scripted

Volume 8, Issue 1, April 2011

SOFT LAW FOR THE INTERNET, LESSONS FROM INTERNATIONAL LAW

Andrew Power & Oisín Tobin[*]

Abstract

This article begins with the international legal environment and the differences between international law and domestic law. Although the state is still the central subject of international law, the sovereignty of the state has been under challenge since the latter part of the 20th century. Developments in international law have resulted in the opening of the legal system of the international community to entities beyond the state. The inclusion of non-state actors in a system of international governance may provide lessons for the governance of the international "virtual" environment. Much current thinking about Internet law is either of the "Grand Internet Treaty" variety, in which the online environment is a simple extension of the territory of a state, or sees the Internet as a libertarian "lawless" environment, unhindered by any restrictions. These views are examined and the nature of the law of the Internet considered in light of the lessons from international "soft" law.

DOI: 10.2966/scrip.080111.32

[*] Andrew Power is the Head of School of Creative Technologies at the Institute of Art, Design and Technology, Ireland and a Doctoral student of Governance at Queens University Belfast.

Oisín Tobin is a tutor and Ph.D. Candidate in the Law School in Trinity College Dublin.

1. International Law

The online legal environment is complicated by the many government, corporate, technical and user groups with a stake in the process. The creation or perhaps evolution of such an environment may be informed by the ways in which international law has learned to accommodate a "soft" rather than "hard" law approach it its own development. Hard law is defined as the rules and regulations that make up legal systems in the traditional sense, and soft law consists of those informal rules that are non-binding but, due to cultural norms or standards of conduct, have practical effect.[1] Senden defines it similarly, as:

> Rules of conduct that are laid down in instruments which have not been attributed legally binding force as such, but nevertheless may have certain (indirect) legal effects, and that are aimed at and may produce practical effects.[2]

The history of international law is generally considered to begin in the early 17th century with the Dutch lawyer, Grotius. Grotius published his legal masterpiece, "*De Jure Belli ac Pacis"* (On the Law of War and Peace) in 1625. He was motivated by the wars and turmoil in Europe, and particularly the Thirty Years War which had begun in 1618. He sought to minimise the bloodshed in war by constructing a general theory of law that would be secular, and therefore independent of different religious factions. It was to be a natural law, born out of mans own nature, of which he said:

> .... there is a common law among nations, which is valid alike for war and in war, I have had many and weighty reasons for undertaking to write upon this subject. Throughout the Christian world I observed a lack of restraint in relation to war, such as even barbarous nations should be ashamed of.[3]

In the time of Grotius, the state was the source and arbiter of power. The notion of law as the commands of the King backed by force seemed sufficient, and survived up to the time of Austin's work.[4] By the time Hart was writing his "Concept of Law", the world was a changed place, and the interdependence of states had been driven home to the politicians and peoples of Europe by a half century of world conflict.[5] Hart conceived of law as a set of rules: primary and secondary rules that provided a framework for the administration of justice, but also as a framework for state interaction. Hart felt that the lack of secondary rules in international law undermined its validity. When Dworkin moved the definition of law further from the embodiment of the state by construing it as interpretation, he put the law in the hands of the

---

[1] P Burgess (2002) "What's So European About the European Union?: Legitimacy Between Institution and Identity" (2002) 5 *European Journal of Social Theory*, at 467.

[2] L Senden, *Soft Law in European Community Law* (Portland: Hart Publishing, 2004).

[3] H Grotius, "*De Jure Belli ac Pacis"* (1625), Encyclopaedia Britannica, available at http://www.britannica.com/EBchecked/topic/246809/Hugo-Grotius (accessed 17 May 2009).

[4] J Austin, *The Province of Jurisprudence Determined* (New York: Prometheus Books, 2000; originally London, 1832).

[5] HLA Hart, *The Concept of Law* 2nd ed (Oxford: OUP, 1994).

judiciary. This provided for the governance of emerging non-state or supra-state law-making bodies.[6]

International law provides the foundation for statehood, including as it does principles such as sovereignty, recognition, territorial competence, non-intervention and so on. States have seen changes in the way they can exercise power. Power has moved to the sub-national and supranational level. Morison has spoken about this as the "hollowing out" of the state and discussed the "fugitive nature of power".[7] This has led to predictions of the end of the nation state[8] but, Pierson[9] argues that states are diversifying, and developing. At the supranational level powers have been seeded upwards to organisations like the European Union. Loughlin argues that the founders of the European project did not wish to abolish the nation state but to minimise its importance by building a supranational European system as a foundation for a future federal Europe.[10] States may not be losing sovereignty, but there is a sense in which there has been a pooling of sovereignty. Slaughter goes further, suggesting that we stop thinking about states and focus instead on governments, by which the elements of legislation, adjudication and implementation interact with each other across borders. As she goes on to say, "[s]tates still exist but they are disaggregated".[11]

