The Political Economy of the Internet and E-Commerce.

Draft book chapter by Henry Farrell

How have new information technologies affected international political economy? In the heady years of the dot com bubble, many academics and commentators predicted that the Internet and e-commerce would empower private actors and weaken states. Indeed, some libertarians hoped that the Internet would lead to a collapse in state authority. However, these predictions have not come to pass. Although private actors have come to play an important role in some areas of Internet and e-commerce regulation, they have hardly come to predominate. In many instances indeed, private actors only play an important role because states have pushed them into doing it.

In this chapter, I examine the changing relationship between states and private actors in the governance of the Internet and e-commerce. This is an important test-case for more general international relations theories about how states and private actors interact with each other. International relations scholars are increasingly interested in how private actors are creating their own "islands of transnational governance," in which they may direct their own affairs, without much regard to international or national law.[1] Initially, it appeared that the Internet and e-commerce would be governed primarily by private authority, with states playing only a peripheral role.[2] However, despite the efforts of private actors to create their own independent governance regimes (and of prominent states such as the US to encourage them in their efforts), this has not transpired. Indeed, private actors, far from displacing states as sources of authority, are increasingly

[1] Stone-Sweet, Alec, 'Islands of Transnational Governance', in Christopher Ansell and Giuseppe di Palma, eds, *On Restructuring Territoriality* (Cambridge: Cambridge University Press 2004).

[2] For examples, see Johnson, David R., and David Post, 'Law and Borders: The Rise of Law in Cyberspace', *Stanford Law Review* 48 (1996): 1367-76; Simon, Leslie David, *NetPolicy.Com: Public Agenda for a Digital World*. (Washington DC: The Woodrow Wilson Center Press 2000); Spar, Debora L. 1999, 'Lost in (Cyber)space: The Private Rules of Online Commerce', in A. Claire Cutler, Virginia Haufler, and Tony Porter eds., *Private Authority and International Affairs* (Albany: SUNY Press 1999), although for an account with important revisions, see Spar, Debora L., *Ruling the Waves* (New York: Harcourt and Brace 2001).

becoming vectors of state influence. States are using private actors to achieve their regulatory goals, sometimes in cooperation with other states, sometimes in conflict with them.

I begin the chapter with a brief discussion of how the Internet works. Next, I discuss the early debates about e-commerce and the Internet. I then go on to examine how these debates led to policies (especially in the US, which had a crucial influence on early regulatory debates) that favoured self-regulatory solutions. I show how these policies have proved, in the long run, to be unsustainable. I conclude by examining how the changes in state-private actor relations that I document affect international regulatory outcomes.

The Nature of the Internet

What precisely is the Internet? The answer to this question is by no means as easy as it seems at first glance. Definitions of the Internet vary from Milton Mueller's succinct definition of the Internet as effectively identical with the TCP/IP protocol, through Lawrence Lessig's distinction between three different layers of the Internet, to Lawrence Solum and Minn Chung's invocation of no less than six different layers of Internet architecture. In this chapter, I simplify Solum and Chung's account, distinguishing between (1) the physical infrastructure of the Internet, (2) the TCP/IP protocol and domain name system (DNS), and (3) the various applications that run on top of the TCP/IP protocol and DNS.

First is the physical infrastructure of the Internet. It is easy to forget that the Internet requires a physical basis if it is to work at all – there is a complicated material infrastructure that intervenes between the source of a piece of information (for example, a web page at www.amazon.com), and its destination (someone trying to download Amazon's web page on her home computer). Information will be carried across cables and/or other communications links (satellite links, wireless links) on its journey from source to destination. In this journey, it will be passed along between different routers (specialized computers for data transfer). The physical infrastructure of the Internet has important political consequences. Those parts of the world in which the physical infrastructure is underdeveloped, or is difficult for citizens to access (because of decisions made by the government, or perhaps other actors) will not experience the same opportunities – or vexing political issues – as regions or countries where the Internet is easily accessible. Second, it may be possible for providers of physical infrastructure (such as cable operators in many advanced industrialized democracies) to limit their subscribers' access to certain kinds of content. This may be at the behest of government, or may alternatively be driven by the providers' own economic interests. For example, one may easily imagine cable operators trying in the future to limit their customers' access to pirated movies which cut into their own profits, or perhaps even limiting access to services provided by their competitors.

