TCLR (2022), Issue 2
DOI: 10.26494/tclr220229

**ARTICLE**

# Cyberspace Institutions, Community and Legitimate Authority

Chris Reed*

## 1. Introduction

To its users, cyberspace appears to be almost completely harmonised. Online services such as Facebook, Google and eBay have a near identical appearance no matter where in the world the user is located, and seem to work identically too. Geography and nationality are apparently irrelevant.

Under the surface, though, there is a mass of diverging law and regulation which these services need to cope with in order to achieve their apparent universality. Some of these legal and regulatory differences reflect fundamental societal choices which cannot easily be harmonised, if at all.[1] But many of the differences are just contingent accidents of history. Ideally, they would be harmonised if that were possible.

Harmonisation[2] usually requires positive collective action to achieve. Admittedly, the arrival of cyberspace has sometimes led to the convergence of national law and regulation without such collective action. Probably the best-known example is the law on electronic signatures which, following an initial burst of legislative activity, rapidly coalesced around a two-tier model of electronic signatures which has become almost universal. But this convergence was only possible because electronic signatures were a

* Chris Reed is Professor of Electronic Commerce Law at the Centre for Commercial Law Studies, School of Law, Queen Mary University of London. This article is a modified version of 'Cyberspace Institutions, Community and Legitimate Authority', previously published as Ch 6 in Orkun Akseli and John Linarelli (eds) *The Future of Commercial Law* (Oxford: Hart Publishing 2020). It is reproduced here by kind permission of Hart Publishing.

[1] Perhaps the clearest example is the wide divergence of national attitudes to freedom of speech, illustrated in the series of cases involving Yahoo! and France's anti-Nazi laws—see *Yahoo! Inc v LICRA* TGI de Paris, 22 May 2000, 20 November 2000; *Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme*, 169 F Supp 2d 1181 (ND Cal, 2001), 379 F 3d 1120 (9th Cir 2004).

[2] Used here to cover both harmonisation and approximation of laws.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

previously unknown phenomenon, and thus no legal system already had an entrenched view about what should be the proper law and system of regulation. This allowed lawmakers to abandon false starts and copy better solutions from elsewhere once these became known. But even here, the coordination work undertaken by UNCITRAL in producing model laws was highly influential, and the convergence might not have happened without it.

Further useful harmonisation of laws affecting cyberspace will usually require the adaptation of existing systems of law and regulation, rather than devising completely new laws. Most of the easy wins have now been achieved. So, if further harmonisation is to take place, positive collective action will be necessary. The question this paper examines is a simple one: are the world's existing transnational institutions capable of undertaking this work and, if not, what kinds of institution will we need for the purpose?

To answer this question, I begin by examining where current transnational institutions derive their authority. Almost all rely on charismatic authority, using this to persuade states and enterprises to adopt their proposals. But to expand beyond mere persuasion, institutions need a stronger form of authority, and those institutions like the World Intellectual Property Organisation (WIPO) which derive their authority from state delegation seem to have little authority in practice over cyberspace users. This means we must find new sources of authority in cyberspace, and I propose that these come from acceptance by the regulated community. Because there is no *ex ante* obligation for a cyberspace user to accept any such authority claim, much depends on the claim's perceived legitimacy. That perception is driven in part by the institution's constitutional legitimacy, but perhaps more by the apparent workableness, fairness and justice of the claim for those to whom it is addressed. I then review how existing cyberspace institutions, ICANN, eBay's consumer dispute resolution system, and Google's right to be forgotten system all achieve a high level of legitimate authority without any reliance on the authority of states. From this, I identify when, and how, new transnational institutions in cyberspace might be expected to emerge and achieve a higher level of legitimate authority than state laws.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

## 2. The authority of current institutions

### *2.1. Sources of Authority*

Authority is a claim that some person should obey a rule, or at least conform his or her behaviour to the precepts of the person making the claim. The main difficulty facing our existing transnational institutions when trying to achieve harmonisation is that their authority claims are generally very weak.

Authority is traditionally conceptualised in terms of the nation state. The state has constitutional authority to make obedience claims because its constitution derives from the consent, or at least acquiescence, of its citizens. Additionally, the state has effective authority[3] because it has enforcement powers against those resident in its territory. Each state claims unlimited authority to regulate those activities which fall within the scope of its constitutional authority.[4]

Few transnational institutions have authority of this kind.[5] The EU might be seen as one, but its constitutional authority is limited to a geographical region, rather than claiming global law-making authority.[6] A global example might be the World Trade Organisation (WTO) which derives constitutional authority from the WTO Treaty, and also has some enforcement powers through the WTO tribunal.[7] WIPO might also be seen as having constitutional authority, through the WIPO Treaty, though it has no direct enforcement powers against a state which refuses to modify its intellectual property laws in accordance with the Treaty. In both cases, the authority only requires compliance by states, and not by individuals.

---

[3] J Raz, *The Authority of Law* (2nd edn, OUP 2009) 5.
[4] ibid 119, and see text to (n 29).
[5] Note, though, Linarelli's argument that the collective body of transnational law for each area of commercial activity has sufficient authority to amount to an independent legal system. See John Linarelli, 'Analytical Jurisprudence and the Concept of Commercial Law' (2009) 114 *Penn State Law Review* 119.
[6] In the field of data protection the EU asserts global authority over personal data processing involving EU citizens or residents—see eg Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the EU judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 (14/EN WP 225, 26 November 2014)—but it does not claim authority to regulate processing where there is no connection to its constitutionally established geographical region.
[7] JP Trachtman, 'The Domain of WTO Dispute Resolution' (1999) 40 *Harvard International Law Journal* 333, 338–39.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

It is, perhaps, worthy of note that although WIPO has achieved formal harmonisation of copyright law as it applies to cyberspace, by introducing a right of communication to the public,[8] this harmonisation has not been successful in persuading the majority of cyberspace users to comply with the law. One might suspect that the combined constitutional authority of WIPO and the states whose law follows the Treaty is inadequate for this purpose, and I will return later to the reasons why this might be so.

Other international institutions, such as UNCITRAL, OECD or ICC, do not even have constitutions which impose compliance obligations on those to whom their authority claims are addressed. These institutions have a different kind of authority, known as charismatic authority. Charismatic authority derives from the acceptance of a person or group as leader, which thus legitimates the authority claim to obedience through the affectual or emotional effects which arise from such acceptance.[9] Unless this authority is institutionalised[10] through law-making and enforcement mechanisms, by means of a constitution of some kind, such institutions can therefore only attempt to persuade others, in our instance most commonly states, to adopt the harmonisation models they propose. How persuasive they are depends on both the respect in which those who crafted the proposal are held, and also on the quality and workability of the proposal as a mechanism for achieving harmonisation.

