, p 96.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

(a) Addressing and communication

Law is not a purely abstract phenomenon, but rather a practical attempt to 'control, order or influence the behaviour of others'.[22] To achieve this end, the law needs to communicate to those others how they *ought* to behave, or sometimes how they *must* behave. If no communication is achieved, there is no way in which the law can be successful in achieving its aims. The way in which the law is framed, and the language through which it attempts to assert its authority claims, are an important aspect of its output legitimacy. If it does not appear to be addressing the cyberspace user, or does so in a way which fails to convince the user that it deserves attention, it loses some or all of its legitimacy.

A common reason for communications failure is that the recipient is simply not listening. And a common reason for not listening is that we do not believe we are being spoken to:

> … law has the normative authority of obligation when – and only when – it specifies obligations of individuals that are extra-legally intelligible.[23]

A simple story, well-known to cyberspace lawyers, can illustrate how this kind of communications failure happens.

Towards the end of 1998 Mrs Lindqvist made a website for her local church in Alseda, Sweden. She included the names and contact details of some of her volunteer co-workers at the church, and used the website to organise the flower rota and to send best wishes to a volunteer who had broken her foot and was off work. No-one at the church seems to have objected, and the administrator of the Swedish Protestant Church's official website even set up a link to Mrs Lindqvist's site.

However, the Swedish public prosecutor *was* unhappy, and prosecuted Mrs Lindqvist for various breaches of the criminal provisions of the Personuppgiftslag.[24] She was found guilty of failing to notify her processing of personal data to the Datainspektionen (the Swedish data protection authority), processing sensitive data relating to health without authorisation from the authority, and exporting personal data outside the EEA. On appeal, the Swedish Göta hovrätt referred a number of questions to the European Court of Justice which decided that Mrs Lindqvist's website activities fell within the ambit of the Data Protection Directive and thus that she had been correctly convicted of the first two offences.[25]

This case has been discussed extensively in the academic literature, but always with a focus either on the interpretation of the Directive[26] or its conflict with the right to freedom of expression.[27] Commentators seem, though, to have ignored the most obvious question: why did Mrs Lindqvist break the law? She appears to have been a moral person, as a church worker and a respected member of the Alseda community. We expect a high degree of legal compliance from such persons, particularly in respect of the criminal law.

[22]J Black 'Critical reflections on regulation' (2002) 27 Austl J Leg Phil 1 at 25.

[23]J Garthoff 'Legitimacy is not authority' (2010) Law & Philosophy 669 at 681.

[24]SFS 1998:204, the Swedish data protection law which implemented the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31 (Data Protection Directive)).

[25]Case C-101/01 *Lindqvist* 6 November 2003. The ECJ also held that merely uploading personal data to a website without more did not amount to the export of that data outside the EEA, even though it was potentially accessible by persons outside the EEA, but this is not directly relevant to the discussion here and so is not considered further.

[26]In particular in relation to the meaning of 'personal and household activity' (D Erdos 'Data protection and the right to reputation: filling the "gaps" after the Defamation Act 2013' (2014) CLJ 536; DB Garrie and R Wong 'Social networking: opening the floodgates to "personal data"' (2010) CTLR 167); meanings of the terms 'personal data' and 'processing' (H Crowther 'Remember to forget me: the recent ruling in Google v AEPD and Costeja' (2014) CTLR 163 at 173; P Gryffroy 'Delisting as a part of the decay of information in the digital age: a critical evaluation of Google Spain (C-131/12) and the right to delist it has created' (2016) CTLR 149); meaning of the Directive's data export provisions (D Kamarinou 'International transfers of personal data and corporate compliance under Directive 95/46/EC, the draft Regulation and the international community: Part 1' (2013) Comms Law 49).

[27]D Erdos 'Data protection confronts freedom of expression on the "new media" internet: the stance of European regulatory authorities' (2015) EL Review 531; D Mac Sithigh '"I'd tell you everything if you'd pick up that telephone": political expression and data protection' (2011) EHRLR 166.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

It might be that Mrs Lindqvist was ignorant about the existence of data protection law,[28] or that she knew about the law but didn't understand it. Neither of these would suggest that the law was making illegitimate claims upon her. But there is another possibility, which is that Mrs Lindqvist knew about data protection law, in general terms, but thought that *it didn't apply to her actions*. What if the law appeared to her to be aimed at governments and large corporations, not at individuals who build church websites? Could a law lack legitimacy if the way it is framed leads some of its addressees to believe that it is intended to be complied with by the general population?