Power has also been ceded to entities such as The United Nations (UN), the International Monetary Fund (IMF), the World Bank, and the World Trade Organisation (WTO). One might assume that a government would resist the transfer of power away from its national parliament, but it has been argued elsewhere that these movements of power have often occurred at the initiative of those who are in power, and against the wishes of those they represent.[12] According to Allain[13]

> The growth of internationalization qua globalization since the end of the Cold War, has meant that states have been willing to cooperate in new and expanding fields. This, in turn, has meant that increasingly states have moved to establish or reinvigorate inter-governmental institutions for the purpose of coordinated action. These institutions, to some extent, have escaped the scrutiny that ordinarily would be felt at the national level. With no true constituency to monitor their international activities and being one step removed from a general public to which they are accountable, states have sought and often achieved collectively what they could not accomplish individually.

---

[6] R Dworkin, *Law's Empire* (Oregon: Hart Publishing, 1986).

[7] J Morison, "The Case Against Constitutional Reform?" (1998) 25 *Journal of Law and Society*, at 517.

[8] K Ohmae, *The End of the Nation State: The Rise of Regional Economies* (New York: The Free Press, 1996).

[9] C Pierson, *The Modern State* (London: Routledge, 2004), at ch 8, 176.

[10] J Loughlin, "Reconfiguring the State: Trends in Territorial Governance in European States" (2007) 17 *Regional and Federal Studies*, at 387.

[11] AM Slaughter, *A New World Order* (Princeton: Princeton University Press, 2004), at 5.

[12] G Monbiot, George "Government in Exile: The Corporate Bid for World Domination" *Captive State: The Corporate Takeover of Britain* (London: Pan, 2001), at 305.

[13] J Allain, "The jus cogens Nature of non-refoulement" (2002) 13 *International Journal of Refugee Law*, at 541.

In the absence of the scrutiny described above, peer review among nations may result in the achievement of improved standards. Boswell reviewed the proposition that international standards strengthen accountability and improve the performance of governance structures.[14] He challenged not the creation of standards, but how they are applied in practice, and the view that peer review was the best way to ensure compliance. Governments must have the political will, the technical capacity, the resources, and there must be civil participation and oversight.

In considering a framework of law for the Internet, lessons may be taken from these writers on international law. They include: a move away from systems of command and control, the decreased autonomy of individual states, the increasing importance of including non-state actors, the improvement of governance through peer review, and the risk of loss of legitimacy as power moves further from the individual citizen. A further lesson is the danger of such a framework being perceived as an instrument of the West. Just as international law can be perceived in the Middle East, for example, "not as a shield but as a sword", so too the governance of the Internet, with its roots in the US, must avoid the trap of being seen as another colonial weapon of the West.[15] If such a perception takes hold, then developing systems of Internet law will be fraught with issues of legitimacy.

2. Hard and Soft Law

In an international context, hard law can provide a basis for enforcement by setting standards of acceptable behaviour, together with reputational and coercive consequences for breach. A system of centralised enforcement though the UNSC or IMF is also possible. Hard law can also be seen in situations where international commitments are incorporated into domestic law. When international laws are incorporated into domestic law they are generally no longer seen as international law, but just another form of domestic law, albeit with an international source. States may choose the hard law route when a) the benefits of cooperation are high and the cost of breach also high; b) when noncompliance may be difficult to detect; c) when states wish to form alliances such as the EU or NATO; d) when domestic agencies are given power to make agreements, with little control from the executive; and e) when a state is seeking to enhance its international credibility.[16] Hard law does however entail significant costs and can restrict the behaviour and sovereignty of nation states. The costs of hard, as opposed to soft, law involve the potential for inferior outcomes, loss of authority and reduction in sovereignty.

In the early days of the Internet, the instinct of governments was to solve the perceived problems of control through hard law. In the US, the Clinton administration tried on many occasions to pass laws to control online pornography. The Communications Decency Act (CDA) was followed by the Child Online

---

[14] N Boswell, "International Law Standards for Domestic Governance: The Impact of International Law on Domestic Governance" (2003) 133 *American Society of International Law Proceedings*, at 113.

[15] J Allain, (2004) "Orientalism and International Law: The Middle East as the Underclass of the International Legal Order" (2004) 17 *Leiden Journal of International Law*, at 392.

[16] K W Abbott, and D Snidal ,(2000) "Hard and Soft Law in International Governance" (2000) 54 *International Organization*, at 429.