This is a very different kind of authority from the effective authority of states over their residents, based on their enforcement power, as understood by positivist scholars.[11] States *assert* their authority, but transnational institutions can merely *claim* authority. Whether such a claim is in fact authoritative depends on its acceptance by a sufficiently large number of those to whom the claim is addressed. Cotterell suggests that:

> ‘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;

[8] WIPO Copyright Treaty, Art 8.
[9] Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (University of California Press 1968) 1139.
[10] See ME Spencer, ‘Weber on Legitimate Norms and Authority’ (1970) 21 *British Journal of Sociology* 123, 124–25.
[11] As described by Raz (n 3).

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

> that is to say, legitimacy indicates an acceptance of the claim of authority as successfully made.'[12]

We might go further and suggest that legitimacy derives from the quality of the justification made for an authority claim—the stronger that justification, the more likely that the claim will be accepted by those to whom it is addressed.[13]

### *2.2. Success or failure?*

Where transnational institutions have used their charismatic authority to persuade states to remove barriers to online activity, they have in general been successful. The best-known example is probably the work of UNCITRAL. The majority of states worldwide have taken inspiration from the Model Law on Electronic Commerce, and have modified (when necessary) their contract law to enable online transactions to take place. The Model Law on Electronic Signatures sets out the fundamental principles which should be applied to decide whether a particular form of online authentication should be treated as a valid electronic signature, and these are reflected in instruments such as the US E-Sign Act 2000[14] and the EU eIDAS Regulation.[15]

However, these institutions have not been well-equipped to deal with those areas of online activity which have allowed cyberspace users to engage in socially undesirable behaviours. Charismatic authority seems to be sufficient to persuade states to harmonise by removing legal barriers to desirable activities. But because constraining undesirable activities requires enforcement action against those who do not comply voluntarily, transnational institutions have largely left harmonisation efforts as matters for the state level. And state attempts to regulate (for example) the unauthorised online dissemination

---

[12] Roger Cotterell, 'Legal Authority in a Transnational World/ Autotytet prawa w świecie transnarodym', The Leon Petrazycki Lecture, University of Warsaw, 22 May 2014 (University of Warsaw Faculty of Law and Administration 2014) 43.
[13] See Chris Reed and Andrew Murray, *Rethinking the Jurisprudence of Cyerspace* (Cheltenham: Edward Elgar 2018) ch 7. This idea is explored further in section 3.1 below.
[14] 15 USC §96.
[15] Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257 28 August 2014, 73–114.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

of copyright works, or infringements of digital privacy, or online defamation, have almost uniformly been unsuccessful in achieving their aims.[16]

An important reason for these failures is that there is a deficit in the legitimacy of authority. There is no global transnational institution which focuses primarily on online defamation or data privacy[17] and might therefore claim charismatic authority to shape regulation in either field. Even if there were such an institution its authority claims would normally be addressed to states, not individuals.[18] States have a legitimate authority claim to regulate the activity of those who are physically present in their territory, but because cyberspace transcends national territories then in practice those claims are also addressed to cyberspace users who are located elsewhere. To these users the legitimate authority of state claims is at best doubtful.[19]

The difficulties which copyright law has faced in regulating cyberspace activities illustrate clearly why there is a legitimacy deficit. Copyright laws are shaped through the WIPO Treaty, and WIPO has constitutional authority by virtue of that Treaty. WIPO's authority claims are addressed to states, who implement treaty changes in their national law, and these states have constitutional authority and also effective authority because of their enforcement powers. How can a deficit of legitimate authority have arisen?

The fact that there is such a deficit is without doubt, simply because of the widespread unauthorised use of copyright works which occurs throughout cyberspace.[20] It is now an established norm among cyberspace users that sharing content, at least if the sharing is not for profit, is generally acceptable. Clearly, the vast mass of cyberspace users does not accept the legitimacy of the WIPO copyright treaty, or even its implementations in national law.

---

[16] See eg M.I. Franklin Franklin, 'Digital Dilemmas: Transnational Politics in the Twenty-First Century' (2010) 16 *Brown Journal of World Affairs* 67, 69; T Hartley, '"Libel Tourism" and Conflict of Laws' (2010) 59 *International & Comparative Law Quarterly* 25. Copyright is explored further below.

[17] It is, though, arguable that the EU's European Data Protection Supervisor (formerly the Article 29 Working Party) has achieved a high degree of charismatic authority in the field of data protection, such that its recommendations often (though not always) set the shape of law and regulation in other countries. I am grateful to my colleague Professor Christopher Millard for this insight.

[18] And further, because regulation would be seeking compliance from individuals, the institution's lack of enforcement powers would weaken the effective authority of such claims.

[19] For detailed analysis of why this might be so, see Reed and Murray (n 13).

[20] See Chris Reed, *Making Laws for Cyberspace* (OUP 2012) ch 1.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

If a law has a legitimate claim to authority, it is likely to be obeyed because of the social norm that we should all act lawfully.[21] But the empirical work of Tyler has shown that copyright law lies outside this social norm:

> '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'.[22]

This is partly because some aspects of copyright in the digital world are perceived as unfair; for example, there is a strong belief that content should have to be paid for only once.[23] Mainly, though, even ordinary citizens (and cyberspace users even more so) do not accept that intellectual property laws have legitimate authority to direct their lives.

Jensen has demonstrated[24] that the law of copyright was developed mainly in order to regulate relations between those involved in the exploitation of creative works, to a lesser 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—

[21] HLA Hart in *The Concept of Law*, (2nd edn, OUP 1994) accepts as foundational that obedience to the law is dependent on general acceptance of the social norm that it should be obeyed (112–18), although his primary distinction is between norms which are obeyed only because of social pressure, and law, whose norms obeyed because they emanate from official lawmaking sources.
[22] TR Tyler, 'Compliance with Intellectual Property Laws: A Psychological Perspective' (1997) 29 *New York University Journal of International Law and Politics* 219, 226.
[23] ibid 228.
[24] Christopher Jensen, 'The More Things Change, the More They Stay the Same: copyright, digital technology, and social norms' (2003) 56 *Stanford Law Review* 531.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

that copyright protections exist for the benefit of Microsoft and Disney—undermines voluntary compliance with copyright law.[25]

If copyright is not addressed to the ordinary citizen, it is hardly surprising that the citizen does not consider that it makes any legitimate claims on him or her.[26]

If we are looking for further harmonisation in cyberspace, it seems clear that it is unlikely to come from our existing transnational institutions. New institutions will be needed, and they will need to possess a high level of legitimate authority, such that their laws and regulations are likely to be obeyed voluntarily by cyberspace users. Reliance on state law enforcement mechanisms is largely ineffective, as the case of copyright law shows. All cyberspace users are foreign residents, except for their home state, and their only connection with the national territory of any other state which claims authority over them is merely a consequence of the user's activities in cyberspace. They will be reluctant to accept the authority claims of a foreign state, because there is no relationship of state and citizen or resident, and the foreign state is likely to have limited enforcement powers over the user and thus little effective practical authority. Even worse, when multiple states claim authority over the same activity, cyberspace users will inevitably ask which, if any, of those laws ought to be obeyed; or, to put it in jurisprudential terms, whether those law-makers have any authority at all to claim obedience to their laws.