Second is the TCP/IP protocol, which is the cornerstone of the Internet. A protocol is a set of technical specifications that permits communication between different systems. The TCP/IP protocol is the basis for 'packet switching' – the fundamental basis for all Internet communications. The two elements of the protocol, TCP and IP, play different roles. TCP disassembles a coherent item of information (such as a web page, or an email) into a series of discrete 'packets,' each of which contains some of the original information, as well as a header, which contains key information about the packet's origin, destination, and contents. Once TCP has disassembled the information into a number of packets, IP allows the information to be routed through the network. When the packets are sent out onto the Internet, IP allows routers to try to figure out the best way to get each data packet to its destination, one step at a time, moving the packet from router to router until it reaches its final destination. Routers do this by examining the IP address (a unique numerical address with up to twelve digits in its current form) for the destination computer, and then consulting tables which tell them which router in their neighborhood is likely to be 'closest' to the final destination. Each packet may travel a separate route from the originating computer to the destination computer, which then uses the TCP protocol to reassemble the packets into a whole again. If blockages prevent some packets from reaching their destination, the originating computer may resend them through alternative routes.

As stated, the TCP/IP protocol uses numerical IP addresses (such as 128.57.224.53) in order to move packets from their origin to their destination. This system, while technically efficient, is hardly very user friendly – human beings have difficulty in remembering long numbers. Thus, in addition to the TCP/IP protocol, there is a secondary system for translating IP addresses into more human-friendly domain names, such as www.amazon.com. There is a master file (the so-called 'root' file) of the domain names that should be associated with various IP addresses, which is maintained under the Internet Corporation for Assigned Names and Numbers (ICANN), and propagated through various specialized computers (domain name servers). Thus, each time an Internet user requests a web page from www.boingboing.net, or sends an email to an address at oxford.ac.uk, a name server will translate the name (oxford.ac.uk) into a numerical IP address, so that the information can be expeditiously routed across the Internet.

While the details of this system are rather technical, they have important political consequences. First, the TCP/IP protocol is *content neutral*. It does not distinguish between different kinds of information, nor does it try to prioritize the delivery of certain kinds of information over others. Second, the TCP/IP protocol greatly facilitates *distributed communication*. Internet communication is not centralized – there is no central server through which all information flows. This allows the system to adapt quickly to breakdowns in communication. If, for example, a major router stops working, other routers will quickly begin to send their information through alternative routes. Third, the existence of the domain name system and a root file does allow for some degree of centralized power over the Internet. As long as most people use domain names rather than IP addresses to send and receive information, the organization in control of the root file will have considerable power over everyday users' access to the Internet.

Third, there are the various applications that run on top of the TCP/IP protocol. At the most basic level these include email, the File Transfer Protocol (which allows files to be sent to or received by remote computers), the Hyper Text Transfer Protocol (HTTP), which allows for the transmission of web-pages, and Telnet and SSL, which allow remote access to computers. There are also a host of other services and applications that invoke the Internet, as well as specialized software packages (web browsers, email clients) that allow users to view web pages and send and receive email without having to struggle themselves with technical protocols. Indeed, very few users have direct contact with the basic protocols of the Internet, instead, they use software and applications that effectively shield them from the (rather complex) technical underpinnings that permit communication. This has important political consequences that I will develop in the course of the chapter.

Early debates on Internet policy

The Internet is not a new phenomenon – its ancestor network, ARPANET, was created to foster academic and military research collaboration in the late 1960s, and the first version of the TCP/IP protocol was described in 1974.[3] However, it was not until the mid-1990's that the Internet began to broaden its appeal beyond the research community, and attract serious political attention. The development of the World Wide Web (WWW) played a key role in popularizing the Internet and e-commerce.

When the Internet became a mass phenomenon, controversies arose as to how or whether it should be regulated. Even though the Internet's development had been funded by the US government, it was actually run by an ad-hoc process of consensual decision-making among its users. The original universe of Internet users was both small and technically sophisticated – the relevant individuals could discuss standards and necessary changes to them through email (one of the first major Internet applications), the Internet Engineering Task Force (IETF) and other forums. Even if arguments were sometimes hard-fought, there was sufficient *ex post* consensus that the Internet could function without hierarchical guidance. Many believed that IETF-style processes could be

[3] See Hafner, Katie and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Touchstone 1998) for a good history of the Internet.

extended to new areas of Internet governance as necessary, so that there was little need for direct government regulation.