Protection Act (COPA), which was followed by the Children's Internet Protection Act (CHIPA). All came into force as law, and all were challenged in the courts on the basis of freedom of speech issues.[17] CHIPA alone survived the challenges, but as it was limited to controlling usage in public libraries, and with libraries given the option to opt in or out, it is also effectively dead.[18] This led Boyle to assert:

> Federal judges had come a long way towards recognizing both the technological resistance of the Internet to censorship, and the fact that a global net could never be effectively regulated by a single national jurisdiction.[19]

Soft law reduces the cost associated with hard law by limiting one or more of the dimensions of obligation, precision or delegation. Escape clauses can be added, commitments can be imprecise, and future political change can be facilitated through delegation to sub-state bodies. Rather than undermining the law, these elements may be seen as permitting states to enter agreements without threat to sovereignty, allowing for future uncertainty, and lowering barriers to future, harder legalisation. In choosing solutions, states face a trade-off between hard and soft law, as each have advantages and disadvantages. Soft law can reduce the sovereignty cost by offering a range of institutional agreements from which states can choose. Soft law offers an effective way to deal with uncertainty, especially when it initiates processes that allow actors to learn about the impact of agreements over time. Uncertainty presents a major challenge for institutions of international governance and is considered below in the context of Cooney and Lang's writing on adaptive governance.[20]

Soft law offers techniques for compromise and cooperation between states and private actors. Non-state organisations will normally press for hard law solutions to raise the cost of violation by other parties, however soft law may be both more achievable, as private actors may lack the ability to enter binding treaties, and also more flexible to changing circumstances.

> States and non-state actors can achieve many of their goals through soft legalization that is more easily attained or even preferable..... Soft law is valuable on its own, not just as a stepping stone to hard law. Soft law provides a basis for efficient international "contracts," and it helps create normative "covenants" and discourses that can reshape international politics.[21]

States will often opt for a soft law solution if substantive agreements are impossible to attain. Soft law can provide opportunities for deliberation, systematic comparisons,

---

[17] *Reno v American Civil Liberties Union*, 521 U.S. 844 (1997); *Ashcroft v ACLU* (2004) (U.S. Supreme Court).

[18] *United States v American Library Association*, 539 U.S. 194 (2003).

[19] J Boyle "Foucault in cyberspace: surveillance, sovereignty, and hardwired censors" (1997) 66 *University of Cincinnati Law Review*, at 189.

[20] R Cooney and A Lang, "Taking Uncertainty Seriously: Adaptive Governance and International Trade" (2007) 18 *European Journal of International Law*, at 523.

[21] K W Abbott, and D Snidal, "Hard and Soft Law in International Governance" (2000) 54 *International Organization*, at 456.

and learning.[22] It may not commit a government to a policy, but it may achieve the desired result by moral persuasion and peer pressure. It may also allow a state to engage with an issue, in a way that would otherwise have been impossible for domestic reasons, and open the possibility for more substantive agreements in the future.

3. Opposing ideas about Internet law

In thinking about the regulation of the Internet some argue that rules for online activities need to come from territorial states.[23] One governance option is a centralised system of control, involving coordination amongst the existing sovereign powers and some form of multi-lateral agreement or "Grand Internet Treaty". The structure of international society is anarchic, however, in the sense that there is no world government to enforce international legal norms.[24] Or as Slaughter has said: "world government is both infeasible and undesirable. We need more government on a global and a regional scale, but we don't want the centralization of decision making power and coercive authority so far from the people actually governed."[25] It may also be said that the kind of norms likely to exist in such a treaty would be contrary to much of the liberal ethos of the Internet that has shaped its formation to date. Benkler sees the Internet as a democratising force, describing it as a "networked public sphere". He suggests that it changes the way in which individuals interact with their democracy and experience their role as citizens:[26]

> The network allows all citizens to change their relationship to the public sphere. They no longer need to be consumers and passive spectators. They can become creators and primary subjects. It is in this sense that the Internet democratizes.

Others argue for considering cyberspace as a different place, in which new rules can and should be made.[27] The argument is that in the offline world there is generally a correlation between the boundaries drawn in physical space and those in legal space. The point at which one set of laws stops and another starts is normally the physical border of a country. This physical-legal correlation has four dimensions for consideration. Firstly, legal authority, the *power* to control a space, gives national governments the ability to enforce the law and impose sanctions. Second, the legal *effect* of a law is related to the proximity of the law-maker and those affected. Thirdly, the *legitimacy* of the law is the degree to which it is implemented with the consent of the governed. Finally, physical proximity permits the delivery of *notice* or warning, to encourage those affected to abide by a given law. The advent of the

---

[22] A Schäfer, "Resolving Deadlock: Why International Organisations Introduce Soft Law" (2006) 12 *European Law Journal*, 194 – 208.