We therefore need to understand where legitimate authority comes from in cyberspace, so that we can understand how a transnational institution could achieve voluntary compliance, and this may tell us what kinds of institutions we need to develop.

---

[25] ibid 540. The story of the negotiation of the US Digital Millennium Copyright Act 1998, 17 USC §512(g), illustrates clearly how little part the interests of content users played in its enactment – see J Litman, *Digital Copyright* (Prometheus Books 2001).

[26] See Jensen (n 24) 543: '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 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.'

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

## 3. Legitimate Authority in Cyberspace

### *3.1. The distinction between legitimacy and authority*

It is important to begin by recognising that although legitimacy and authority are closely connected, they are nonetheless conceptually separate. Cotterrell recognises this separation when, as we saw earlier, he proposes that authority is a claim by power, whilst legitimacy is the acceptance of that claim.[27] This might be an accurate description of the relationship in the physical world,[28] but I would suggest that in cyberspace things work differently. This is because authority and legitimacy in the physical world can be, and usually are, assessed at the systemic level. The question is whether this particular institution or legal system's overall claim to authority should be accepted, on the basis that membership of the system requires either that all the rules of the system should be obeyed, or that none need to be. Raz describes this as 'comprehensive' authority and argues that legal systems: 'claim authority to regulate any type of behaviour … They do not acknowledge any limitation of the spheres of behaviour which they claim authority to regulate'.[29] In Raz's terms authority is an all-or-nothing proposition—either *all* the system's laws have authority, or *none* of them do.

But this can only hold true for members of the rule system.[30] No state claims comprehensive authority over the residents of other states. So far as outsiders are concerned, authority claims are only made in respect of specific rules, and only when the outsider's activity brings him or her within the ambit of the rule, for example when the activity has effects within the territory of a nation state. The majority of cyberspace users are outsiders[31] to any particular rule system, and not members of the community which, in positivist jurisprudence, is obliged to accept the authority of the rules.

---

[27] See text to (n 18).
[28] Though I have doubts whether legitimacy is demonstrated simply by the fact of acceptance of authority. Hart's gunman (see Hart (n 21) 19–23) is obeyed, but only through fear and not because there is any normative obligation to do so. His claim to obedience is surely illegitimate, and if the fear is removed by the gunman being disarmed there is no reason why anyone should even considering following his orders.
[29] Raz (n 3) 116–17.
[30] I adopt this term to avoid needing to discuss how far 'law' is limited to rules issued by a nation state, and where the boundaries lie between law and regulation, and between 'hard' and 'soft' law.
[31] Or at the least, are likely to consider themselves to be outsiders. As we are focusing on voluntary compliance, recognising that rule enforcement in cyberspace is inevitably problematic, it is the internal

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

This tells us that the source of authority in cyberspace is different from that of states. Not only are all authority claims merely claims, which there is no *ex ante* obligation for a cyberspace user to accept, but additionally we need to consider the question of authority at the level of each individual authority claim, rather than assessing the authority of the rule system as a whole. It also means that we have to determine the answer afresh for each cyberspace user, because an authority claim is only made if the user's activities fall within the ambit of the rule and also because merely falling within that ambit does not itself legitimate the authority claim.

An assessment of legitimate authority is thus a three-stage process. First, we must examine the authority claim to see if it is made against the particular cyberspace user. This requires us to evaluate the meaning of the rule and, also, if the claim is made by a national legal system, to decide if that system's rules of public and private international law make the rule applicable to that user.

Second, we must decide if the claim is legitimate.[32] Addressees of an authority claim are, of course, entitled to ignore an illegitimate claim. But if the claim is legitimate, this does not itself determine whether the claim has authority. Cyberspace users are faced with a multitude of legitimate authority claims, and because they cannot comply with them all they are forced to choose between them. Authority claims which are routinely ignored cannot, with any accuracy, be said to have any actual authority. Thus, legitimacy determines whether the user is under a normative obligation to consider the authority claim; it is what gets the claim a hearing.

---

understanding of actors which is the most important factor, rather than whether the rules of public and private international law hold them to be subject to the rule system.

[32] In cyberspace, the legitimacy of a law's authority claim cannot be assessed purely by reference to the constitution of the state making that claim, but additionally needs to achieve legitimacy in the eyes of those to whom it is addressed through the fairness, justice and appropriateness of the claims it makes –Reed and Murray (n 13) ch 7. This conception of legitimacy has similarities to Baldwin's analysis of legitimacy in relation to a state's administrative rule making, where he identifies five grounds for legitimacy: a democratic mandate, accountability for decisions, due process, expertise in the field, and efficiency of outcome in both popular and economic terms – Robert Baldwin, *Rules and Government* (Clarendon Press 1995). However, Baldwin's conception of legitimacy is a basis for challenge to those rules, either politically or via judicial review, and the authority of the rules remains effective for members of the state's law system unless challenged successfully. Because most cyberspace actors are outsiders to the rule system in question, the legitimacy of authority claims is instead used by them in deciding whether to confer authority on the claim by accepting it, or at least considering it.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Finally, we need to decide if the claim is accepted by a sufficiently large number[33] of those cyberspace users to whom it applies. To have authority a law-maker needs a legitimating community,[34] and that community confirms the legitimacy of the claim by accepting it, and thus granting the law-maker authority.

### *3.2. Achieving institutional legitimacy*

An institution might assert, with reference to its constitution, that its authority claims are legitimate. But this does not tell us whether legitimacy has in fact been achieved.[35] Instead, we must recognise that legitimate authority is a political rather than a legal construct, and a matter of fact which can only be determined by observing the behaviour of those to whom its claims are addressed: 'An institution is legitimate in the sociological sense when it is widely believed to have the right to rule.'[36] This tells us that it is necessary to identify the group to which those claims are directed, which will thus constitute the institution's legitimating community.

It is difficult to envisage a transnational institution which could realistically claim that the entire group of cyberspace users constituted its legitimating community. But we can easily find cyberspace institutions whose communities consist of identifiable subsets of the actors in cyberspace. Three examples of such institutions are examined in section 4 of this article.