We cannot, of course, know what Mrs Lindqvist believed about the addressing of the law, but it is certain that the Data Protection Directive, which was implemented by the Personuppgiftslag, looks very different from those laws which are clearly addressed to the public at large. These tend to be expressed briefly and in simple language, as we can see from the anti-discrimination provisions of Norway's General Civil Penal Code,[29] Art 349:

> Any person who in any commercial or similar activity refuses any person goods or services on the same conditions as apply to others, because of his religion or life stance, skin colour or national or ethnic origin, shall be liable to fines or imprisonment for a term not exceeding six months. The same penalty shall apply to any person who in any such activity refuses any person such goods or services because of his homosexual inclination, lifestyle or orientation.
>
> The same penalty shall apply to any person who for any such reason as is mentioned in the first paragraph refuses a person admission to a public performance or exhibition or other public gathering on the same conditions as apply to others.
>
> The same penalty shall also apply to any person who incites or in any other way who aids and abets any act mentioned in the first or the second paragraph.

This is the whole of the law on this matter, and is clearly understandable by the average citizen. There is nothing in its wording to suggest that it is addressed only to a particular sector of society.

By contrast, laws which *are* addressed to specific sectors tend to adopt a very different style of lawmaking. The most extreme example is the regulation of banking and financial services. The UK Financial Conduct Authority (FCA) Handbook sets out detailed regulations made under UK financial services law, and is a hugely complex piece of legal documentation.[30] It is clear that any organisation which is subject to this scheme of regulation will need to employ a number of specialist compliance officers to gain a complete understanding of the entire regulatory regime and how it applies to all the regulated activities. Laws of this type change rapidly as well, with major amendments being made several times each year.

The reason why such a complex and constantly altering rule-set can be effective is that this style of lawmaking depends on the development of an interpretive community,[31] which consists of the regulator together with those specialists within each regulated entity who work on regulatory compliance. The community engages in regulatory conversations,[32] through which the regulatees and the regulator

[28]Though the Swedish Data Act (Datalagen, 1973:289), the predecessor legislation to the Personuppgiftslag, had been in force for 25 years and, at least in the UK, data protection issues were widely reported in the general press during that period (see eg 'First data protection conviction' (*The Times* 16 December 1987); 'Protecting the people – The Data Protection Act works in the public interest, says its registrar' (*The Guardian* 13 December 1990); 'Pressing questions over personal rights' (*The Times* 1 September 1994)).

[29]English translation from http://www.ub.uio.no/ujur/ulovdata/lov-19020522-010-eng.pdf. Unfortunately no translation of the Swedish Penal Code more recent than 1999 is available, so neighbouring Norway has been used as the comparator for addressing.

[30]To give some idea of the level of detailed lawmaking, in Release 6 of May 2016 the Glossary alone ran to 538 pages. The Conduct of Business Sourcebook section (a small part of the whole) was 522 pages long. The full Handbook amounts to many thousands of pages and is constantly growing in size. Each part of the Handbook contains cross-references to other parts, so that a full understanding of any part requires some mastery of the whole.

[31]J Black *Rules and Regulators* (Oxford: Clarendon Press, 1997) pp 30–37.

[32]J Black 'Talking about regulation' (1998) Public Law 77.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

continually renegotiate the content, application and interpretation of the rules. These conversations develop agreed meanings for those parts of the regulation which are discussed, and any remaining uncertainties can be dealt with through the regulator's discretion over enforcement.[33]

The lawmaking aim here is to produce rules which describe as precisely as possible the conduct required from regulatees. There should be little or no need for judgment or discretion on the part of the regulatee when assessing whether compliance has been achieved, and in the case of doubt advice on the application of the rules can be secured through a conversation with the regulator. Highly precise rules will inevitably require constant amendment, because the achievement of the regulatory objectives is a moving target which requires continual adjustment of the rules to take account of new behaviours and other relevant factors. But again, regulatees learn about these changes, usually in advance, through the process of regulatory conversations.

So, returning to data protection, to whom does the law appear to be addressed? Is it trying to communicate with the general populace, or only with a specialist interpretive community of data protection professionals?

Certainly data protection law is extremely complex. At the time of writing, to discover the law for a single EEA state one needs to examine the Directive itself (20 pages in the Official Journal) together with its national implementing laws (over 50 pages for the UK Data Protection Act 1998). It would clearly be sensible to read also the various recommendations and guidance issued by EU bodies, in particular the Article 29 Working Party which publishes around ten Opinions and Working Documents each year.[34] National data protection authorities also produce guidance documents and these too need to be read. In total, there are thousands of pages of documents which are required to explain the law and its meaning. The replacement law, the General Data Protection Regulation[35] which came into force in 2018, is a mere 88 pages long, but the existing guidance material will still be relevant in interpreting its meaning and doubtless further guidance will be issued in copious amounts. There is also evidence that an interpretive community of data protection officers has evolved.[36]

This looks much more like banking regulation than a law of general application. It seems to me that it would be entirely reasonable for a member of the general public to assume that such a complex law is not addressed to her. As a comparator, the *entire* Norwegian General Civil Penal Code is expressed in a mere 137 pages.

