1. The lawmaking authority of states

It is pretty much axiomatic in jurisprudential thought that nation-states have unlimited authority to make laws, subject only to the constraints those states accept voluntarily by signing up to agreements with other states. The only doubts arise in respect of failing states or states in transition between governing regimes. Cyberspace forces us to challenge that axiom.

The challenge arises because cyberspace users continually face the situation that multiple nation-state laws claim to be applicable to their activities. Such claims appear uncontroversial if the cyberspace user is a resident or citizen of the state in question.¹ In that case, the state will have the ultimate power to enforce its authority claim against the person of the cyberspace user, or against property located in the state. In addition, by being present in the state the cyberspace user has submitted to the authority of the state. The authority of a state’s laws in this situation is largely undisputed.

But it is less obvious that a claim to authority is well-founded if the cyberspace user is a foreign resident whose only connection with the national territory of the claiming state results from the user’s activities in cyberspace. In this case, there is no relationship of state and citizen or resident, under which the cyberspace user can have expected to be subject to authority claims. Nor will it be obvious to the cyberspace user why else submission to the authority claim should be made, as the state is likely to have limited enforcement powers in that situation. It is inevitable, particularly if multiple states claim authority over the same activity, that cyberspace users will ask which, if any, of those laws ought to be obeyed; or to put it in jurisprudential terms, whether those lawmakers have authority to claim obedience to their laws.

Nation-states have never restricted their lawmaking claims to activities taking place within the geographical boundaries of the state. Commonly, states assert jurisdiction over their nationals throughout the world, none

¹ Though we will see in Ch 2 that there are circumstances in which a different rule-system may have greater authority even than a person’s home state law.
more so than in the regulation of activities of locally registered multinational companies. For example, in 1979 President Carter froze assets of the Iranian State held in accounts in London branches of US banks. Additionally, states claim authority over activities outside their physical jurisdiction but which nevertheless have effects, of the kind aimed at by the law, within the state territory. Typical examples include anti-competitive agreements between persons outside the state but which adversely restrict competition on markets in the state, pollution which crosses national boundaries, and so on. Of this type of activity perhaps the best known is the harm doctrine in informational torts. This allows an individual defamed within any jurisdiction in which the harm (damage) occurs to take a claim to the local courts. One consequence has been the rise of libel tourism before the High Court of England and Wales.2

In the pre-globalised world this ‘effects’ doctrine was mainly of concern only to multinational corporations and states themselves, because, with the exception of internationally published authors or writers – a very narrow group – most individuals and smaller businesses did not undertake activities whose effects might be felt outside the territory where they believed themselves to be acting. In cyberspace, however, things are very different:

… domestic laws now commonly regulate extraterritorial conduct and transnational litigation has blossomed. No longer limited to the antitrust and commercial contexts, courts apply all sorts of public and private laws to activity occurring abroad. Academics have encouraged the trend, finding the notion that law should be tied to territory to be an archaic remnant of a preglobalized world. In an age of globalization, the argument goes, law should find national and political borders of little significance. The enactment and application of extraterritorial laws have become unexceptional.3

Thus, a US publisher whose newsletter is available online can find itself sued in Australia for defamation even if the focus of the publication was the local, American, market,4 or a US-based online auction service can find itself accused of offences under France’s anti-Nazi laws.5

5 Ligue Contre Le Racisme et L’antisémitisme et Union des Étudiants Juifs de France v Yahoo! Inc et Société Yahoo! France (Tribunal de Grande Instance
Although there are moral and practical arguments in favour of defining a law’s sphere of extraterritorial application when it is enacted, in practice states rarely make any attempt to do this. A law which is silent on how far it applies outside its state’s territory leaves extraterritoriality to be decided by the relevant tribunal of that state. This tribunal will use the national rules of private international law (largely embodying the effects test) to determine the law’s applicability to activities in cyberspace. Unsurprisingly, once a tribunal has accepted jurisdiction over a case it is rare for that tribunal to decide that its national law does not apply.

The effects test, where a state may claim jurisdiction over conduct which has an effect or impact within its jurisdiction, wherever that conduct may have originated, is of general application. Thus, potentially any law, including laws made in the pre-cyberspace era and designed to control very different kinds of behaviour, might be held by the relevant national tribunal to apply to a cyberspace user. The consequence is that, analysed in their own terms, much of each nation-state’s body of laws is potentially applicable to cyberspace users who have no offline connection with the state. There are around 200 nation-states, and an even greater number of devolved or federal jurisdictions within nation-states, such as US States or the constituent jurisdictions of the United Kingdom. Thus all nation-states, and local lawmakers in federated or devolved jurisdictions, make authority claims in cyberspace.

This means that we cannot produce a satisfactory answer to the authority question merely by examining it from the internal perspective of a nation-state’s (or a devolved or federal legislature’s) legal system. From that perspective it will always be legitimate for the adjudicatory bodies of that system to apply its laws extraterritorially. Such an evaluation tells us nothing about the authority of that legal system’s claims when assessed from the external perspective of a non-resident person such as a cyberspace user. To investigate this matter, we need first to understand more about the nation-state’s lawmaking authority.
1.1 FRAMING THE QUESTION

To begin with, we need to decide whether to ask about authority at the level of the law system,\(^7\) or at the level of each individual law’s claim to authority. This distinction is vital.