A cyberspace institution is likely to have at least some degree of constitutional authority to make rules and regulations for its community. However, that authority is

[33] It is worth noting that in some fields of cyberspace activity there may be a small number of cyberspace actors who effectively set the standards for the other players in that arena, or perhaps even only one, and acceptance by that group or single entity might be sufficient to establish authority and legitimacy. Amazon, Facebook and Google are obvious candidates. Again, my thanks are due to Professor Christopher Millard. This issue is explored further in Andrew D. Murray, 'Nodes and Gravity in Virtual Space' (2011) 5 *Legisprudence* 195.

[34] See Christopher A. Thomas, 'The Uses and Abuses of Legitimacy in International Law' (2014) 34 *Oxford Journal of Legal Studies* 729, 747–49.

[35] See Niklas Luhmann, *Law as a Social System* (tr. KA Ziegart, Oxford: OUP 2008) 407, discussing the paradox that the legality of a constitution can only be determined by the institutions established by that constitution, which therefore have to presuppose the constitution's legality in order to give themselves power to decide the question.

[36] Allen Buchanan and Robert O. Keohane, 'The Legitimacy of Global Governance Institutions' (2006) 20 *Ethics & International Affairs* 405.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

likely to be weaker than in the case of physical world institutions, because of the more remote and impersonal nature of relationships in cyberspace. This suggests that cyberspace institutions will need to achieve a high level of charismatic authority, in addition to their constitutional authority. Charismatic authority would also assist intermediary service providers who wish to persuade their own user communities to comply with an institution's rules.

Both constitutional and charismatic authority, but especially the latter, can be enhanced by focusing on non-constitutional normative sources of legitimacy. These are what Paiement describes as the input, throughput and output aspects of law-making.[37] Input legitimacy concentrates on the participatory nature and inclusiveness of the norm-creation process, while throughput legitimacy examines the rule-making processes for procedural fairness and impartiality. Both of these are likely to be visible only to involved members of the institution's legitimating community, and so will mainly work to enhance constitutional legitimacy.

Output legitimacy is based on the quality of the rules themselves, particularly in terms of achieving their desired outcomes. This is something which is visible to all those who become aware of an institution's rules, not merely to involved members of its community, and is therefore a very strong component of that institution's charismatic authority.

One important element of output legitimacy is the status of the institution as a credible rule-maker. This is something which the institution itself, or the community which establishes it, can control through the development of its constitution and the selection of its members. But, so far as individual cyberspace users are concerned, this is perhaps the least visible element of output legitimacy.

Far more important is the manner in which the institution makes its authority claim, and also the normative content of the claim. Unlike the physical world where a

[37] Phillip Paiement, 'Paradox and Legitimacy in Transnational Legal Pluralism' (2013) 4 *Transnational Legal Theory* 197, 213–15.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

resident must either accept all the claims of a state's law system or deny them all,[38] in cyberspace the addressee can choose to accept only some of those claims and reject others.

What, then, will influence a cyberspace user's decision to accept the legitimacy of a law's authority claim? Three factors seem particularly important:

- the extent to which the law is perceived as being addressed to the cyberspace user, rather than to some other person;
- how far the law's provisions are congruent with the rest of the environment in which the cyberspace user acts; and
- the perceived fairness and justice of the law's claims to obedience.

There is insufficient space in this paper to examine these in detail,[39] but a single example of a spectacular failure of output legitimacy might serve to illustrate the pitfalls of ignoring these factors.

In 2003 the UK Financial Services Authority (FSA), the then financial regulator, attempted to impose the requirements of the e-Money Directive 2000[40] on mobile telephony companies.[41] Under the Directive, issuers of e-money were prohibited from engaging in non-financial service activities, which of course includes providing telephony services.[42] At that time mobile telephony companies were starting to allow pre-pay customers to make payments using the unspent float on their accounts. The FSA interpreted this as issuing e-money, and sent letters to those companies requiring them to obtain authorisation as e-money issuers.

---

[38] See J Finnis, *Natural Law and Natural Rights* (Clarendon Press 1980) 317: 'each obligation-stipulating law is a member of a system of laws which cannot be weighed or played off one against the other but which constitute a set coherently applicable to all situations and which exclude all unregulated or private picking and choosing amongst the members of the set. … either you obey the *particular* law, or you reveal yourself as lacking or defective in allegiance to the *whole* [system], as well as to the particular.'
[39] See further Reed and Murray (n 13) ch 7.
[40] Directive 2000/46/EC of the European Parliament and of the Council on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275/39, 27 October 2000 ('e-Money Directive 2000').
[41] UK FSA, Electronic Money: perimeter guidance (February 2003).
[42] e-Money Directive 2000, Art 1(5).

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

These letters highlighted the first problem of legitimacy. The mobile telephony companies did not dispute that the EU could legitimately regulate e-money, or that the FSA had constitutional legitimacy to seek compliance with financial regulation. But the e-Money Directive appeared to be addressed to new market entrants, who intended their main business to be the provision of a new kind of payment mechanism, and not to established businesses in other fields who were offering a payment service as a sideline to their main activities. Because it was not apparently directed to telephony companies, they perceived the claim that it should regulate their activities as unwarranted.

The second problem of legitimacy arose because the prohibition on non-financial services activities placed the companies in an impossible dilemma. If they complied with the FSA demand and registered as e-money issuers they would be prohibited from continuing to offer telephony services and would thus be in breach of their telecommunications licence terms as well as being forced out of business. If they continued to offer telephony services, they could not seek authorisation as e-money issuers. They thus denied that the FSA had any legitimate claim to apply the Directive to them, because it required behaviour which was practically impossible for them.

There followed a period of negotiation between the FSA, in which the companies proposed various solutions which would have enabled them to comply with the Directive while still carrying on business in telephony, but the FSA refused to consider any solution other than registration as e-money issuers or ceasing to offer payment services. The companies considered this application of the law to be illegitimate because they saw it as producing unfair and unjust results, the third legitimacy deficit. So, they responded in a commercially realistic way by defying the FSA and refusing to register, thus denying the legitimate authority of the Directive and the FSA's interpretation of it. Rather than force the issue, the FSA backed down and left the matter to be resolved as part of a then forthcoming review of payment services regulation at EU level, which eventually abandoned the prohibition on undertaking non-financial activities.[43]

[43] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L267/7 10 October 2009 Art 6(1)(b). In theory this Directive, together with the Payment Services Directive (Directive 2007/64/EC

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

The story is instructive because it shows that mere constitutional legitimacy, which was never in doubt, is not necessarily sufficient to achieve voluntary compliance with rules, even within a nation state's legal and regulatory system. It should be clear from this narrative how much less effective mere constitutional legitimacy will be in cyberspace, where institutions are likely to lack enforcement powers or experience real practical difficulties in exercising them.