All these factors might suggest to an observer that data protection law is addressed to a limited group of regulatees, and is attempting to communicate primarily with a sub-group of specialist practitioners. Mrs Lindqvist was not a member of that group, and the church at Alseda would have no capacity to employ such a specialist. It would hardly be surprising if she considered that the Swedish data protection law was not addressed to her.

Indeed, the exception in Art 3(2) of the Directive for data processed 'by a natural person in the course of a purely personal or household activity' would be likely to confirm that belief. But it seems that neither counsel for Mrs Lindqvist nor the judges of the ECJ recognised this possibility, as the judgment concentrates exclusively on interpreting the meaning of these words as restrictively

[33]M Sparrow *The Regulatory Craft* (Washington: The Brookings Institution, 2000).

[34]Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[35]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1, 4 May 2016 (General Data Protection Regulation).

[36]The International Association of Privacy Professionals has more than 12,000 members in 78 countries (https://www.privacyassociation.org/about_iapp) and accreditation for data protection professionals has been introduced (eg the British Computer Society's Certificate in Data Protection, http://certifications.bcs.org/content/conCertification/8). Most, perhaps all, organisations of any size recognise the need to employ such professionals to assist them in complying with the law, and Art 37 of the Regulation will require all enterprises which engage in large-scale processing of personal data to appoint such a person.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

as possible, based on the examples ('correspondence and the holding of records of addresses') given in Recital 12.[37] The holding that posting private information online can never be a purely personal activity[38] is certainly at odds with the understanding of private individuals, even in 2003.

We saw earlier that the legitimacy of a law's claim to authority is conferred on it by the collective acceptance of those to whom it is addressed. It must surely follow that structuring or wording a law of general application in a way which leads its intended addressees to believe that it is not intended to apply to them will reduce the likelihood of such acceptance. Achieving legitimacy requires attention to style as well as to substance.

This issue of whether a law is properly addressed to the cyberspace actor, and thus makes legitimate claims to obedience, might explain the differences between the *Moberg*[39] and *Kernal Records*[40] decisions, in both of which the output legitimacy of the law appears to have played a part. In *Moberg* the Swedish plaintiff was an artistic photographer, who uploaded photographs of his work to a German website which took orders for high-quality physical prints, and the defendant in the US had taken those images and incorporated them into website design templates which were sold commercially. Because Moberg had not registered his images with the US Copyright Office, which was at that time a prerequisite to bringing a copyright infringement action in the US courts if the work was first published there, a finding of simultaneous world-wide publication would have deprived him of any remedy. A finding that first publication occurred in the US would thus result in an illegitimate authority claim by US law, and indeed the court recognised this expressly:

> the acceptance of defendants' position would overextend and pervert the United States copyright laws, and would be contrary to the Berne Convention.[41]

In *Kernal Records* there were three important differences from *Moberg*. First, the requirement of registration as a prerequisite for bringing suit had been abolished, so that the consequences of non-registration were limited to a loss of the statutory presumption of infringement and an inability to claim statutory damages and attorney's fees.[42] Thus the location of first publication was only relevant to US procedural law and not substantive copyright law. Secondly, the intention of the plaintiff was that the work, which was a sound file for a computer gaming platform, should be downloaded for immediate use and not, as in *Moberg*, merely viewed as a precursor to ordering physical prints. And perhaps most importantly, the court recognised that this was a commercial dispute between litigants who both worked in copyright industries, and found that the plaintiff had ignored procedural rules of which it should have been aware and failed to take opportunities to correct the defects in its claim.[43] These differences make it unsurprising that the court found against the plaintiff, because they raise no prospect of applying US law illegitimately to someone who would not perceive themself as being its addressee.