By asking whether a state’s law system, taken as a whole, has authority over a cyberspace user, we are implicitly making an assumption that the law system’s authority is what Raz describes as ‘comprehensive’. He argues that legal systems

\[
\text{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}.\(^8\)
\]

From this it follows that authority is an all-or-nothing proposition – either all the system’s laws have authority or none of them do. It also follows, says Raz, that a law system claims its authority to be supreme and therefore denies the authority of all other law systems in respect of those over whom it claims authority.

Since all legal systems claim to be supreme with respect to their subject-community, none can acknowledge any claim to supremacy over the same community which may be made by another legal system.\(^9\)

These assumptions are challenged in Johnson and Post’s seminal article, ‘Law And Borders’.\(^10\) They argue that no state has authority to regulate activities which occur in cyberspace for four, interconnected reasons. First, they take the position that lawmaking is the exercise of power over those persons whom the state can control:

\[
\text{Control over physical space, and the people and things located in that space, is a defining attribute of sovereignty and statehood. Law-making requires}
\]

\(^7\) This useful term is borrowed from Aernout Schmidt, ‘Radbruch in Cyberspace: About Law-System Quality and ICT Innovation’ (2009) 3 Masaryk University Journal of Law and Technology 195. ‘Legal system’ implies a formal legislator and territorial boundaries, whereas ‘law system’ merely describes the set of laws which in fact apply to a particular activity, whatever their individual origins.


\(^9\) Ibid 119.

some mechanism for law enforcement, which in turn depends on the ability to exercise physical control over, and impose coercive sanctions on, law-violators.\textsuperscript{11}

By asserting a claim to apply national law, the state in question is also asserting a right to control the cyberspace activities of individuals who reside in other states, and this conflicts with those other states’ monopoly rights to exercise power over their citizens.

Johnson and Post recognise that some overlap in power claims is legitimate, via the effects test of private international law which is accepted and adopted by all states,\textsuperscript{12} and that these overlaps can be justifiable in the physical world. But they argue, as their second reason, that the effects test should not apply at all to activities in cyberspace. This is because those activities have no greater effect in any one state than in the remainder of the world, and so no state can legitimately claim to apply national law in preference to any other national law merely on the ground of effects.\textsuperscript{13}

The third limb of the Johnson and Post argument is based on their assertion that the legitimacy of a state’s lawmaking power derives from the consent of the governed and their participation in the lawmaking process. Claiming to apply national laws to cyberspace activities goes beyond the boundaries of that legitimacy because it extends the ambit of those laws to persons who have not so consented and who have no way to participate in the lawmaking process, for example through elected representatives.\textsuperscript{14}

Finally, Johnson and Post point out that one important role of geographical national borders is to give notice to individuals that they are entering a space to which different laws apply. But these borders do not exist in cyberspace, so that cyberspace users do not receive the notice to which they are entitled that their activities are now subject to a particular

\begin{footnotesize}
\begin{enumerate}
\item Ibid 1369.
\item But see Thomas Schultz, ‘Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface’ (2008) \textit{European Journal of International Law} 799, 811–816, arguing that the effects test is not compliant with general principles of public international law and should not be used, at least in its most expansive form, to determine the applicability of national law to online activities.
\item Johnson and Post (n 10) 1369, 1375.
\item Ibid 1369.
\end{enumerate}
\end{footnotesize}
state’s laws. The rule of law requires notice of a law’s claim to authority over one’s actions.

For these reasons, Johnson and Post conclude that the a-territorial nature of the internet precludes any state from making a legitimate claim to regulate it:

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.

Their answer to the question ‘Who, then, should regulate?’ was that the internet would develop ‘decentralised, emergent law’ wherein customary and privately devised laws, or rules, would be produced by decentralised collective action leading to the emergence of common standards for mutual co-ordination. In other words, they believed that the decentralised and incorporeal nature of cyberspace meant that the only possible regulatory system was one which developed organically with the consent of the majority of the citizens of cyberspace. In the longer term, cyberspace would develop its own governing institutions, whose legitimacy would derive from the consent of the internet users to whom the new rules would apply. Even though ‘established authorities will likely

---

15 Ibid 1370.
16 See further Ch 8, section 8.1.
17 Ibid 1376. See also 1390: ‘Governments cannot stop electronic communications from coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations. One nation’s legal institutions should not monopolize rule-making for the entire Net.’
continue to claim that they must analyze and regulate the new online phenomena in terms of some physical locations, the existence of a separate legitimate system of law for cyberspace would counter those claims.

There is an obvious response to this argument, which was swiftly made by a number of commentators, who suggested that Johnson and Post had failed to take account of the international nature of law in the late twentieth century. Drawing upon the international nature of legal settlements such as the law of the sea, aviation law, the laws and principles of human rights and environmental law, they pointed out that it was the nature of law in the modern global environment to display pluralistic characteristics. Thus, to say that cyberspace was effectively ungovernable due to its nature as a global communications media was naïve.