## 4. New kinds of institutions?

Most of our current institutions derive their legitimacy from nation states; in other words, their legitimating community is made up of states rather than individuals. This makes them ill-suited to regulate many cyberspace activities because, so far as achieving compliance by individual cyberspace users are concerned, they have to rely on national law implementation of their rules. Unless all (or at least most) states agree to implement the same rules, the cyberspace user is faced with a multiplicity of differing rules about the matter, all of which have an equal claim to constitutional legitimacy and none of which can convincingly assert that they should be obeyed in preference to their rivals.[44] And the areas of law where harmonisation would be desirable are generally those where states disagree substantially about what the rules should be.

This suggests that further harmonisation in cyberspace will need to be achieved through new kinds of institutions which can regulate individual cyberspace users directly, bypassing the authority of nation states. What, ideally, might such an institution look like?

---

of the European Parliament and of the Council on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/1, 5 December 2007), creates a coordinated system of regulation for non-credit institution payment services. However, the dividing line between e-money issuers and other payment service providers is by no means clear, and this opens the way to further contradiction.

[44] DR Johnson and DG Post 'Law And Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367, 1376 (emphasis added): 'Because events on the Net occur everywhere but nowhere in particular, are engaged in by online personae who are both "real" (possessing reputations, able to perform services, and deploy intellectual assets) and "intangible" (not necessarily or traceably tied to any particular person in the physical sense), and concern "things" (messages, databases, standing relationships) that are not necessarily separated from one another by any physical boundaries, *no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws*.'

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

First, it will need to have a legitimating community which consists of that subset of cyberspace users to which the institution's rules are directed. The development of an institution which attempts to deal with all the harmonisation issues in cyberspace is unlikely because its legitimating community would consist of almost every person in the world. It is possible, though, to imagine an institution which attempts to regulate a single field of activity, and thus has a legitimating community which is limited to those cyberspace users who take part in that activity.[45]

Second, the institution itself will need a high degree of constitutional legitimacy. This can be achieved if the constitution is developed in partnership with members of the legitimating community and updated as the activities and needs of the community develop. This constitutional legitimacy can be enhanced by focusing on input and throughput legitimacy in the rule-making process. Community members, or their representatives, need to be involved in identifying the need for rules and devising their form.

Third, the rules produced by the institution should exhibit a high degree of output legitimacy. Achieving voluntary compliance has to be the aim, and this requires community members to be convinced about the appropriateness and fairness of the rules. Accountability, both in terms of rule-making and decision-making, plays an important role here.[46] Explaining the reasoning behind a rule or decision, the consultations which led to its adoption and then changes made in response to consultations, all play their part in persuading community members that the outcome was appropriate and fair. And if the constitution of the institution provides representation for community members, the ability

[45] This voluntary participation in the activity is what gives normative force to the institution's rules. See Linarelli, (n 5) 196: 'In a normative community that is not determined by state boundaries, the internal reflective attitude exists in both norm givers and norm users, towards both secondary and primary rules. … Role or identity seems to be key in understanding the practical authority of rules in normative communities not formed by political borders. For example, if a person accepts a role or identity of a merchant, then the law merchant rules relevant to that merchant grouping apply to her.'

[46] 'Accountability is a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgment, and the actor may face consequences.' M.A.P. Bovens, 'Analysing and assessing accountability: A Conceptual framework' (2007) 13(4) *European Law Journal* 447-468, 450.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

of representatives to participate and to challenge further enhances the legitimacy of the institution's authority claims.[47]

Finally, there should ideally be some mechanism for enforcing the rules against that minority of community members who refuse to comply voluntarily. Cyberspace institutions lack the enforcement powers of states, but as we shall see, their technical and economic power may be sufficient to achieve effective enforcement.

At first sight, this looks like a highly idealistic wish list. Nation states, even those with a long history of effective law-making and citizen acceptance, cannot meet all its requirements. And yet, there is already a small number of cyberspace institutions which largely does so.

### *4.1. ICANN*

The Internet Corporation for Assigned Names and Numbers (ICANN) is a US not-for-profit corporation which controls the internet's addressing systems, without which the internet would simply not work. It is clearly one of the most important regulators in cyberspace.

ICANN's authority as regulator derives from the charismatic authority of John Postel, who effectively ran both the IP number addressing system and the top-level (transnational) domain name system[48] from the early 1970s until the mid-1990s. ICANN took on these functions when it was formed in 1998 and has controlled them ever since.[49]

From the moment of its formation ICANN's constitutional legitimacy was challenged.[50] Initially it was governed by a board of directors who consisted mainly of

[47] For a detailed analysis of the democratic deficit in governance systems which are decoupled from democratic institutions see Yannis Papadopoulos, 'Problems of democratic accountability in network and multilevel governance' (2007) 13(4) *European Law Journal* 469-486. Although Papadopoulos deals only with governance systems which involve public actors such as politicians and administrators together with private actors, the analysis is clearly equally applicable to purely private cyberspace institutions such as those discussed below.

[48] This maps human-readable names, such as bloomsburyprofessional.com, to numerical IP addresses.

[49] For a history of this period, including the attempt by the US Government to assert control over the system, see SP Sonbuchner, 'Master of Your Domain: Should the US Government Maintain Control Over the Internet's Root?' (2008) 17 *Minnesota Journal of International Law* 183, 187–97.

[50] See JP Kesan and AA Gallo, 'Pondering the Politics of Private Procedures: the case of ICANN' (2008) 4 *I/S:* A Journal of Law and Policy for the Information Society 345; SM Ryan, RA Plzak and J Curran,

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

well-known figures from the internet technical community, but successors were merely appointed by the board and there was no effective representation of the user community. Eventually ICANN recognised the need to legitimate its authority, and adopted a new constitution which represents each of its legitimating communities, primarily registries and registrars, the internet technical community and national governments. All these have representation on the board and involvement in standards-setting and rule-making.[51] ICANN also publishes its policy development processes and working papers, invites participation by the public in policy development and engages in public consultation over policy changes.[52] This, together with the broad representation of its legitimating communities, provides a high level of accountability. In 2016 the US agreed to relinquish its residual elements of control in ICANN's governance, which has been revised to increase ICANN's constitutional legitimacy.[53] Now that this process is complete, there should be few doubts as to ICANN's legitimacy, in input and throughput terms as well as constitutionally.