(b) Congruence with the law's environment

Laws aim to achieve changes in behaviour. Whether an addressee will accept those demands for change as legitimate depends very much on how radical the change is. Major modifications to behaviour need stronger justification than minor changes. And the plausibility and strength of those

[37] *Lindqvist*, above n 25, paras 46–47.
[38] Ibid, para 47.
[39] *Moberg v 33T LLC* 666 F Supp 2d 415 (D Del 2009).
[40] *Kernal Records Oy v Mosley* 694 F 3d 1294 (11th Cir 2012).
[41] *Moberg*, above n 39, at 420.
[42] 17 USC §410(c), at §412.
[43] 'We will not ascribe bad faith to Plaintiff for failing to seek registration earlier in the case. Plaintiff made a calculated decision not to do so even though the issue was contested. Plaintiff's decision to hedge its bet supports our conclusion that Plaintiff has not met the good cause standard … for a tardy amendment of the pleadings': *Kernal Records*, above n 40, at 1370.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

justifications depends very much on how the addressee is currently behaving, which is influenced very largely by the environment in which the addressee acts. Changing behaviour is costly, and a demand for change which is not justified in terms of the wider benefits which compliance will bring is likely to be perceived as lacking legitimacy to some degree. At the extreme it is, I would suggest, uncontroversial that a demand to perform the impossible is not a legitimate demand.

The environment of cyberspace users is constituted by the technologies in use, the current normative landscape, and the social and business practices adopted by cyberspace users. If the change demanded by the law fits easily into the current environment it is quite likely that the legitimacy of the demand will be accepted. If it would produce major disruption to the environment, it is more likely to be resisted and thus legitimacy denied.

I do not intend to spend much time discussing online technology itself, because lawmakers rarely have the practical ability to require technology producers or operators to modify their technology. Lessig has explained how technology can influence and constrain the behaviours of cyberspace users,[44] and the power that technology has to weaken the normative force of law should not be underestimated – for example, the prevalence of technology for quick and simple sharing of content has had a real and negative impact on the response of cyberspace users to the demands of copyright law.[45]

More important is avoiding unnecessary clashes between the law's demands and the established norms for using technology. As an example we might take the controls in data protection law on personal data export.[46] These prohibit the transfer of personal data to a non-EEA country unless a range of conditions are met, and are completely out of step with how computing technology is actually used. They mean, for example, that in many cases[47] a mobile phone ought not to be taken outside the EEA without deleting most of the records for those people whom the owner is likely to want to contact while abroad. These export controls should also require users not to post to Facebook unless they confine their postings to information about themselves and corporate entities, because any personal data they post about third parties will almost certainly migrate to Facebook's servers in the US.[48] As readers will be aware, this law has had almost no influence on the ways that Facebook users behave. A law which demands behaviour that reduces the usefulness of widely adopted technology is unlikely to achieve much acceptance from technology users.

An equally important part of any law's environment is the normative landscape in which the law's addressees undertake their lives. Laws which clash with social norms may well find that the social norm is more powerful than the legal one. A particularly glaring example is the extra restrictions which data protection law imposes on those who process 'sensitive' data.[49] We might all have legitimate concerns about the collection and processing of sensitive data by corporations and governments, but in one's personal life this kind of information is exchanged freely. Gossip and discussion about the sex lives or political views of acquaintances and celebrities is the mainstay of conversation. Indeed, telling one friend that another is ill is not only socially acceptable but often mandatory, and this might well have influenced Mrs Lindqvist's actions. There is little doubt that individual cyberspace users do not consider this law to have legitimate authority for them, and both the Directive and

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

[45]See C Reed *Making Laws for Cyberspace* (Oxford: Oxford University Press, 2012) ch 7, 'Community norms and copyright'.

[46]Data Protection Directive, above n 24, Art 25; General Data Protection Regulation, above n 35, Art 44.

[47]Data protection law does not apply to personal data processed 'in the course of a purely personal or household activity': Data Protection Directive, Art 3(2); General Data Protection Regulation, Art 2(2)(c), but most mobile phone users also store their professional contacts on the phone, thus losing the benefit of the exception.

[48]In *Lindqvist* the web page was hosted on a server in Sweden, and it seems likely that the court would have decided that an export occurred had the server been situated outside the EEA. Although Facebook adheres to the US Privacy Shield (see https://www.facebook.com/about/privacyshield) its Data Policy (see https://www.facebook.com/policy.php) is unclear about whether information uploaded by users falls within the scope of the Privacy Shield.

[49]Defined in Data Protection Directive, above n 24, Art 8 as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … data concerning health or sex life'. See now GDPR, above n 35, Art 9, replacing the concept of sensitive data with 'special categories of personal data'.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

the General Data Protection Regulation accept that sometimes it does not. The difficulty is that the private sphere has fuzzy edges. Academics will want to engage in online discussion with their students, but telling them about a classmate's political opinions is prohibited under General Data Protection Regulation, Art 9(1) unless an exception applies. The organisers of a concert which is cancelled through illness of the musicians will want to explain the situation to those who had bought tickets, which requires the disclosure of sensitive personal data. Although the law apparently says that behaving in accordance with long-accepted social norms is no longer allowed,[50] even the most cursory glance at Facebook, Twitter or the host of other social media services will reveal that what is followed is the social norm rather than the law. Of course the law can attempt to change social norms, but this requires a degree of gradualism and is rarely successful if the distance to be bridged is very great.[51]

Social norms make up just part of the normative landscape. Legal norms are equally important, and any law's claim to authority will be assessed in the light of the norms established by other laws (which in cyberspace includes the legal norms of *all* other jurisdictions).