This counter-argument was best encapsulated in Goldsmith’s paper ‘Against Cyberanarchy’, where he argued that the Cyberlibertarian argument is ‘in the grip of a nineteenth century territorialist conception of how “real space” is regulated and how “real-space” conflicts of law are resolved’. This conception, he notes, ‘was repudiated in the middle of this century’. Goldsmith argues that the concept of law tied to a bordered territory is no longer applicable, and further that cyberspace transactions are no different to other forms of transnational transactions as both involve ‘people in real space in one territorial jurisdiction transacting with people in real space in another territorial jurisdiction in a way that sometimes causes real-world harms’ and ‘in both contexts, the state in which the harms are suffered has a legitimate interest in regulating the activity that produces the harms’. A few years later Goldsmith partnered with Wu to argue that order in cyberspace is only possible if that order is based on national laws. Thus, for example, they

20 Johnson and Post (n 10) 1390.
22 Ibid 1205.
23 Ibid 1200.
24 ‘Public goods and related virtues of governmental control of the Internet are necessary across multiple dimensions for the Internet to work, and as a practical matter only traditional territorial governments can provide such goods’: Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World (New York, Oxford University Press, 2006) 142.
assert that eBay’s commercial success demands that there be an enforceable law of contract and state law mechanisms for the detection and punishment of fraud.25

Although this line of thought reasserts the authority of national law systems, it does not adequately address the normativity of those authority claims. Indeed, Goldsmith and Wu base their entire argument on the enforcement power of the nation-state:

What we have seen, time and time again, is that physical coercion by government – the hallmark of a traditional legal system – remains far more important than anyone expected.26

This refocusing of legal authority on the state therefore deals only with practical authority. It tells us that every nation-state which has the power to enforce its claims to legal obedience against a cyberspace user has some degree of practical authority over that user. It does not tell us whether that authority claim is legitimately made, except in the very narrow sense that such authority claims must comply with the law system’s own internal rules.

Adopting a system-centric viewpoint in which the law system’s authority is comprehensive asserts a number of logical contradictions.

First, though implicitly rather than expressly, it claims that every cyberspace actor is subject to the collective set of those national laws which are applicable (in their own terms) to cyberspace. The effect is to posit a single, global system of law, which emerges from the unconnected activities of disparate national law systems.27 Although we may not be able to positively identify such a system of ‘global’ law, examples abound of its effects, such as Richard O’Dwyer, an English student

---

25 Ibid Ch 8.
26 Ibid 180.
27 Few would argue that such a global system of law actually exists, though some commentators suggest that it is, conceptually at least, a possibility. See e.g. Werner Krawietz, ‘The Concept of Law Revised – Directives and Norms in the Perspectives of a New Legal Realism’ (2001) 14 Ratio Juris 34, 38: ‘From the point of view of a theory of norms and action, the legal systems of modern society as a whole in their form, structure and functions could – virtually, at least – be regarded as one single information and communication system, although this has not been achieved completely as yet.’ See also Benedict Kingsbury, ‘The Concept of “Law” in Global Administrative Law’ (2009) 20 European Journal of International Law 23, 29: ‘A convincing rule of recognition for a legal system that is not simply the inter-state system has not been formulated, the institutions for “adjudication” are often non-judicial and sometimes absent, and the processes of change are not easily articulated in terms of rules.’
operating a website primarily for a UK audience who, in 2012, found himself before the Southern District Court of New York facing two charges of criminal copyright infringement,28 or more recently the finding of the Supreme Court of Canada in 2017 that Google must comply with an order of the Court of Appeal of British Columbia to filter global as opposed to local search results.29 Further, because the applicability of each of those laws is dependent on the effects of the cyberspace actor’s activities in each national territory, and as these effects are likely to differ as between actors, the result is that each actor is subject to a different and individualised emergent law system. In other words, cyberspace is subject to as many different law systems as there are cyberspace actors.

Second, because each state’s law system has comprehensive authority, then if that particular law system has authority over the cyberspace actor its laws should be obeyed in preference to other states’ laws. This is also true for every other state’s law system, so that each is supreme to every other. This is a logical impossibility, and cannot be avoided by somehow identifying a hierarchy of supremacy between states because, as Johnson and Post demonstrated, there is no justification for any one state claiming higher lawmaking authority over cyberspace than any other.

In addition, as we shall show in Chapter 7, contradictory national laws that are applicable (in their own terms) to a cyberspace actor drastically weaken the legitimacy of the authority claims of those laws. This is not in itself a reason to deny the authority of a law system completely, but it may justify denying the authority of that particular claim and is likely to weaken the force of all other authority claims by that law system.

However, it might still make sense to examine this problem of authority from a law system perspective if we depart from the assumption that law systems must claim comprehensive authority. If a law system limits its authority claims in cyberspace to those claims which are

---

28 USA v O’Dwyer, SDNY, Case No. 1:10-mj-02471 (28 November 2012).
29 Google Inc v Equustek Solutions Inc [2017] SCC 34 (Canada). It should be noted however that following the pattern set out in LICRA v Yahoo! Inc. (discussed here) the Northern District of California issued a preliminary injunction on 2 November 2017 (in the case of Google LLC v Equustek Solutions Inc, Case No 5:17-cv-04207-EJD, 2017 WL 5000834 (ND Cal Nov 2, 2017)) enjoining Equustek from enforcing the global de-indexing order it had obtained against Google in Canada. On 14 December, with Equustek choosing not to defend the proceeding, the court issued a one-page default judgment making the injunction permanent (Google LLC v Equustek Solutions Inc, Case No 5:17-cv-04207-EJD (ND Cal Dec 14, 2017)).
The lawmaking authority of states

legitimate then, even if the problem of competing authority claims does not disappear, it is certainly diminished to perhaps a manageable level.