But even before this work on legitimacy began, ICANN developed a rule system for dealing with disputes over the ownership of domain names. These disputes tend to arise because, although the system in theory operates on a first-come-first-served basis, in practice many of those who claim strong rights to the usage of a name (eg through registered or unregistered trademarks) find that someone else has beaten them to registration and wish to seek a remedy.

The rule system is embodied in ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP).[54] These rules apply only to the top-level domains (most importantly .com, .org and .net) over which ICANN asserts its authority, but the country-level domain systems such as .uk have adopted very similar principles in their own

---

'Legal and Policy Aspects of Internet Number Resources' (2008) 24 *Santa Clara Computer & High Tech Law Journal* 335.

[51] Details of the constitution and working processes can be found in the *ICANN Accountability & Transparency Frameworks and Principles* (ICANN, January 2008), available at <www.icann.org/en/system/files/files/acct-trans-frameworks-principles-10jan08-en.pdf> accessed 2 July 2021.

[52] See <https://www.icann.org/policy#participate> and <https://www.icann.org/public-comments> accessed 2 July 2021.

[53] <www.icann.org/stewardship-accountability> accessed 2 July 2021.

[54] ICANN, 'Uniform Dispute Resolution Policy' (24 October 1999) <https://www.icann.org/resources/pages/policy-2012-02-25-en> accessed 2 July 2021.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

regulations. The rules of the UDRP define when a domain name should be transferred to a claimant, and disputes are decided by online arbitration, which is outsourced to a number of providers, most importantly WIPO.[55]

The UDRP is the constitution for this rule system, and registrars sign up to the ICANN rules when seeking authorisation, while registrants of domain names enter into contracts with registrars which oblige them to submit to the dispute resolution system. Similarly, complainants who wish to contest a domain name registration sign up to the rules when submitting their complaint. This creates a web of contractual obligations which demonstrates the acceptance of the constitution by all those who have agreed to take part.

The UDRP has remained unamended since it was devised in 1999, so there is no space for community participation in rule-setting. The fairness and justice of arbitration panel decisions, all of which are published, is inevitably a matter of debate. There are suggestions that decisions tend to favour trademark-holders over ordinary cyberspace users,[56] but choices made by complainants[57] suggest that these decisions have strong legitimacy, in their eyes at least. The system runs in parallel to national trademark law, so complainants can choose between litigation and the UDRP, but the volume of complaints submitted to the WIPO element of the system alone (over 3,000 per annum in 2016-19 and over 4,000 in 2020[58]) suggests that the UDRP is seen as more legitimate by a very substantial margin.

Additionally, UDRP decisions are directly enforceable. Where a decision is in favour of a complainant, the registrar of the domain name is instructed to transfer it to the complainant. Registrars comply with these instructions because they are obliged to do so by the terms of their authorisation from ICANN. In theory a recalcitrant registrar

[55] WIPO decisions can be found at <www.wipo.int/amc/en/domains/decisionsx/index.html.> accessed 2 July 2021.
[56] See Michael Geist, 'Fair.Com: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP' (2002) 27 *Brook Journal of International Law* 903; Daniel M. Klerman, 'Forum Selling and Domain-Name Disputes' (2016) 48 *Loyola University Chicago Law Journal* 561.
[57] Participant choice, where such a choice is possible, has been proposed as a strong measure of the quality of a rule system – see A Schmidt, 'Radbruch in Cyberspace: about law-system quality and ICT innovation' (2009) 3 *Masaryk University Journal of Law and Technology* 195.
[58] <www.wipo.int/amc/en/domains/statistics/cases.jsp> accessed 2 July 2021.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

could be forced to comply or have its authorisation removed, but there are no reports of this ever happening.

It can be seen that the ICANN UDRP rule system largely meets all four elements of the legitimacy wish list. This is fortunate, because ICANN comes very close to regulating the whole community of cyberspace users within its limited sphere of activity. It is, though, a very complex institution which has taken nearly 20 years to achieve this state, and might not therefore be an ideal model for institutions which aim to regulate smaller communities.

### *4.2. eBay*

The regulatory problem facing eBay was simply that national law is inadequate to resolve disputes between its buyers and sellers. Most disputes are for small sums, usually far less than the fees chargeable even in national law small claims proceedings. Where seller and buyer are in different countries, national law is even less effective. This led eBay to develop its own rule system for consumer protection, which has been copied with some additional elements by other online trading platforms such as Alibaba. Schultz suggests that this system is so much superior to national law in practice that it could be seen as a community legal system, operating outside national law.[59]

The earliest eBay users developed a set of trading norms which achieved a high level of voluntary compliance because the eBay community was so small that participants felt they knew each other. As the community of traders and buyers grew this feeling could not be sustained, and so a feedback system was introduced to give each participant a public reputation, based on the experiences and comments of their trading partners.[60] Ultimately, continued growth produced the need for a formal way of resolving disputes,

[59] Thomas Schultz, 'Private Legal Systems: What Cyberspace Might Teach Legal Theorists' (2007) 10 *Yale Journal of Law & Technology* 151.
[60] A useful short history of the development of norms in eBay is in Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a borderless world* (Oxford: Oxford University Press 2006) 130–45.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

and so the community's trading norms were entrenched in the eBay user terms, to which buyers and seller must sign up to become members.[61]

The resulting rule system is known (in English) as the 'eBay Money Back Guarantee', and is included in substantially identical wording, allowing for language differences, in the terms of the eBay sites for the US, UK, France, Germany, Ireland and Australia. It appears probable that it is drafted to achieve the same effect in all of eBay's other sites. eBay claims that its sites attract buyers from 208 countries,[62] so there is no doubt that this system is a global one.

Sellers agree to comply with the procedures which underpin the Money Back Guarantee, and buyers are promised that eBay will operate those procedures to give redress in the specified circumstances so long as the buyer purchased using one of the specified payment methods.[63]

The eBay seller's obligations under the scheme are simple:

(a) sellers must deliver the products they sell; and

(b) the products must be substantially as described by the seller.

If sellers fail to meet these obligations, eBay runs an online mechanism for mediating and determining disputes. It begins by requiring buyer and seller to communicate in an attempt to reach a mutually acceptable settlement. If a settlement cannot be agreed, eBay staff review the claims of each side and decide whether the seller was in breach. If the buyer is successful eBay arranges for a refund; if PayPal was used, the seller's account with Paypal will be debited[64], or if the eBay site offers alternative

[61]For ebay.com, <https://www.ebay.com/help/policies/member-behaviour-policies/user-agreement?id=4259> accessed 2 July 2021, and for ebay.co.uk <https://www.ebay.co.uk/help/policies/member-behaviour-policies/user-agreement?id=4259> accessed 2 July 2021. All the eBay User Agreements, so far as is possible under the national laws which apply, impose the same trading obligations on sellers and buyers.