The first challenge for lawmakers is the fact that a cyberspace actor is likely to be a member of multiple communities. These will include not only the actor's 'home' physical world community, but also purely cyberspace communities with their own internal norms. If the cyberspace actor already accepts the normative obligations which his own communities impose on him, he is unlikely to recognise the authority of new normative obligations which a different lawmaker attempts to impose unless those new obligations do not conflict to any great degree with existing norms. This is not to say that a lawmaker can only successfully make laws which copy existing norms in cyberspace. One of the functions of law is to establish or reinforce norms by giving them the greater authority which derives from their status as law. But a decision to make laws which conflict with other legal norms will inevitably face difficulties in persuading cyberspace actors to accept the authority of those laws.[52]

These kinds of lawmaking failure are difficult for judges to remedy. If a law is constitutionally legitimate and its wording leaves insufficient room for interpretation, a judge cannot refuse to apply it on the grounds that it conflicts with a norm which is external to the legal system. All that can be done is to point out the law's problems in the judgment.[53]

However, where a judge does have scope to decide whether, or how, the law should be applied, then the law's output legitimacy can be enhanced by doing so in a way which is congruent with the legal norms which apply to similar physical world activities. Those offline rules already possess strong normative force because they are the rules according to which cyberspace actors conduct their offline lives. If the cyberspace user's expectation is that the rule in cyberspace will be the same as it is offline, because the activity he is engaged in is perceived as being the same kind of activity transposed to a new space, then a claim to legal authority which makes similar demands is more likely to be perceived as being legitimate.

This approach accords with two lawmaking principles which are widely espoused: that laws should be technologically neutral[54] and that there should be equivalence between the offline and online rules.[55] Equivalence guides the law maker as to the principles of law which should apply to cyberspace

[50]'In the new data protection landscape, the state criminalises activities which are in other contexts perfectly lawful and community-oriented': P Leith 'The socio-legal context of privacy' (2006) Int JLC 105 at 128, 129.

[51]See D Kubler 'On the regulation of social norms' (2001) 17 JL Econ & Org 449 at 452–453; TR Tyler 'Compliance with intellectual property laws: a psychological perspective' (1997) 29 NYU J Int'l L & Pol 219 at 234.

[52]See C Reed 'How to make bad law: lessons from cyberspace', above n 18, at 915–916 for examples.

[53]See eg *Gutnick v Dow Jones* [2002] HCA 56.

[54]First enunciated in the Bonn Ministerial Conference Declaration of 6–8 July 1997, which declared in its principle 22:

Ministers stress that the general legal frameworks should be applied on-line as they are off-line. In view of the speed at which new technologies are developing, they will strive to frame regulations which are technology-neutral, whilst bearing in mind the need to avoid unnecessary regulation: http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html.

[55]See eg Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, *Principles and guidelines for the Community's audiovisual policy in the digital age* COM (1999) 0657 final, note 17: 'identical services should in principle be regulated in the same way, regardless of their means of transmission'.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

activities and thus shapes the substantive rules of any law. Technology neutrality addresses the choice between the available substantive rules which could be used to implement those legal principles, and aims at futureproofing the law by ensuring that developments in technology do not make its rules outdated. It is equivalence which attempts to harness the existing normative force of offline laws as a means to persuade cyberspace actors to accept the authority of their online version.[56] It also helps to counter the natural human tendency to treat cyberspace as somewhere 'other', where different, and usually lower, standards of behaviour are permissible.[57]

The early history of defamation law in cyberspace is a good illustration of a missed opportunity to aim at equivalence. Those early cases[58] focused almost exclusively on the mechanical application of the established offline rule that a publisher is liable to the person defamed, as well as the author being liable, without considering whether the consequences of doing so would produce equivalent effects.[59] The result was to produce a defamation regime which had quite different consequences online, so that the host of an internet resource, such as a website or newsgroup, was liable for defamatory content of which the host had no knowledge and which it could not discover without taking unusual precautions.[60] A further consequence was to extend the jurisdictional reach of national defamation law to the whole world, because content hosted on a server located in one country is still accessible, and thus published under that conception, everywhere else as well.[61]

The threat that the development of the internet would be stifled by litigation was clear, and so the US rushed the Communications Decency Act 1996[62] into law, aiming to confer immunity from liability on those internet intermediaries who took steps to deal with undesirable communications. However, the requirement to take action against indecent content as well as unlawful content was struck down in *ACLU v Reno*[63] as infringing the First Amendment protection for freedom of speech, leaving the immunity provisions of section 230(c) to stand alone. This now produced the effect that online intermediaries were immune from liability even if they had actual knowledge of unlawful content and failed to take any action in respect of it,[64] a result equally lacking in equivalence to the offline rule but in the other direction.