The case of LICRA v Yahoo! Inc\(^{30}\) illustrates how such a conflict might be managed. In that case a French judge ordered Yahoo! to take ‘all necessary measures … to make impossible’ access to Nazi material via Yahoo!’s California-based online auction service because making such material available to persons in France infringed the state’s anti-Nazi laws.\(^{31}\) The judgment justified this claim to apply French law on the basis that the auction service was accessible from France, and following a report from experts Ben Laurie and François Wallon that ‘the association of two procedures, geographical identification of the IP address and declarations of nationality, would probably make it possible to reach a rate of filtering close to 90%’.\(^{32}\) On this basis, and despite some dissenting opinion from the third expert, Vint Cerf, Judge Jean-Jacques Gomez found that Yahoo! could control its accessibility via geolocation information to a level of certainty enough to justify ordering such controls to be put in place. In response, Yahoo! sought and secured a declaration from the Northern District of California court that this order would not be enforceable against Yahoo! in the US.\(^{33}\) The US judge recognised the potential legitimacy of the French law claim to authority,\(^{34}\) but gave precedence to the US First Amendment so far as enforcement by a US court was concerned. These judgments left Yahoo! to devise an appropriate course of action for itself, and ultimately it decided to

\(^{30}\) Above n 5.

\(^{31}\) This order clearly could not be obeyed completely, and so at a subsequent hearing it was indicated that substantial, rather than full, compliance would suffice to fulfil the order, on the basis that expert evidence indicated that it was feasible for Yahoo! to identify the location of around 90 per cent of its auction site users, and this would be enough for substantial compliance (Tribunal de Grande Instance Paris, Court Order No. 00/05308, 20 November 2000).

\(^{32}\) Ibid.

\(^{33}\) Yahoo! Inc v La Ligue Contre Le Racisme Et L’Antisemitisme, 169 F Supp 2d 1181 (ND Cal, 2001), overturned on appeal on the ground that the first instance court had no jurisdiction to hear the suit because enforcement had not yet been threatened: 379 F 3d 1120 (9th Cir 2004).

\(^{34}\) ‘In a world in which ideas and information transcend borders and the Internet in particular renders the physical distance between speaker and audience virtually meaningless, the implications of this question go far beyond the facts of this case … The government and people of France have made a different judgment based upon their own experience. In undertaking its inquiry as to the proper application of the laws of the United States, the Court intends no disrespect for that judgment or for the experience that has informed it’: 169 F Supp 2d 1181 (ND Cal, 2001) 1186.
prohibit the sale of Nazi memorabilia via its service, world-wide, although the company denied that its decision was in direct response to the French court ruling on the case, saying instead that it was responding to users who had requested a more active policy for its site’s content.

Nation-states do accept some limitations on the authority of their laws. As an example, most states choose to restrict the application of company law to companies that are registered in the state. Thus if a multinational company established in state A does business in state B, state B will normally claim authority over some of the company’s activities, including contracts to be performed within the state, employment of staff in the state, and local consumer rights. However, it will not normally claim authority over the company’s internal management structure, rules of audit or their corporate or group tax affairs – these are left to the law of state A as the state of incorporation. Provided the law in question has a clear geographical scope of application it is common for the authority claim to be limited to the state’s territory.

Further, it is possible (though not common) for states expressly to limit the extraterritorial application of laws by making it clear, or at least clearer than the effects doctrine does, which effects will trigger the application of the law. As an example, the UK Financial Services and Markets Act 2000, s 21(3) provides that, ‘In the case of a communication originating outside the United Kingdom, subsection (1) [the prohibition on issuing an invitation or inducement to engage in investment activity] applies only if the communication is capable of having an effect in the United Kingdom’. The effect envisaged here is clearly that some person in the UK engages in investment activity as a consequence. This drafting, which was a response to the growth of online advertising, recognises that a claim by the UK law system to regulate all investment advertising, world-wide, would be an excessive attempt to exercise authority.

More commonly, states limit the authority claims of their laws by means of their internal rules of private international law. These determine whether a foreign individual is subject to the authority of the state’s adjudicatory bodies, and whether a particular law of that state applies to the individual. For the most part these rules of private international law are based on the state’s conception of when it is legitimate for the state to make an authority claim.

This is explicit in the US rules, which derive from the due process provisions of the US Constitution, set out in the Fifth and Fourteenth Amendments. In a long line of jurisprudence originating in the Supreme
Court decision in *International Shoe Co v Washington*,35 due process has been interpreted as meaning that it is not permissible for a non-resident defendant to be subject to judicial proceedings unless there is a sufficiently close connection between the defendant and the jurisdiction (often described as the ‘minimum contacts’ doctrine). As explained in *CompuServe v Patterson*:36

This court has repeatedly employed three criteria to make this determination: First, the defendant must purposefully avail himself of the privilege of acting in the forum state or causing a consequence in the forum state. Second, the cause of action must arise from the defendant’s activities there. Finally, the acts of the defendant or consequences caused by the defendant must have a substantial enough connection with the forum to make the exercise of jurisdiction over the defendant reasonable.