Furthermore, the Internet seemed to be directly relevant to two major debates on the governance of 'cyberspace.'[4] First, there was an intra-US dispute over the proper scope of government authority in cyberspace. Prior to the popularization of the Internet, US law enforcement authorities had gone to counter-productive extremes in their efforts to stamp out certain forms of computer use (hacking, software piracy).[5] This provoked a backlash from many prominent computer users, and the creation of an organization, the Electronic Frontiers Foundation (EFF), which sought to defend individual freedom in the sphere of electronic communication. While the EFF represented a variety of political viewpoints, the libertarians in its ranks were especially vociferous – they perceived government efforts to regulate cyberspace as a fundamental assault on free speech and other liberties. This characterization of politics was to have substantial consequences for Internet policy, both within the US and abroad.

Second was a disagreement between the US and other OECD countries over proposed international instruments to regulate electronic communications. As multi-national corporations began to engage in early forms of e-commerce and information exchange, some OECD countries worried that 'trans-border data flows' would undermine their citizens' privacy and other human rights. They proposed binding international agreements as a solution, but met strong opposition from the US, which was guided by

[4] The term, which has its origins in William Gibson's science fiction novel *Neuromancer*, has come to serve as a catch-all for the social environment created by the Internet and e-commerce.

[5] See Bruce Sterling's *The Hacker Crackdown*, available at http://www.eff.org/Misc/Publications/Bruce_Sterling/Hacker_Crackdown/Hacker_Crackdown_HTML/ (checked April 15, 2004).

the interests of its large firms.[6] This led to a stalemate, in which many OECD countries wished to create strong and comprehensive international instruments, but found it difficult to do so without US agreement. They were forced either to reach agreement on new institutions among themselves, accepting that the US would opt out (and thus perhaps undercut the effectiveness of the institution in question), or negotiate non-binding agreements (such as the OECD Privacy Guidelines) which had little substantive force.

The Internet affected both of these disputes in important ways. First, it initially seemed to provide a technology that would, by its very nature, protect individual liberty against government intrusion. Because the TCP/IP protocol was designed to allow communication to flow around blockages in the network, many believed that it was effectively invulnerable to censorship. In John Gilmore's famous formulation, "the Net interprets censorship as damage, and routes around it."[7] This led libertarians to hope that the Internet would be impossible for governments to control.[8] Some even anticipated that the combination of the Internet, and the use of powerful cryptographic techniques ('public key' encryption) to conceal information, might undermine the power of states to tax their citizens (who could hide their money beyond the reach of the state) and thus reshape national and international politics.

These libertarians found allies in the burgeoning e-commerce sector, which in turn was able to influence the US administration towards an emphasis on self-regulation.

[6] Drake, William J., 'Territoriality and Intangibility: Transborder Data Flows and National Sovereignty', in Kaarle Nordenstreng and Herbert I. Schiller, eds., *Beyond National Sovereignty: International Communications in the 1990s* (Norwood: Ablex 1993).

[7] The precise moment at which Gilmore came up with this pithy formulation of libertarian ideas about the Internet is uncertain.

[8] See Barlow, John Perry, *A Declaration of the Independence of Cyberspace* (1996). Available at http://www.eff.org/~barlow/Declaration-Final.html (checked 5 March 2002).

E-commerce firms were strongly opposed to government regulation – they argued that it was likely to strangle an economic sector that was in the throes of rapid change. They found a ready audience in Ira Magaziner, the Clinton administration's e-commerce 'czar,' who indeed drafted industry figures to write large portions of the administration's e-commerce and Internet policy.[9] E-commerce firms, like libertarians and privacy advocates, wanted strong cryptography to be readily available; it was a key component of secure payment systems across the Internet. When the US security establishment sought to use existing laws to restrict the availability of cryptography to the general public, Magaziner, together with a coalition of businesses and privacy advocates, succeeded in changing administration policy towards a more 'hands-off' stance.

The increased salience of the Internet also had important consequences for international disagreements over data flows. The US administration could point to the success of the IETF and similar bodies as evidence in favour of self-regulatory solutions. In 1997, the White House issued its key policy document, the "Framework for Global Electronic Commerce," which attributed the "genius and explosive success of the Internet … in part to its decentralized nature and to its tradition of bottom-up governance."[10] It recommended that governments should refrain from regulating the Internet and e-commerce, except where absolutely necessary. Instead, it proposed that industry should be allowed to take the lead in regulating itself where at all possible. In other words, firms would sign up to self-regulation – they would voluntarily commit themselves to adhere to market-driven standards without any need for government intervention. This accorded well both with the existing US regime, and with the express wishes of large e-commerce

[9] Simon, *NetPolicy.com*.