[23] JL Goldsmith, "Against Cyberanarchy" (1998) 65:4 *University of Chicago Law Review*, at 1199.

[24] R Eckersley, "Soft law, hard politics, and the Climate Change Treaty" in Christian Reus-Smit (ed), *The Politics of International Law* (Cambridge: Cambridge University Press, 2007) at 81.

[25] AM Slaughter, *A New World Order* (Princeton University Press, 2004) at 8.

[26] Y Benkler, *The Wealth of Networks*, (New Haven and London: Yale University Press, 2006) at 272.

[27] D Johnson and D Post, "Law and Borders – The Rise of Law in Cyberspace" (1997) 48:5 *The Stanford Law Review* 1367 – 1402.

Internet has broken the link between geography and these four principles. The advent of virtual machines, where servers can exist as software rather than hardware, makes the notion of tracking online activity to a physical location a meaningless concept.[28] An individual does not know where other individuals, services or institutions might be located or what rules, if any, apply.

Taken to an extreme, one view might be that no law should apply to the Internet. In 1996, for example, in reaction to the Communications Decency Act in the US, John Perry Barlow, a Fellow at Harvard University's Berkman Center for Internet and Society, published "A Declaration of the Independence of Cyberspace" calling upon "Governments of the Industrial World.....I ask you …to leave us alone. You are not welcome among us. You have no sovereignty where we gather".[29]

This view seems to originate in the idea that there should be no regulation of the press because it is an affront to free speech. The print and broadcast media, however, all benefit from government regulation. Legally conferred property rights, in the form of monopolies over frequencies, are protected at taxpayers' expense through civil and criminal law, in order to prevent people from gaining access to what broadcasters "own". The US Government funded the creation of the Internet, and the European Government that funded the CERN research in Geneva that resulted in the World Wide Web. As Sunstein states:

> the real question is what kind of regulation to have, not whether to have regulation. Even those who create open-source software rely heavily on property law, contract law (through licenses) and at least some form of copyright law to control what happens to their software.[30]

4. The Nature of Online Crime

Before exploring the contribution that a soft law approach might make to online law, it is necessary to consider whether the problems that require resolution are different from those encountered offline. The Internet provides a new medium in which technology and crime interact. Online crime can be divided into three categories. The first is crimes that exist offline, but are greatly facilitated by the Internet. These include misuse of credit cards, information theft, defamation, blackmail, obscenity, hate sites, hate speech, money laundering, and copyright infringement. States have tried to use existing laws to combat these crimes, but rulings against the person in this area seem to be limited to lesser charges of harassment.[31] The first online libel action in the UK, however, arising when a councillor used Twitter to make libellous claims

---

[28] C Arthur and A Brown, How to turn one computer into many, The Guardian, Thursday 8 November 2007, available at http://www.guardian.co.uk/technology/2007/nov/08/news.software (accessed 28 March 2001).

[29] CR Sunstein, *Republic.com 2.0* (Princeton: Princeton University Press, 2007), at 153.

[30] *Ibid*, at 160.

[31] *People of the State of New York v Alan Munn*, 179 Misc 2d 903 (Criminal Crt, City of NY, February 9, 1999); *Kathleen Smith v Alan Smith*, 24 AD 3d 822, 804 NYS 2d 854 (3rd Dept, 2005).

about a political rival, resulted in a payment of £3,000 in damages and £50,000 in costs.[32]

Secondly, the Internet introduces crimes that did not exist before, including hacking, spamming[33], cyber vandalism, dissemination of viruses, denial of service attacks, and domain name hijacking. In many jurisdictions, national laws were introduced in an attempt to combat these crimes[34]. The move to Web 2.0 has changed the nature of online activities from communications to social engagement, which has in turn led to the growth of a third category of crime: crimes against the person or the online public. Some crimes against online personas have existed for some time, but the capabilities of applications developed for Web 2.0 have seen significant growth in this area. Crime against an online persona presents the most difficulty to law makers and deserves some further explanation.

Technology is becoming cheaper, more intuitive and more prevalent, and the barriers to entry are falling. More people are spending time in social networks and acting out through online avatars[35] or alternate personas. Targeting another individual through their online representation may be criminal or antisocial or may lead to crimes offline. Theft of online virtual goods has lead to serious crime offline. In June 2005, the theft of a virtual sword in the online game "Legend of Mir 3" led to an offline murder when the police refused to take it seriously.[36] In 2008, fights between Russian gang members resulted from a virtual assault in an online role playing game.[37] In 2007, a Dutch teenager was arrested for stealing virtual furniture from "rooms" in "Habbo Hotel", a 3D social networking website; this virtual furniture was valued at €4,000.[38] Activities such as online assault and rape have very real effects, with reports of resulting depression and suicide.[39]

Much of this activity can be attributed to a change in our understanding of identity. Jurisprudence in the area of identity theft indicates that many of the same principles that apply to offline apply to the online crime.[40] What is different in online or virtual

---

[32] C Baksi, "Damages awarded in the first UK twitter libel action", *Law Society Gazette*, available at http://www.lawgazette.co.uk/news/courts-news/damages-awarded-first-uk-twitter-libel-action (accessed 28 Mar 2011).