The EU has specifically legislated on this matter although the legislation is less explicit as it attempts to establish a number of ‘bright line’ tests for deciding applicable law and jurisdiction. The tests are based on the connections between the dispute and the relevant state, such as the residence of the defendant or the place where tortious damage occurred, and it is implicit that these connections are sufficient to justify the state’s authority claims. In respect of applicable law, the legislation expressly recognises that the law otherwise applicable under the bright line rules should be disappplied in favour of another country’s laws if the dispute is ‘manifestly more closely connected’37 with that other country.

However, all these internal limits on a law system’s authority claims apply at the level of individual rules of law, rather than at the system level. To return to our company law example, there is no point in a multinational company incorporated in state A asking itself whether state B’s law system has authority over its corporate affairs. Instead it needs to examine the individual rules of state B’s company law to decide which are applicable only to entities incorporated in state B, and which potentially have wider application, and then to review state B’s private international law to decide if any of the latter group are likely to be

35 326 US 310 (1945).
36 89 F 3d 1257 (6th Cir, 1996).
applicable. If states themselves deal with claims to authority at the rule level rather than the system level, our analysis must do the same.

1.2 THE AUTHORITY OF INDIVIDUAL RULES OF LAW

Thus far we have seen that states cannot justifiably claim comprehensive lawmaking authority in cyberspace, and that in fact they accept that the authority of their lawmaking has to be limited at the level of individual rules of law. Thus we cannot explain whether our cyberspace user should accept a state’s authority claim by examining the authority of that state’s law system as a whole. Instead, we need to seek the answer for each individual authority claim, that is, each individual rule of national law.

Cyberspace creates a situation where multiple and overlapping systems of rules all claim some degree of authority over our actions, a phenomenon which Santos has described as ‘interlegality’. Faced with this situation, the individual is forced to make choices as to which rules to follow. By making such a choice, the individual is accepting the authority claims of the rules which are followed, and denying the authority claims of those which are not followed.

It is important to stress here that this denial of authority is unlikely to be a conscious process. Rarely is the individual faced with a simple choice between two conflicting rules. Far more likely is the situation where the individual is aware that multiple authority claims are likely to be being made, and selects the rule which will be followed for a combination of largely pragmatic reasons.

A good illustration would be the publishing of a statement online which has the potential to be objected to as defamatory by the subject of the statement. Because that statement will be visible world-wide, there are potential claims to apply multiple national defamation laws.


39 Though such instances of conflict are not unknown, and can often lead to complex political negotiation. A comparatively recent example is the conflict faced by the interbank financial network SWIFT between US anti-terrorism laws, which required the disclosure of personal data and EU data protection law, which forbade its disclosure. See Article 29 Working Party Opinion 10/2006 (WP 128) for a detailed explanation of the issues involved.

40 Usually on the basis that the claimant has sufficient reputation in that country to justify its courts accepting jurisdiction to hear a defamation claim –
publisher might⁴¹ be aware of (or investigate and discover) some of these, but will remain ignorant of most.⁴² Defamation law is notoriously variable between jurisdictions, and in many cases the statement will clearly be actionable in some, clearly not actionable in others, and in the remainder the likely outcome of litigation will be uncertain. By making a decision to publish or not to publish, the individual is deciding to frame his or her actions in accordance with some set of these known rules and, therefore, refusing to accept the authority of the others. In respect of all unknown rules, by deciding not to investigate them the individual is in effect denying their authority from the outset. Whether the individual accepts the authority of all the rules which are congruent with the chosen course of action is probably not something ever considered – decisions like this tend to be framed in terms of risk analysis rather than acceptance and denial of authority – but as a matter of fact, choosing not to follow a rule of law which is applicable (in that law system’s own terms) is a denial that the rule is authoritative, for that individual, in those circumstances.⁴³

Why, then, might the individual deny the authority of a national lawmaker in relation to an individual rule of law?

Most obviously, the individual might decide (or be advised) that the rule is not applicable according to the rule’s own law system. For example, the state’s authority claim might be illegitimate under the internal rules of that state’s law system, perhaps if the law in question does not meet the requirements for internal legitimacy such that it has no authority for persons resident in the state.⁴⁴ This would be a law which fails to meet Hart’s rule of recognition or to comply with Kelsen’s grundnorm. A typical instance is a law which is unconstitutional.

see e.g. Dow Jones & Co Inc v Gutnick [2002] HCA 56, [2003] 1 LRC 368 (Australia); Don King v Lennox Lewis [2004] EWCA Civ 1329 (England and Wales).

⁴¹ Some publishers, especially individuals using social media, are likely not to consider any laws at all.

⁴² This is likely to be true even for large multinational enterprises, who demand that their legal advisers investigate only the most ‘important’ or ‘relevant’ authority claims rather than researching the laws of every country in the world. See further the discussion of corporate decision-making in Ch 3, section 3.2.2.

⁴³ This final caveat is important – the question of authority arises afresh for each activity to which it might apply, so that in different circumstances the individual might make different authority choices.

⁴⁴ See further Ch 7.
Alternatively, the law might be authoritative for persons resident in the state, but the claim to apply it to persons outside the state is recognised by the state’s law system to be unjustifiable, at least in the particular case of the individual in question. As explained above, a state’s rules of private international law deal explicitly with this issue, limiting the state’s authority to claim to apply its laws extraterritorially, usually by reference to the connection between the individual and the state.