[10] White House, "Framework for Global Electronic Commerce," available at http://www.technology.gov/digeconomy/framewrk.htm (Checked April 04, 2004).

firms with deep pockets and a commensurate influence on administration policy. The US further sought to create a series of bilateral agreements with its important trading partners, encouraging them to favour self-regulation instead of government mandated rules.[11] Many other states, including some member states of the European Union (EU), were at least temporarily impressed. The US administration advocated the widespread use of self-regulation at least in part because it believed that self-regulation would undermine other states' efforts to push for comprehensive regulation of cyberspace. Self-regulation would not only prevent the creation of binding inter-state institutions - it would create a 'fait accompli' that would forestall external demands for regulatory changes within the US.[12]

Thus, in the mid-1990's, there was a strong tendency towards self-regulation of the Internet as a means of promoting policy goals. Because the Internet was for the most part a US creation, internal US politics played a crucial formative role in shaping the politics of the Internet. This led to a strong bias towards self-regulatory solutions, and against government regulation. This satisfied vocal groups which had succeeded in politicizing previous efforts by US authorities to impose law on electronic communications. Perhaps more importantly, it accorded with the interests of wealthy and influential firms, which did not want their freedom of action to be stymied by strong regulations. Finally, it helped protect the US against pressures from other states, which had previously pressed for regulation of 'trans-border data flows' that might have had substantial repercussions for the regulation of the US economy.

Promoting Self-Regulation on the Internet

[11] Farrell, Henry, 'Constructing the International Foundations of E-Commerce: The EU-US Safe Harbor Arrangement', *International Organization* 57, 2 (Spring 2003): 277-306.

[12] Ibid.

The early US proponents of self-regulation on the Internet assumed that the key to encouraging self-regulation was to keep government out. In the absence of government interference, firms and individuals would be willing to regulate themselves; indeed, they would have little choice. As Debora Spar described it, in the absence of an effective state, "firms [would] have to write and enforce their own rules, creating private networks to facilitate and protect electronic commerce."[13] To the surprise of many, firms showed no such willingness. Indeed, they only appeared willing to set up meaningful systems of self-regulation when it was the only viable alternative to direct state intervention. Paradoxically, US government actors found that after they had tried to foreswear direct government involvement in the regulation of cyberspace, they had to intervene, if only to press private actors to regulate themselves (and thus remove any future excuse for government intervention). Two examples of this may serve to illustrate a more general trend.

The first of these was in the realm of privacy regulation. As previously mentioned, the right to privacy was a source of contention between the US (which opposed comprehensive privacy agreements) and other industrialized democracies (which wanted such agreements). These tensions came to a head in the late 1990s, when the European Union (EU) began to demand that the American government introduce formal privacy laws. EU decision-makers were worried that the privacy of EU citizens could be compromised by US firms who could export personal information (or gather it on the WWW) and process it in the US, outside the grip of European authorities. They thus demanded that the US introduce legislation along European lines to protect individual

[13] p.32, Spar, Debora L., 'Lost in Cyberspace'.

privacy. The US response was to argue that privacy should be protected through self-regulation rather than through law. Unfortunately, this argument was not very credible: there was little evidence that US firms had any interest in signing up to self-regulatory schemes if they could avoid it. Although one self-regulatory scheme for privacy protection, TrustE, had been set up, businesses had shown little interest in signing up to its (not very demanding) principles. European negotiators, not surprisingly, were unconvinced that self-regulation of individual privacy had any merits.

The response of the US administration was twofold. First, it pushed a second organization, the Better Business Bureau to set up a self regulatory program for privacy protection. The Better Business Bureau had no experience or prior interest in privacy protection, but was a well established organization that might help convince the Europeans that self-regulation was a possible solution. Second, the US administration began to threaten that it would indeed introduce legislation unless firms began to show their commitment to self-regulation. This had immediate results; in the words of TrustE's Chairman, firms began to sign up to TrustE in large numbers, "strangely coincidental to about the time when the government started really putting down their heavy hand."[14]

The US administration had a somewhat similar experience in the area of domain name assignment. Through a series of developments, the US government found itself in control of the process for assigning top level domain names; that is, of deciding who had authority to issue domain names like 'http://www.amazon.com.'[15] As the Internet took

[14] Susan Scott, Chairman of TrustE; remarks available at http://www.research.ibm.com/iac/transcripts/internet-privacy-symp/johnpatrick.html (checked August 20, 2001).