[33] *America Online v LCGM*, Inc, et al, 46 F Supp 2d 444, Civ Act No 98-102-A, (ED Va, November 10, 1998).

[34] For a good overview of the UK law in this area see "Legal Guidance for ICT Use in Education, Research and External Engagement", *JISC Legal*, available at http://www.jisclegal.ac.uk (accessed 28 March 2011).

[35] The Sanskrit word "avatara" means incarnation. In computing an avatar is a representation of the user in the form of a three-dimensional model.

[36] "Chinese gamer sentenced to life", *BBC News Channel*, available at http://news.bbc.co.uk/1/hi/technology/4072704.stm (accessed 29 March 2011).

[37] F Truta, "Russia - Gamer Kills Gamer over Gamer Killing Gamer…Er, in-Game!", *Softpedia*, available at http://news.softpedia.com/news/Russia-Gamer-Kills-Gamer-over-Gamer-Killing-Gamer-Er-In-Game-76619.shtml (accessed 28 March 2011).

[38] "'Virtual Theft' Leads to Arrest, *BBC News Channel*, 14 November 2007, available at http://news.bbc.co.uk/2/hi/technology/7094764.stm (accessed 28 March 2011).

[39] G Kirwan, "Presence and the Victims of Crime in Online Virtual Worlds" in *Proceedings of Presence 2009*, 12th Annual International Workshop on Presence. Los Angeles, 11-13 November.

[40] *Joel Ruiz v Gap Inc et al*, Case No 07-5739 SC (ND Ca, 24 March, 2008).

environments it that users are able to distance themselves from their own identities, and as a result change their behaviour and attitudes. Early studies of computer mediated communication in the 1980s suggested that email removed the social context clues such as gender, age, race, social status, and facial expression, which had a disinhibiting effect upon participants.[41] Three dimensional virtual environments in which participants can represent themselves as avatars provide an opportunity to not only hide social context clues, but to create alternate ones. As a result, users can explore elements of their personality in the absence of a sense of responsibility for their actions. The objectification of the "characters" of a game, who may be another player or just software, has the potential to undermine the inhibitions of an individual.

From this brief review, it is clear that the nature of online crime presents some of the challenges of offline crime but also some new ones. Online crime is more anonymous, more impersonal and more detached. There can be a sense of diminished responsibility towards a community and less accountability for one's actions. At the very least there is a reimagining of the meaning of community. Traditional law struggles to deal with these issues, as it can be hard to identify any crime that has been committed. While it can be argued that many of these acts break Terms of Service (which usually stipulate that users do not engage in anti-social behaviour) this is generally a contractual, rather than criminal matter. In the case of cyber-bullying there has been some attempt to turn a breach of contract into a criminal conviction, but this was held to be unconstitutional on grounds that it allowed criminal law to be delineated by a civil contract.[42]

5. A framework for online law

A legal framework for the Internet needs to take into account the nature of the activities taking place and the individuals and organisations using it. The legitimacy and appropriateness of hard and soft laws will depend in part on the context or society in which they are used. In relation to online social networks, soft laws may be more effective than hard laws, as a result of their power and potential for support. The combination of states, individuals, businesses, and other non-state actors that make up the legal, regulatory and technical web of behaviours that constitute the Internet make it somewhat unique.

Morison wrote in 1998 that "Government now is only one of many actors that may influence the course of events in society".[43] Rose went further in 1999 stating that:

> The state now appears simply as one element – whose functionality is historically specific and contextually variable – in multiple circuits of power, connecting a diversity of authorities and forces, within a whole variety of complex assemblages.[44]

---

[41] M Williams, "Avatar watching: participant observation in graphical online environments" (2007) 7:1 *Qualitative Research*, 5 – 24.

[42] B Stelter, "Guilty Verdict in Cyberbullying Case Provokes Many Questions Over Online Identity", *The New York Times*, 27 November 2008, available at http://www.nytimes.com/2008/11/28/us/28Internet.html?ex=1385614800&en=660f9239fe3c6450&ei=5124 (accessed 28 March 2011).

[43] J Morison, 'The Case Against Constitutional Reform?' (1998) 25 *Journal of Law and Society*, at 518.

[44] N Rose, *Powers of Freedom* (Cambridge: Cambridge University Press, 1999) at 5.