But how often will the individual who needs to choose between the authority claims of states have any information about the status of those claims under the state’s own internal rules? This is arcane knowledge, accessible only to particularly expert lawyers, and is unlikely to play much of a role in making the decision.

The more likely reason for such a denial of authority is that the cyberspace user does not accept that their activities place them within the group of persons over whom the state can make a justifiable claim of authority to legislate, at least for the particular rule of law in question. If no state has universal authority to make laws regulating cyberspace, and states do not in fact claim such authority, there must be limits on those persons over whom a state can make a legitimate authority claim. What are those limits? In order to decide this question, we will need to understand what it is that gives a state authority to make laws in the first place.

This question cannot be answered simply by referring to the state’s internal rules for lawmaking legitimacy because these are merely elements of the claim by the state to authority. Arguing, as Kelsen does,45 that each law system gains its authority from its grundnorm, and that the scope of authority of these grundnorms cannot overlap, assumes rather than proves that only established law systems are capable of producing authoritative laws.46 Similarly, 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. The result of adopting this purely internal viewpoint, as Cotterrell points out, is that ‘a diversity of valid, competing legal systems or legal regimes, co-existing in the same social environment yet not integrated, cannot be envisaged’.

But as we have seen, in cyberspace we do have such a diversity of valid, competing legal systems, even if we only take nation-state laws into consideration. The grundnorms of these systems cannot be what confers external legitimacy on their authority claims, even if those grundnorms legitimate the authority claims internally to the state. As MacCormick points out, this should be seen as an opportunity, not a challenge: ‘To escape from the idea that all law must originate in a single power source, like a sovereign, is thus to discover the possibility of taking a broader, more diffuse, view of law.’

Instead, we need to look outside the law system itself for the sources of legitimacy. Cotterrell 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.

It seems clear that 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’ and as the reasons behind ‘voluntary subjection to a claim to authority’.

---

50 Roger Cotterrell, ‘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.
But of course, authority cannot be merely a matter of individual choice, for if it were the concept of authority would be so diffuse as to be meaningless. Instead, we must look for a collective acceptance of an authority claim by the overwhelming majority of those to whom the claim is addressed. A rule of law will be recognised by this group of addressees as having legitimate authority if they collectively agree that it was properly addressed to them, and rejected if they collectively believe it was improperly addressed.

So this returns us to the relationship between a state and the individual addressed by the law. What is the nature of the relationship which leads to acceptance of the state’s lawmaking authority?

1.3 LEGITIMATING AUTHORITY AND THE COMMUNITY OF THE STATE

The most plausible answer, generally accepted by commentators, is that a legal system’s rules of law have legitimate authority for the members of the community which that system regulates. Thus, for example, Hart’s discussion of the idea of obligation53 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 if the nation-state is taken as the starting point, as it is in positivist writings at least, the identity of the community becomes confused with the territory of the state. This is because in pre-cyberspace times the overwhelming majority of the community were resident in that territory. As a result it was rare to ask how far the community might extend beyond the geographical territory of the state.

Nonetheless, we will take as given that the residents of a state’s territory are a part of the community which accepts and acknowledges the authority of laws produced by that state’s law system. Our inquiry will focus on those persons whose only connection with the state is via their activities in cyberspace. We need to decide whether, and in what circumstances, they are part of that state’s law system’s community, and ought thus to acknowledge the authority of its laws.

The conception that a state might have an extended community, going beyond the state’s territorial borders, is not new. Raz, taking the position that perceived membership of a community which has a legal system

53 Hart (n 47) 82–91.
might be one (though not the only) source of respect for the law, recognizes the potential difficulty in defining the boundaries of the community though he does not address the question further:

The search for an obligation to obey the law of a certain country is an inquiry into whether there is a set of true premisses which entail that everyone (or every citizen? every resident?) ought always to do as those laws require …

More in-depth assistance can be found from the thinking of natural lawyers and legal sociologists, because their starting points are not fixed to the nation-state and its territory.

Finnis, the leading modern scholar from the natural law tradition, asserts that the authority of a lawmaker within a community is derived from the fact that its authority is by and large obeyed by members of that community. This fact of general obedience creates an obligation that all members should obey those rules because doing so advances the common good of the community. Achieving this aim requires coordination between the community members, which creates a need for norms, which in turn creates authority.

There is no assumption here that the community which is obliged to obey the laws of a particular legal system is necessarily the same as the residents of a state’s geographical territory. Rather, the community is a group which is interacting towards a common end, or set of common ends:

… political community exists partially (and sometimes primarily) as a kind of business arrangement between self-interested associates … partially (and sometimes primarily) as a form of play, in which the participants enjoy the give-and-take, the dissension, bargaining and compromise, for its own sake as a vastly complex and absorbing performance; partially (and sometimes primarily) as an expression of disinterested benevolence, reinforced by grateful recognition of what one owes to the community in which one has

---

54 'A person identifying himself with his society, feeling that it is his and that he belongs to it, is loyal to his society. His loyalty may express itself, among other ways, in respect for the law of the community': Raz (n 8) 259.
55 Ibid 234.
56 'These normative consequences derive from a normative principle – that authority is a good because required for the realization of the common good – when that principle is taken in conjunction with the fact that a particular person, body, or configuration of persons can, for a given community at a given time, do what authority is to do (ie secure and advance the common good)'. John Finnis, Natural Law and Natural Rights (Oxford, Clarendon Press, 1980) 246.
57 Ibid 153.
been brought up and in which one finds and founds one’s family and one’s life-plan, and further reinforced by a determination not to be a ‘free rider’ who arbitrarily seeks to retain the benefits without accepting the burdens of communal interdependence; and characteristically by some admixture of these rationales.\textsuperscript{58}

Geography is not the determining factor. Finnis specifically notes that communities can transcend geographical boundaries: ‘sharing of aim rather than multiplicity of interaction is constitutive of human groups, communities, societies’.\textsuperscript{59}

This line of thinking is helpful in understanding how a state law system’s subject community can extend outside the state’s borders, but it does envisage some degree of permanence or persistence in community membership. A community without at least a stable core membership cannot generate a conception of the common good.