[62]<https://web.archive.org/web/20160425033304/http://sellercentre.ebay.co.uk/where-to-sell-internationally> accessed 2 July 2021.

[63] PayPal is always one of the specified methods, and still the most popular one, but eBay also operates the Money Back Guarantee if payment is made by credit card, debit card via eBay as an intermediary, or (in Australia) via the Paymate system.

[64] Under the PayPal User Agreement (clauses 5.3, 10.1 and 13 for UK customers, see <www.paypal.com/uk/webapps/mpp/ua/useragreement-full?locale.x=en_GB#4> accessed 2 July 2021.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

payment mechanisms, then eBay deducts the amount from monies it owes to the seller or otherwise reclaims the funds from the seller.[65] Most disputes are resolved within 14 days without any fee being charged.[66]

The eBay rule system garners some minimal constitutional legitimacy from the contractual agreement by sellers and complaining buyers to participate in it, though the rules themselves are controlled autocratically by eBay so there is no element of input legitimacy here. There appear to be few complaints that the dispute resolution process itself is flawed, though there are plenty of complaints by sellers that the results unfairly favour buyers (and, unsurprisingly therefore, few complaints about fairness from buyers). Perhaps the most telling measure of the system's legitimacy is how extensively it is used in preference to national law, even though national law in theory provides buyers with far more extensive rights than the eBay rules in many countries.[67] In 2010, the last year for which statistics appear to have been released, eBay handled in excess of 60 million disputes worldwide, averaging US$70–100 in value.[68] To put this number in context, in 2011 the *total* number of small claims handled by the UK courts (under £5,000 at that time) was in the region of 30,000, and the vast majority of these did not relate to complaints by buyers of products.[69] If any eBay buyer is dissatisfied with a decision there is nothing in the rules to prevent bringing a national law claim against the seller, but there appear to have been few if any such cases.

eBay's decisions under this rule system are enforceable entirely by eBay itself, without the need to refer to external legal systems. eBay has sole decision-making power once a buyer has referred a dispute to the process and, because the only remedy available is a refund, can enforce that remedy autonomously through its relationships with payment

---

[65] See Australian eBay User Agreement Clause 10, available at <https://www.ebay.com.au/help/policies/member-behaviour-policies/user-agreement?id=4259> accessed 2 July 2021.

[66] Though this, of course, means that the cost of the system is covered from the seller fees collectively and thus, ultimately, shared between all buyers.

[67] For example, the EU Consumer Rights Directive 2011/83/EU gives EU consumers the rights, inter alia, to prior information about the seller and charges, a right to withdraw from the contract, and rights to receive goods of appropriate quality. None of these are provided for in the eBay rules.

[68] LF Del Duca, Colin Rule and Brian Cressman, 'Lessons and Best Practices for Designers of Fast Track, Low Value, High Volume Global E-Commerce ODR Systems' (2015) 4 *Penn State Journal of Law & International Affairs* 243, 248, citing eBay Corporate Factsheet Q4 2010.

[69] UK Ministry of Justice, *Court Statistics Quarterly October to December 2012* 12, figure 1.3.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

providers. In practice the eBay rule-system operates like an autonomous transnational law system and is the primary source of regulation for the trading activities of its participants.

### *4.3. Google search and the right to be forgotten*

In 2014 the CJEU decided in *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Google Spain)*[70] that individual data subjects would sometimes have the right to request under the Data Protection Directive[71] that particular elements of their personal data available on third-party websites should no longer be disclosed by internet search engines. The court's reasoning, in simplified terms, was that in the case before it the information in question was so outdated that its continued processing by Google for the purposes of search had ceased to be fair, as required by Article 6 of the Directive.[72] This is usually referred to as the 'right to be forgotten', though it would be more accurate to described it as a right to be delisted.

Importantly, though almost in passing, the court made it clear that the decision whether any such demand was justified should initially be made by the data controller, ie the internet search provider: 'Requests … may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question.'[73] However, the court gave no guidance as to how internet search providers should make these decisions, other than that they should follow the provisions of the law.

---

[70] C-131/12, 13 May 2014.
[71] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31, 23 November 1995. The rights in question were to request erasure and blocking of data (Art 12(b)) and to object to further processing (Art 14(1)). The Directive has since been replaced by 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 (GDPR), but data subjects continue to have all these rights under the Regulation.
[72] *Google Spain* (n 70), para 72.
[73] ibid, para 77.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Following the initial spike of requests, the number of requests to Google fell slowly from an average of around 4,000 per week in November 2014 to around 2,000 per week in September 2017 and appears to have settled at that figure.[74] The volume of these requests has made it necessary for Google to set up an internal system for deciding whether to de-list; in effect, a non-state transnational judicial system.

Notionally, the rules to be applied by Google are those set out in the CJEU judgment. But, as commentators have pointed out,[75] that judgment does not explain in sufficient detail which rules are to be applied and how they interact, and in particular how the right to be forgotten should be balanced against other fundamental rights such as that to free speech. It is to be hoped that at some point Google will find a way of publishing key decisions whilst maintaining data subject privacy, but at present the body of decisions is rightly described as 'a jurisprudence built in the dark'.[76]

What is interesting for the purposes of this paper is the ways in which Google has (and has not) sought to achieve legitimacy for its decision-making system. The constitutional legitimacy of the system is established by the CJEU judgment, which holds that the law requires Google to make these decisions, but as we have seen, constitutional legitimacy alone is rarely sufficient to achieve user acceptance.

To date, Google's main focus has been on the input legitimacy of the system. Because the CJEU did not fully explain the rules which Google should apply, Google has adopted two external documents for this purpose. The first is the opinion of the EU's Article 29 Working Party, which was published in November 2014 and attempts to consolidate the views of the EU's national data protection supervisors about the rules and the process which should properly be applied.[77] Google has committed largely to follow

---

[74] Data from graph in Google, 'Requests to delist content under European privacy law' <https://transparencyreport.google.com/eu-privacy/overview> accessed 2 July 2021.

[75] See eg Pieter 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) *Computer and Telecommunications Law Review* 149, 158–59.

[76] 'Open Letter to Google from 80 Internet Scholars: Release RTBF Compliance Data' (*Medium*, 13 May 2015), available at <https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-datacbfc6d59f1bd> accessed 2 July 2021.

[77] Article 29 Working Party, 'Guidelines on the Implementation of the Court of Justice of the EU judgment on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja GonzáLez" C-131/12' (WP225, 26 November 2014).