Ten years on, reviewing the growth in data available to all online users, Morison was still of the view that:

> the Web 2.0 phenomenon combined with the power of information approach has potentially dispersed this governing resource much more widely. While it may remain the most powerful, government is still only one of a range of actors able to develop this information.[45]

Considering the many players and the fluid nature of the development of the Internet, Cooney and Lang describe the need to develop flexible and adaptive international institutions, to respond to rapidly changing global conditions, as well as to changes in our knowledge of the causes of global problems.[46] They also describe the recent development of learning-centred alternatives to traditional command-and-control regulatory frameworks, variously described as "experimentalist" governance, "reflexive" governance, or "new" governance. Elements of these approaches contribute to what Cooney and Lang call adaptive governance.

The key elements of this adaptive governance are first its focus on facilitating continuous learning as a response to uncertainty and systemic unpredictability, redefining the problem and revisiting the question as to what constitutes relevant "knowledge" about a particular problem. Secondly, adaptive governance sees policy-making as experimentation. It is a process of "learning by doing", and treating policy interventions as quasi-experiments. Finally adaptive governance is an iterative process of review and revision. Monitoring and feedback mechanisms help facilitate learning, not only by fine tuning the particular policy instruments chosen, but also by drawing attention to relevant knowledge gaps. Policy-making is less about the attainment of a single optimal solution and more about providing a forum for the on-going creation of consensual knowledge and agreed processes to guide policy.

> Adaptive governance accepts and responds to uncertainty through promoting learning, avoiding irreversible interventions and impacts, encouraging constant monitoring of outcomes, facilitating broad participation in policy-making processes, encouraging transparency, and reflexively highlighting the limitations of the knowledge on which policy choices are based.[47]

In common with the thinking about soft law demonstrated above, adaptive governance allows for a broader participation in the formulation of policy and law than hard law would permit. Secondly, it allows for an iterative or progressive approach to policy-making and law-making. The solution, which needs to come from state, citizen, and corporation, will develop over time as knowledge, systems, and technologies develop.

> The identities and interests of States can be shaped by both domestic and transnational discursive practices, and NGOs are increasingly significant

---

[45] J Morison, "Gov 2.0: Towards a User Generated State?" (2010) 73:4 *The Modern Law Review*, at 563.

[46] R Cooney and A Lang, "Taking Uncertainty Seriously: Adaptive Governance and International Trade" (2007) 18 *European Journal of International Law*.

[47] *Ibid*, at 1.

> to any understanding of the discursive processes and legitimacy of multilateral agreements.[48]

Examples of soft law in the area of cyberlaw include the Council of Europe's Convention on Cybercrime[49] and the US National Strategy to Secure Cyberspace.[50] The European Convention was created to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation." It deals particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. The countries of the European Union have, under various political, economic and regulatory frameworks, developed many methodologies for working together. What Slaughter describes as the "vibrant laboratory" of the European Union provides many lessons on how to establish the necessary degree of collective cooperation amongst a diverse group of states and yet maintain the locus of political power at national level.[51] America's national strategy is part of the greater "Homeland Security" project that focuses on prevention of terrorist attack. This combines soft law and some very hard law that permits the Department of Homeland Security to issue directives for implementation by Internet providers.[52] The UN General Assembly initiated a World Summit on the Information Society (WSIS) to offer a further platform for the development of principles and guidelines. The first phase took place in Geneva in 2003 and the second in Tunis in 2005.[53]

Perhaps the main application of a soft law approach can be found in the technical standards that underpin the Net. Such standards are set out in the requests for comments (RFCs) run by the Internet Engineering Task Force (IETF), but having emerged informally through discussions between various parties, were never turned into hard law by statutory definition.[54] This is quite a peculiar situation, given that nearly every other product or technology is presently defined in the law by formal regulation.

---

[48] R Eckersley, "Soft law, hard politics, and the Climate Change Treaty" in Christian Reus-Smit (ed), *The Politics of International Law* (Cambridge: Cambridge University Press, 2007), at 105.

[49] Council of Europe, "Convention on Cybercrime", *CETS No: 185*, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (accessed 28 March 2011).

[50] Office of the Whitehouse, *U.S. National Strategy to Secure Cyberspace*, available at http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed 28 March 2011).

[51] AM Slaughter, *A New World Order* (Princeton: Princeton University Press, 2004) at 264.

[52] L Phillips, "House Leaders Announce Support for Lieberman, Collins, Carper Cybersecurity Bill", *Senate Committee on Homeland Security and Governmental Affairs*, available at http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=42e2542c-5056-8059-7604-87cb5518d790 (accessed 28 March 2011).

[53] See the website of the World Summit on the Information Society (WSIS), available at http://www.itu.int/wsis/index.html (accessed 28 March 2011).