From a very different starting point, that of empirical investigation, the sociologists of law come to remarkably similar conclusions. Cotterrell identifies that globalisation has produced transnational ‘networks of community’ which might act as the basis of regulatory authority.\textsuperscript{60} This does not mean the monist law system community of cyberspace envisaged by Johnson and Post, but rather a diversity of communities:

In its dominant modern form, constitutional authority has been treated as presupposing a supporting, legitimising community – ‘the people’ – which hardly seems to exist on a transnational basis. In fact, I shall argue here, transnational legal authority \textit{does} need to be linked to an idea of ‘community’ but this idea must be understood sociologically and examined empirically. It is not productive to rely on rhetorical appeals to some global ‘international community’, understood as a diffuse demos, to provide democratic legitimacy for transnational constitutionalism … but \textit{some kind} of particularity of a constitutional community is essential and a sociological perspective is needed to examine empirically what kinds of community exist transnationally to support regulation.\textsuperscript{61}

\textsuperscript{58} Ibid 149.
\textsuperscript{59} Ibid 152.
\textsuperscript{60} Cotterrell (n 48) 12–13.
\textsuperscript{61} Ibid 40.
This understanding links authority and legitimacy in a clear way. To have authority a lawmaker needs a legitimating community, and that community confers legitimacy by accepting the lawmaker’s authority and thus subjecting itself to that authority.

From this perspective, the likely solution to the problem of multiple claims to lawmaking authority becomes clearer. The cyberspace individual should accept the authority claims of those nation-states where the individual is a member of the state’s extended community in cyberspace, but should reject the claims where the individual is not a community member:

instead of continuing to invoke such old criteria for jurisdiction as the physical presence of people or things in a geographical location, law and globalization scholars should be at the forefront of thinking about how communities are appropriately defined in today’s world and whether there might be new ways of delimiting the scope of legal jurisdiction or developing hybrid jurisdictional or choice-of-law models.

If we apply this analysis to activities in cyberspace it is often easy to see when a cyberspace actor has joined a foreign community as a member. The simplest example is an e-commerce business. In metaphorical terms, either it has used cyberspace to transport its shop to the customer’s computer, phone or tablet; or the customer has travelled online to visit the shop at the business’s home location. Which of these is the case can be determined by reference to the marketing activity of the e-commerce business and the quantity of transactions undertaken with foreign customers.

For example, a UK-based e-commerce business which places its offline advertising solely in UK print publications or broadcast media

---

64 This mirrors Orin Kerr’s Internal/External Perspective as found in ‘The Problem of Perspective in Internet Law’ (2003) 91 Georgetown Law Journal 357. There, Kerr notes that ‘the internal perspective adopts the point of view of a user who is logged on to the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct’ while ‘from the external viewpoint the Internet is simply a network of computers located around the world and connected by wires and cables’ (at 359, 360). We may say that applying an internal perspective the e-shop has created a virtual branch in the buyer’s local community, while applying the external perspective the buyer has used its tablet or phone to communicate with the business at its place of business.
focuses its online marketing on UK users will identify itself as part of the UK law system community only. If an order is received from a foreign customer, the business will perceive the customer as travelling via cyberspace to the UK, and thus not consider itself under any obligation to obey that customer’s home state laws even if they are, on their own terms, applicable. However, if orders are received regularly from a particular foreign country then, at some point, the business is likely to see itself as participating in the commercial life of that foreign country as well. This transition may well be marked by a change in marketing practices, such as quoting prices in that country’s currency, directing online advertising to its residents using their national language, and perhaps also by seeking advice as to that country’s laws.

Conversely, an e-commerce business which deliberately sets out to make sales to customers in a particular country will consciously be joining that country’s community from the outset. An e-commerce business which sells physical products will need to arrange effective logistics in each country where it makes sales in order to achieve timely delivery. Thus, a common strategy for business expansion is to add one country at a time to the list of those from which the business is prepared to accept orders. This is often accompanied by customisation of part of the website for that country, written in the relevant national language and incorporating pricing in the local currency. This is clear evidence that the business has joined the target country’s trading community, and thus that it is legitimate for the country to impose its trading laws on the business’s activities.

But this last scenario immediately raises a further question. Do these facts give that country authority to regulate the whole of the e-commerce business’s activities, or only that part of them which relates to sales and marketing to persons in the country? If we are to avoid reintroducing the problem of overlapping and incompatible claims to authority, we have to recognise that the state’s authority claim is only legitimate in relation to that part of the business activities which constitutes trading with the country.