(c) Fair and just outcomes

The third important aspect of output legitimacy is based on the perceived effects of complying with a law. If the outcomes which the lawmaker is seeking are thought to be fair and just, and the law seems likely to achieve those outcomes, then the law is more likely to be accepted as making legitimate claims.

[56]See further Reed, above n 45, ch 7, 'Transposing offline legal norms to cyberspace'.

[57]A well-documented example is the degree of aggression and casual abuse that many users of online discussion sites engage in, which they would not show in face-to-face conversations. See A Sengupta and A Chaudhuri 'Are social networking sites a source of online harassment for teens? Evidence from survey data', NET Institute Working Paper #08-17 (September 2008, http://www.NETinst.org); T Byron *SaferChildren in a Digital World: Report of the Byron Review* (2008) para 3.63 (http://www.dcsf.gov.uk/byronreview/).

[58]For a useful review of the early history see L Edwards 'Defamation and the internet' in L Edwards and C Waelde (eds) *Law and the Internet: A Framework for Electronic Commerce* (Oxford: Hart, 2000).

[59]It is worth noting that these judges had alternative conceptions available within the existing offline rules, such as conceptualising ISPs and content hosts as mere distributors whose liability would depend on knowledge of the content.

[60]For an example from the UK, see *Godfrey v Demon Internet Ltd* [1999] 4 All ER 342, though in that case the claim was carefully drafted to apply only to publication which occurred subsequent to the defendant receiving notice of the presence of the defamatory material in a newsgroup which it hosted.

[61]See eg the judgment of Kirby J in *Gutnick v Dow Jones* [2002] HCA 56, at paras 164–166.

[62]47 USC § 230.

[63]929 F Supp 824 at 830–838 (ED Pa, 1996), affirmed 117 S Ct 2329 (1997).

[64]See eg *Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997). Those few cases where an intermediary was held liable had unusual facts – see eg *Barnes v Yahoo!*, 570 F3d 1096 (9th Cir 2009) where liability arose from breach of an oral contract to remove offending material.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

But good aspirations alone are insufficient. From an external perspective, laws need to be perceived by their addressees as striking a fair and just balance between the interests of all those affected by them. It is by no means uncommon for a law to focus almost exclusively on the interests of one particular group, with the consequence that those outside the group question its fairness and justice.

Copyright law is a well-known example. Tyler, writing about social attitudes to copyright pre-cyberspace, notes that:

> one crucial problem is the lack of a public feeling that breaking intellectual property laws is wrong. In the absence of such a conception, there is little reason for people to follow intellectual property laws.[65]

Part of the reason for this is that intellectual property laws do not match the public's conception of fairness, for example that they should have to pay for something only once.[66] But the main reason seems to be that intellectual property laws are viewed as lacking legitimate authority to direct the lives of ordinary citizens:

> People need to believe that the rules established serve reasonable social purposes and are not simply efforts to create profits for special interest groups, such as large corporations. Again, the key to developing an effective strategy in this area is to understand better how the public currently views copyright laws. Are such laws regarded as illegitimate efforts by corporations to enrich themselves at public expense?[67]

Jensen takes this last point and analyses it at length in relation to cyberspace actors.[68] He points out that the law of copyright was developed in order to regulate relations between those involved in the exploitation of creative works, only to a limited extent to regulate relationships with creators, and hardly at all in relation to the use of works by the general public. Because the law was not developed for 'ordinary' people, they do not perceive it as imposing meaningful obligations on them:

> Voluntary compliance with intellectual property laws in general and copyright laws in particular suffer from a perceived lack of procedural fairness and public mistrust. The process of drafting copyright legislation often amounts to little more than negotiations among narrow interest groups; without a seat at the bargaining table, the public has no meaningful opportunity to participate in the legislative process. This process fosters the (often accurate) perception that copyright law is designed by and for the benefit of a small circle of vested interests. This widespread sense of unfairness – that copyright protections exist for the benefit of Microsoft and Disney – undermines voluntary compliance with copyright law.[69]