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

these guidelines in making its decisions: 'We have carefully developed criteria in alignment with the Article 29 Working Party's guidelines.'[78] The second is a report by the Advisory Council which Google set up following the CJEU judgment. The Advisory Council held hearings in seven European capitals in the autumn of 2014, video of which is available online,[79] and took written evidence following a public call. The Council's report was published in February 2015,[80] and Google states that its findings will 'inform' the development of Google's de-listing policies.[81]

How far this legitimates the rules and process design is still a matter for debate. It is clear that in one respect, at least, Google is not following the recommendations of the Article 29 Working Party because it informs webmasters when their web pages are de-listed for a particular name search and also informs search users that some results are omitted under data protection law. Both these run counter to the Working Party's recommendations.[82] The work of Google's Advisory Council has been analysed at length by Chenou and Radu,[83] who point out that Google selected the topics for discussion in the public meetings, that the membership of the Council was largely chosen to be sympathetic to Google's interests, and that the public interest, particularly the view of data protection supervisors, was not adequately represented in the discussions. They conclude that: 'Rather than a broad dialogue, the work of the Advisory Council on "the right to be forgotten" can be better described as a framed and controlled process aiming to legitimize Google's practices.'[84] It seems likely that over time Google will need to do more to enhance the input legitimacy of its system.

So far, little attention has been paid to throughput and output legitimacy. The decisions made within Google remain obscure, and were not even available to the

[78] Google (n 74).
[79] <https://archive.google.com/advisorycouncil> accessed 2 July 2021.
[80] Google Advisory Council, 'The Advisory Council to Google on the Right to be Forgotten' (6 February 2015)<https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf> accessed 2 July 2021.
[81] Google (n 74).
[82] WP225 (n 77) 9-10.
[83] Jean-Marie Chenou and Roxana Radu, 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' (2017) *Business & Society* 1, 12–23.
[84] ibid 16.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Advisory Council as part of its work.[85] Google has made some attempt to bolster output legitimacy by publishing brief summaries of decisions which it believes raise important points of principle, as part of its Transparency Report,[86] but as at May 2019 only 108 summaries were disclosed from over 800,000 de-listing requests, although aggregated data analysis of the reasons for refusals to de-list is also published.[87] Although this information is interesting, it is hardly an adequate basis on which to assess whether the decisions Google makes are fair and just.

It is too early to predict how things will develop, but it seems clear that at some point Google will need to address the independence of this decision-making system because there is a conflict between Google's judicial role and its commercial interest in disseminating as much information as possible as widely as possible.[88] Other search providers such as Bing and Yahoo! are necessarily developing their own systems, and it would seem obvious for them to pool their experiences and develop a consolidated set of guidelines for making de-listing decisions. These might in turn evolve into a quasi-independent decision-making system, funded by search providers but not directly controlled by them, which would help legitimate the system further by demonstrating a degree of independence.

## 5. Conclusion

Can we, then, predict when and where these new kinds of transnational cyberspace institution are likely to develop? I suggest that there are three factors which, when they occur together, are likely to lead to a new institution.

---

[85] ibid 16.
[86] Google (n 74).
[87] <https://storage.googleapis.com/transparencyreport/faqs/eu-privacy/Google_EU_privacy_data_nov2015.pdf> accessed 2 July 2021.
[88] See Chenou and Radou (n 83) 20: 'The power delegation from the public to the private sector transforms the latter not only by adding new responsibilities (from indexing information to assessing the content of the links) but also by entrusting the corporation to adopt a public interest approach that would be typical of an independent agency. In principle, the public interest logic would encourage the deindexing of content, yet the corporate strategy would advise in favor of minimizing risks.'

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

First, there must be a single transnational problem in cyberspace, or a set of related problems, which nation states seem powerless to resolve. Powerless here means powerless in practice – it might be that states could in theory coordinate to solve the problem, but the time it will take to do so is longer than cyberspace users can tolerate. All the institutions discussed in section 4 were formed in reaction to an immediate need.

Second, the problem will need to affect a subset of cyberspace actors whose membership is sufficiently clear, usually from their participation in the regulated activity, that they can constitute the transnational legitimating community for an institution. Additionally, those members (or some of them) will need to be in a position to set up an institution and sufficiently motivated, often by their commercial interests, to do so.

Third, there will usually need to be tools of enforcement which do not require the involvement of national legal systems, and which the institution can control. These are likely to be technical/commercial tools, operating via the technological architecture of cyberspace.

To be successful, such an institution will need to legitimate its activities, primarily through the output legitimacy achieved by issuing decisions which are perceived by the legitimating community as being fair and just. If the institution achieves this, it arguably has greater legitimacy to regulate the problem than does any nation state or any transnational institution based on nation states.[89]

It might be objected that such institutions oust the authority of nation states, but as the examples in section 4 show, this is not so. Those institutions all defer to judgments of national courts, if judgments are issued. But such judgments are rare (I would argue because community members perceive the institution to be a more appropriate decision-maker), and in their absence the institutions instead operate, simply, as if the concept of the nation state did not exist. It should be clear that for all three examples, in the unlikely

[89] As between states, comparative legitimacy is embodied in the principle of comity which requires that a state should not claim to regulate persons within another state unless it is reasonable to do so, which normally means that regulation should be undertaken by the state which has the greater interest in so doing—see eg Restatement (Third) of Foreign Relations Law of the United States §403(1) (1987). In the case of a dispute between an eBay buyer and seller who are located in different states, it is hard to argue that either state has a closer connection with the dispute than eBay.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

event that all the world's nation states simply disappeared, then the institutions could continue their operations without interruption and without changing their rules. On a day-to-day basis, nation states are simply irrelevant to them.

Lawyers are often unhappy when it appears that private 'law' is taking over a domain previously reserved to national or international law, most likely because their training and experience is based on traditional understandings of law. But it must be remembered that this phenomenon is neither new nor exceptional. As Graz tells us:[90]

> 'On a long-term historical basis, the influence of non-state actors is not necessarily new. The state as we know it now, related to a given territory, controlling a closely defined population whose sovereignty is allegedly embodied in it, centralising monetary emission in conjunction with private agents – all this is a creation of the last third of the nineteenth century in the western world.'[91]

As Halliday points out, '"non-state" is in fact a continuation of something that prevailed until the modern state was formed'.[92]

[90] Jean-Christophe Graz, 'Hybrids and regulation in the global political economy' (2006) 10 *Competition & Change* 230, 235.
[91] Eric Helleiner and Andreas Pickel (eds), *Economic Nationalism in a Globalizing World* (Cornell University Press 2005).
[92] Fred Halliday, 'The romance of non-state actors' in D Josselin and W Wallace (eds), *Non-state Actors in World Politics* (Palgrave 2001) 27.

© 2022 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.