We also need to ask whether the authority of the state in question is limited to imposing only those laws which regulate trading activities, or whether all of the laws of the country apply. Again, the only way to avoid the multiple authority problem is to accept that the country’s authority is partial, and thus restricted to those business activities which directly affect the country. Thus, as explained earlier, the e-commerce business should not be subject to the country’s corporate laws, or at least not the majority of them, but would clearly be under an obligation to comply
with its sales law, consumer law and parts of its tax law, such as collection of local sales taxes.

This tells us that a law system’s authority works differently outside its geographical territory, and particularly in cyberspace. Far from being ‘comprehensive’ in Raz’s sense, a state’s authority is partitioned into spheres of activity, each of which is potentially capable of being authoritative for cyberspace actors who are engaging in that activity, whilst the state’s other laws have no authority for that actor. Cyberspace actors are similarly ‘partitioned’ – to take our e-commerce business again, most (though perhaps not all) of its home country laws will apply to all its activities, but its trading activities will (also) be subject to the authority of a range of other state’s laws depending on the nature of the relationship between those activities and those states.

These differences may only be differences of degree however. It seems to us that the territorial authority of state law systems might work in the same way, even though this has not so far been recognised because the exceptions to the conventional wisdom are so trivial.

Let us imagine Alicia, a resident of Utopia who visits Ruritania. Alicia telephones from her home in Utopia to book a hotel room. In so doing she subjects herself to the authority of Ruritanian law insofar as it relates to this transaction, but at this stage to no further extent. Once she arrives on Ruritanian territory she, by doing so, accepts the authority of the major part of Ruritanian law and accepts its legitimacy to control her everyday actions and transactions while in Ruritania, but vitally she does not accept the complete body of Ruritanian law – she does not, for example, accept the authority of the rule that residents of Ruritania must pay tax on their world-wide income, because her period of residence in Ruritania is only temporary. However, should she undertake paid employment while in Ruritania it would be expected that she would be liable to local Ruritanian taxation on that particular part of her global earnings. Should she fail to declare and pay this tax bill while in Ruritania she will remain subject to the authority of Ruritanian law once she has returned home with regard to this claim, even though she is no

---

65 See text to n 8 ff above.
66 For example, a state’s sales law might not apply to a resident e-commerce business in relation to its sales to foreigners because the state’s rules of private international law make the buyer’s national sales law applicable.
67 This might arguably be because the wording of Ruritanian tax law applies the rule only to ‘permanent’ residents, but we would contend that our tourist would be likely to deny the legitimacy of a law which omitted this word and attempted to tax her on the basis of her temporary visit.
longer present in the jurisdiction. However, this only gives Ruritania legal authority over her in respect of proceedings to recover her unpaid tax levied in Ruritania, not general authority to apply Ruritanian law over other aspects of her life. Even that Ruritanian law which continues to have legitimate authority over her once she has left the country may be seen to be practically lacking in force. The practical difficulty in enforcing this legitimate authority once she has left the country might lead Ruritania to choose not to exercise its authority after all, and to write off the unpaid tax bill.

This analysis also tells us that the community over which a state has legitimate authority is diverse, diffuse, and most importantly that it is dynamic rather than static. Its core is made up of persons resident in the state, who are subject to the authority of all the state’s laws and are clearly part of its legitimating community. Membership of this part of the community changes comparatively slowly. There is, however, a second part of the state’s community in cyberspace which consists of those who have continuous and persistent communication with residents of the state. Our example e-commerce business, with a section of its website devoted to sales to that state, would be such a member. This group is justifiably subject only to the authority of those laws which relate to the online activities of its members, and not to the other laws of the state. Whether the group constitutes part of the state’s legitimating community is a difficult question, to which we will return in Chapter 3. The final part of the community consists of visitors to the state, both to its physical territory and to its virtual sphere of authority in cyberspace. These visitors subject themselves temporarily to the authority of those laws of the state which are pertinent to their visit, but cannot form part of the legitimating community because their connection to the state is insufficiently permanent to allow them to engage in the political discussions which define the common good or shared objectives of the community.

---

68 As Cotterrell (n 50) observes, ‘Social relations (especially those that concern transnational law) tend to flourish and decay, contract and expand, assume varying forms and transmute in complex, intersecting, overlapping patterns. But one can envisage these relations as having a communal character when they have some degree of stability and are built on mutual trust between the participants’ (at 50, emphasis in original).
1.4 CONCLUSIONS

The conventional picture of a state’s lawmaking authority is that it has comprehensive authority to make laws which regulate activities taking place within its geographical territory. It also has the authority to regulate activities taking place outside its territory, but which have effects within the territory. Because states are sovereign, there are no limits on what these laws might require.

The rapid rise of activities in cyberspace has shown us that this picture is far too simplistic. State laws often have no practical authority for a cyberspace user, and we argue that there are circumstances in which they have no legitimate authority either.

Legitimacy does not arise from the mere fact that the state exists, but rather is conferred on the state by its legitimating community. This has the consequence that the state only has comprehensive authority over that legitimating community.

Further, the community over which a state law has at least some authority is larger than the population of its geographical territory. Each state has an extended community in cyberspace, and its laws have authority over the members of that community which is derived from their interactions with the state. The deciding question, which needs to be posed at the level of the individual rule of law rather than at the level of the state’s law system as a whole, is whether the cyberspace user has such a relationship with the state that it is legitimate for the state to assert the authority of that rule of law.