[54] See the website of the Internet Engineering Taskforce, available at http://www.ietf.org (accessed 28 March 2011).

These ideas of soft law and adaptive governance offer further lessons for the framing of a legal structure for the Internet. These include: systems of informal rules which may not be binding but have effect through a shared understanding of their benefits; adaptable law that is flexible and open to change with the development of knowledge; agreements that include both states and non-state actors, and involve both the citizen and business. Finally, soft law offers lessons on continuous learning in a changing environment, resulting in an evolving system of laws.

By decentralising law-making and permitting a new framework of laws to emerge, online service providers are able to develop their own systems of governance and standards of behaviour. Law may develop from the bottom up, as users select the services, products and environment that match their own ethical and behavioural standards. In this scenario, our understanding of justice may change as we see what emerges from un-coerced individual choice.[55] MacSíthigh argues that the increased availability of user-generated content is influencing the development of cyberlaw.[56] As individuals and businesses develop more content, services and applications, the ability of the state to provide timely and appropriate legislation, or even guidelines, is limited. He lists several examples of self-regulation and co-regulation of activities online. For example a joint government/industry group like the Broadband Strategy Group in the UK has established guidelines for British media producers. In other cases, governments have drafted codes of behaviour for industry groups that are observed on a voluntary basis.[57] Notably, one of the drawbacks of self-regulation is that users often lack either the knowledge or concern to make a properly informed choice as to the rules underpinning the service they are selecting. It is also true to say that many of the self-regulating policies developed by industry are designed to favour their own interests.

An approach suggested by Cannataci and Mifsud-Bonnici is that "there is developing a mesh of private and State rules and remedies which are independent and complementary".[58] This language is echoed by Eckersley who talks of the "mutual enmeshment" of law and politics and the "constitutive tensions" between the regulative ideals of treaty law and the actual production of treaty law.[59] In terms of the law as experienced by the users of the Internet community, rules and remedies are often adopted on the basis of their "fitness for purpose". State regulation may be appropriate for the control of certain activities, technical standards in other situations, and private regulation where access to national courts or processes is impossible.[60] Private regulation will only be most effective if it does not require enforcement through the national courts. Technical or architectural enforcement would be more effective.

---

[55] D Post, "Governing Cyberspace" (1996) 43:1 *The Wayne Law Review* 155 – 171.

[56] D MacSíthigh, "The mass age of Internet law" (2008) 17:2 *Information & Communication Technology Law* 79 – 94.

[57] *Ibid*, at 86.

[58] J Cannataci and JP Mifsud-Bonnici, "Weaving the Mesh: Finding Remedies in Cyberspace" (2007) 21:1 *International Review of Law, Computers & Technology*, at 60.

[59] R Eckersley, "Soft law, hard politics, and the Climate Change Treaty" in Christian Reus-Smit (ed), *The Politics of International Law* (Cambridge: Cambridge University Press, 2007), at 81.

[60] A Power, "The Online Public or Cybercitizen" (2010) 7:1 *Script-ed* at 185 – 195.

Technical control may be exercised by the state, but is often in the hands of the commercial organisations that design and develop the technologies we use. Software engineers will determine certain aspects of what can and cannot be done, or even what may be considered right or wrong. They will find ways to prevent file sharing, or illegal downloading, or other aspects of our online activities. Blocking or filtering software has largely removed the need for states to struggle, as they did in the late 1990s, with issues of censorship. If individuals can control the flow of information to their (or their child's) computer it is less imperative that the state should eliminate it from the web. The challenge for these "technical governors" of behaviour is to recognise the full potential of their role. Will managers "utilize ICT to support, and reinforce existing political, social and organizational structures and processes or will they use ICT as a transformational agent to access its full potential?"[61] This is an important question, as the choices that are made will often be made by technologists and designers rather than public representatives or the judiciary. These are normative choices with far-reaching impacts. For example, the design of Facebook made certain normative assumptions about privacy which may be consistent with the thinking of young, liberal, Californian IT professionals but may not align with other sections of society. In fact, social networking technologies illustrate how we have learned to describe ourselves and our relationships in ways that fit the preordained limitations of the software interface, and established new meanings for words such as friends or relationship status or interests.[62]

Private regulations exist in the realm of codes of behaviour agreed amongst groups of users or laid down by commercial organisations that provide a service or social networking environment. One method of establishing standards of behaviour is through online dispute resolution. The growth of ODR was "not intended to challenge or displace an existing legal regime but to fill a vacuum where the authority of law was absent".[63] A mix of state and private regulation is both inevitable and necessary to provide real-time solutions to millions of online customers and consumers. This should lead to greater collaboration between private groups and states in the development and administration of rules. An example of this is the World Intellectual Property Organization (WIPO), a specialised agency of the United Nations. It is dedicated to developing a balanced and accessible international intellectual property system. One of its functions is the domain name dispute resolution process which provides an inexpensive way of dealing with cyber-squatting, and bypasses the cumbersome use of national law. The case goes to arbitration on the basis of certain rules determining the right to a domain name, and if the arbitrator rules that cyber-squatting is taking place an order is issued to the relevant domain name registrar who simply re-assigns the domain name. This is a good example of a new regime emerging to address a vacuum in national law.