This sense that copyright has little meaning for the ordinary citizen has been compounded by the way in which the operation of the law remained hidden from them, before the digital technologies and cyberspace expanded the scope of copyright to cover the everyday activities of members of the public:

> … groups such as authors and publishers formed relatively small communities of repeat players. As such, they knew the rules of the game and knew that, as repeat players, following the rules in one transaction would affect their success in future interactions with other players. In this context, constructing a widely embraced normative justification for copyright law was unnecessary to

[65]Tyler, above n 51, at 226.
[66]Ibid, at 228.
[67]Ibid, at 233.
[68]C Jensen 'The more things change, the more they stay the same: copyright, digital technology, and social norms' (2003) 56 Stan L Rev 531.
[69]Ibid, at 540.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

> ensure that the commercially significant players obeyed the law. Under any circumstances, the game went on outside the view of the ordinary consumer of copyrighted works, who remained unsocialized in any 'copyright culture' that developed among those involved in the business of making and selling copyrighted works.[70]

Cyberspace has brought consumers within the game, and has also given them the tools to become producers and reusers of content which inevitably leads to conflict with the established players. The main arena in which this new aspect of the game is played out is that of content hosting platforms such as YouTube, most of which are operated by US entities.

Under the US Digital Millennium Copyright Act[71] (DMCA) these platforms are given immunity from liability for the content they host. However, if a copyright owner gives notice to a host that particular content is infringing, the host has to take down that content unless the person posting disputes the infringement claim, or lose the immunity and risk liability. Such a notice has to assert a good faith belief that the identified content infringes.[72] Because of the sheer volume of content posted to such platforms,[73] the search for potentially infringing content is carried out by automated software tools rather than human viewing.

Inevitably, rights owners also automated the process of issuing notices to hosts, with the result that many uploaders received notices in respect of content which they believed to be lawful. In *Lenz v Universal Music*[74] the video in question showed the uploader's young son dancing to a tune on the radio, which was playing a song by Prince. She believed that this amounted to fair use[75] of the music and thus did not infringe Universal's rights, and so brought an action for damages under 17 USC §512(f), which imposes liability on the rights owner if the notice 'knowingly materially misrepresents … that material or activity is infringing …'. On the evidence before the court Universal had not actively considered the fair use question, and the court held that without such consideration it could not have formed a good faith belief that the video infringed, and thus made a material misrepresentation in its notice.[76] This finding raises the difficult question whether it is possible to automate such consideration, or whether review by a human for possible fair use is a prerequisite to issuing a DMCA notice.

In the cases on DMCA notices it is possible to detect a difference of approach to this question, depending on whether the issue is raised by an individual uploader or by a host. Hosts are of course commercially significant participants in the copyright system and their motivation is to protect their platform's commercial interests, rather than the individual rights of their users. Thus where hosts raise the issue, the courts have held that a notice system which produces a tiny proportion of notices relating to non-infringing material does not amount to bad faith[77] unless there is additional evidence which suggests that the rights owner is not carrying out a proper review.[78] By contrast, when *Lenz* was appealed to the 9th Circuit Court of Appeals the court reasserted the requirement for the content in question to be individually reviewed for fair use but left open the possibility that such a review

[70] Ibid, at 543.

[71] 17 USC §512.

[72] A DMCA notice is required to assert 'that the complaining party has a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law': 17 USC §512(c)(3).

[73] Each minute, 400 hours of video are uploaded to YouTube – https://www.blog.google/topics/google-europe/improving-our-brand-safety-controls/.

[74] 572 F Supp 2d 1150 (ND Cal 2008).

[75] 17 USC §107.

[76] 572 F Supp 2d 1150 at 1154–1155.

[77] *Capitol Records v MP3Tunes* 611 F Supp 2d 342 at 345 (SDNY 2009).

[78] *Disney Enterprises v Hotfile* 2013 WL 6336286 (SD Fla 2013).

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

might be undertaken through automated means,[79] and in *Online Policy Group v Diebold*[80] bad faith was found on the basis of evidence that the rights owner's motivation was to secure suppression of publicity rather than to protect its copyright.

Although the wording of the DMCA inevitably focuses judicial attention on the acts and motives of the rights owner, the discussion in these cases clearly demonstrates that the courts are also considering the competing rights of the defendant. Individual uploaders are outsiders to the copyright system, as explained above, and so the output legitimacy of the DMCA (in terms of the fairness and justice of receiving an incorrect notice) is a matter to which I would argue the courts need to pay attention in their role as upholders of the rule of law.

This will become increasingly important because the notice and takedown system has evolved. Rights owners now partner with the major platforms, such as YouTube and Facebook, working with them to identify possibly infringing content. Notices are now issued by hosts, rather than rights owners, treating this as purely a matter of contract with the result that the DMCA no longer applies and so uploaders are not entitled to invoke the DMCA procedures to preserve the availability of their uploads.[81] Uploaders now receive far less information about the alleged infringement[82] which makes it less likely that they will dispute the notice. The courts may need to decide how far these new systems are a legitimate way to protect the rights of copyright owners, as at least one action has been commenced asking for declarations that the YouTube Content ID system should comply with the DMCA and that the YouTube terms are unlawful.[83] In doing so, the fairness and justice of the outcomes produced by their interpretation of the law should play an important part, even if this is not expressed in terms of output legitimacy.

Conclusions

The aim of this paper has been to demonstrate that any judicial decision to take jurisdiction over a case involving cyberspace, or to apply national law when deciding that case, also makes an assertion about the legitimate authority of the law. But because legitimacy in cyberspace is primarily determined not by the constitutional basis of the law, but by its output legitimacy as assessed by those cyberspace users to whom the authority claim is addressed, an inappropriate assertion of authority can damage that legitimacy. If judges are concerned to maintain the legitimacy of their legal systems in the eyes of the world, they need to take these jurisprudential considerations into account when making their decisions.

This does not mean that judges should start to declare particular national laws to be illegitimate, except on constitutional grounds. The external perspective does not ask whether the law itself is legitimate, but rather whether it makes a legitimate claim to apply to *this* cyberspace actor in *these* circumstances. But attempting to answer this latter question can help lead the judge to the best answer in cases of conflict about jurisdiction or applicability, or in interpreting how the law should be applied, so long as the judge has some margin of choice in making that determination.

Of course, judges are limited in what they can do here. A judge working within a legal system and reviewing a law which is constitutionally legitimate in that system has no grounds under national law

[79]'We note, without passing judgment, that the implementation of computer algorithms appears to be a valid and good faith middle ground for processing a plethora of content while still meeting the DMCA's requirements to somehow consider fair use': 801 F 3d 1126 at 1135 (9th Cir 2015).

[80]337 F Supp 2d 1195 at 1203 ff (ND Cal 2004).

[81]TB Bartholomew 'The death of fair use in cyberspace: YouTube and the problem with content ID' (2015) 13 Duke L & Tech Rev 66; M Perel and N Elkin-Koren 'Accountability in algorithmic copyright enforcement' (2015) 19 Stan Tech L Rev 473.

[82]Thus in 2014 a stop-motion video by a child using Lego figures received a Facebook notice which gave no details at all about the rights which were allegedly infringed – https://ip-appeals.com/take-down-abuse-from-harry-potter-to-legos/.

[83]*Ligeri v Google*, Complaint CA15-188M (District of Rhode Island 2015) – http://digitalcommons.law.scu.edu/historical/959/.

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press

to declare that the law should not be applied solely because its authority claim lacks legitimacy in the eyes of those to whom it is addressed. But if the judge has choices available about whether the law applies at all, or how it should be applied in cyberspace, choosing the option which enhances the law's output legitimacy is not only permissible but, in my view, highly desirable.

Murray has argued convincingly[84] that the legitimacy of authority claims by lawmakers and regulators is the biggest challenge posed by cyberspace. This is because maintenance of the rule of law requires law and regulation which is actually obeyed, and obedience is founded in legitimate authority. Mere technocratic or utilitarian approaches cannot achieve this end, because it demands a fundamental reassessment of the jurisprudence of cyberspace.[85]

And if lawmakers and regulators need to understand the scope of legitimacy in cyberspace, so too do judges. Law and regulation have no practical meaning until they are applied to a specific case, and all the efforts of lawmakers will be vain unless the judges also strive to maintain the rule of law. Judicial decisions which assert or reinforce illegitimate demands for legal obedience are unlikely to assist in doing so. To avoid this, judges will need to dust off the jurisprudence they learnt at Law School and perhaps bring it up to date if they wish to deliver appropriate judgments in cyberspace matters.

[84]A Murray 'Looking back at the law of the horse: why cyberlaw and the rule of law are important' (2013) 10 SCRIPTed 310. I am delighted to acknowledge this article as the inspiration for the line of inquiry set out in this piece.

[85]Ibid, at 317–319.

Cite this article: Reed C (2018). Why judges need jurisprudence in cyberspace. *Legal Studies* **38**, 263–278. https://doi.org/10.1017/lst.2017.15

https://doi.org/10.1017/lst.2017.15 Published online by Cambridge University Press