The technical component of the regulatory mix is as important as the private/public components. As Boyle colourfully puts it,

---

[61] S Zuboff, *In the age of the smart machine: The future of work and power* (New York: Basic Books, 1988).

[62] J Lanier, *You are not a Gadget*, (London: Penguin, 2011) at 52.

[63] E Katsh, "Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace" (2007) 21:2 *International Review of Law, Computers & Technology*, at 99.

> ...information wants to be free and the thick fingers of Laviathan are too clumsy to hold it back, [but] the position is less clear if the information is guarded by digital fences backed by state power maintained through private systems of surveillance and control.[64]

This kind of thinking is not unique to governance of the Internet. Other areas of the law require cross-border, multi-state and non-state involvement. Morison cites environmental law as a field in which an international approach is required and one enabled by technology:

> Acid rain and river pollution means that preventing pollution in one country may require action in another. Since television and radio signals can cross frontiers, regulatory action which stays within one set of boundaries is likely to prove of limited effectiveness.[65]

Writing in 1995, Morison could see the impact of television and radio signals crossing borders. The arrival of the Internet has only served to increase this issue. Eckersley (2007) also uses the environment as an example of a policy area in which states have risked loss of individual sovereignty to achieve a greater objective.[66]

> Any serious and concerted effort to reduce greenhouse gas emissions necessarily entails measures that strike at the heart of the domestic policies of states, including energy, industry, transport, infrastructure development, taxation, and pricing policy. For many states, any attempt to regulate such "domestic" matters is tantamount to an infringement of their sovereignty. Nonetheless, against these enormous odds, a principled agreement to reduce greenhouse gas emissions has been reached by a majority of states.

Other areas in the international arena in which a soft law approach has worked include forestry, labour rights and sustainable development.[67] Sindico describes soft law as a "pioneer" of hard law, and voluntary standards in particular as a stage in the creation of legal norms. They are necessitated by the challenge of sustainable global governance. However in the case of the law of the Internet, it is unclear whether soft law can be seen as a route to hard law. The prevalence of non-state actors in the creation and management of the virtual space, and the uniquely strong position of technical standards and rules in the governing of that space, make the route to a hard law solution nonlinear at best and, at worst, opaque.

---

[64] J Boyle (1997) "Foucault in cyberspace: surveillance, sovereignty, and hardwired censors" (1997) 66 *University of Cincinnati Law Review,* at 201.

[65] J Morison and S Livingstone, *Reshaping Public Power* (London: Sweet & Maxwell, 1995), at 180.

[66] R Eckersley, "Soft law, hard politics, and the Climate Change Treaty" in Christian Reus-Smit (ed), The Politics of International Law (Cambridge: Cambridge University Press, 2007), at 82.

[67] F Sindico, "Soft Law and the Elusive Quest for Sustainable Global Governance" (2006) 19 *Leiden Journal of International Law,* 829 – 846.

6. Conclusion

With the advent of Web 2.0 and the growth of social networking and online environments, we are having to learn how to recognise the concept of the cybercitizen in the law. The intertwining of state, private, and technical solutions is likely to continue to develop as a de-facto model of Internet governance. The likelihood of some "Grand Internet Treaty" being agreed between states seems less and less likely as we seek to come to grips with what Willcocks describes as "understanding control in liquid modernity".[68] The experience gained by states in the development of soft law solutions to issues of international law provides a path towards solving issues of governance related to the Internet. The working definition of Internet governance adopted at the World Summit on the Information Society in Tunis in 2005 is:

> Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures and programmes that shape the evolution and utilization of the Internet.[69]

The idea that behaviour will be governed by a mix of national laws, user-defined principles, technical requirements and corporate guidelines seems to be the *de facto* position. How this type of regulation is to be consistently enforced in the online world will only be determined over time.

---

[68] LP Willcocks, "Michel Foucault in the Social Study of ICTs, Critique and Reappraisal" (2006) 24:3 *Social Science Computer Review,* 274 – 295.

[69] World Summit on the Information Society, *Report of the Working Group on Internet Governance*, June 2005, available at http://www.wgig.org/docs/WGIGREPORT.doc (accessed 28 March 20011).