[15] For histories, see Froomkin, Michael, 'Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution', *Duke Law Journal*, 50 (2000):17-184 and Mueller, Milton L., *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge: The MIT Press 2002).

off, this became a potential source of political controversy. There was a landrush for potentially valuable domain names, and conflicting pressures to expand the supply of 'top level' domain names (which would favour those who had not already gotten valuable domain names), or alternatively to continue to restrict it (which would favour those who had property rights in valuable names). In response to these pressures, the US government sought to privatize the domain allocation process, and hand over responsibility and authority to a private sector actor. The US administration issued a policy paper calling for the 'spontaneous' formation of a private sector body, and committed itself to cooperating with such a body, if it came into being, and fulfilled certain conditions. Unsurprisingly, just such a body, ICANN, was created by Jon Postel, a key figure in the debate, and was duly assigned control of key aspects of domain name management. In Michael Froomkin's words, "ICANN exists because the [US] Department of Commerce called for it to exist. Once ICANN was formed, it owed its power, purpose and relevance to the Department of Commerce."[16] ICANN is nominally an independent, self-regulatory body, which only has a contractual relationship with the US government, for which it has agreed to undertake certain duties. This has led over time to an ever-growing role for the US and other states in ICANN's decision-making processes. Increasingly, government actors set the rules for ICANN, excluding other actors such as Internet activists from the process.

Thus, the second wave of 'self-regulation' differed in key ways from the first. The IETF and other early examples of Internet self-regulation may genuinely be described as spontaneous examples of 'bottom-up' self-organization, in which actors came together to meet specific technical needs. However, the success of this mode of

[16] p.70, Froomkin, Michael, 'Wrong Turn in Cyberspace'.

self-regulation depended to a very great extent on the relatively limited set of issues involved, and the willingness of the relevant actors to engage in reasoned debate over technical standards. The second wave of self-regulation was not spontaneous – instead it was the direct result of US administration policy. The US sought, for its own political purposes, to ensure that self-regulation predominated in the Internet and e-commerce. The move to self-regulation thus did not represent a fundamental challenge by private actors to state authority. Instead, it flowed from a set of choices made by the most powerful state in the international system. However, these choices have had consequences that the US did not expect – I turn to this in the next section.

Self-regulation and the international system

In the previous section, I have documented how the move towards self-regulation in e-commerce and the Internet was in large part the result of choices made by US authorities. These choices had an important international dimension – the US believed that it could forestall other states' demands for formal regulation by creating an effective international lowest common denominator of self-regulation. This would mean that the US's domestic regulatory preferences would effectively become the international default.

In retrospect, it is clear that this policy was based on a false assumption. Key policy-makers in the US administration advocated a 'pure' form of self-regulation, in which private actors would set the rules for the Internet and e-commerce, independent of states. Even though private actors came to play an important role in governance, this did not transpire. Instead, private actors are increasingly serving as channels of influence, or proxies for states. In other words, private actors are *not* creating self-regulatory realms that are outside the reach of states. Instead, they are increasingly coming to serve as vectors of state influence. They are able to do this in large part because few individuals access the Internet directly; most employ intermediaries of some sort, whether those intermediaries be ISPs, e-commerce companies, web browsers supplied by firms etc. Insofar as these intermediaries are choke-points through which most Internet users go, they provide states with a potential means of influencing a large number of individuals at low cost, through persuading or compelling the intermediary to do their will.

This has important consequences for the regulation of the Internet, and more generally for areas of policy that have been affected by the Internet. Just as in earlier eras, states continue to disagree about fundamental issues of governance. However, they now have new tools at their disposal. Those states that are able to exert influence on the relevant private actors may be able to insulate themselves from aspects of the Internet that they consider to be undesirable. In some cases, they may even be able to use their influence over private actors to shape the effective international lowest common denominator so that it reflects their preferences rather than the preferences of other states.

Consider each of these possibilities in turn. First, states are increasingly using their influence over Internet Service Providers (ISPs) and other actors, in order to insulate their societies from aspects of the Internet that they dislike. Most obviously, many non-democratic regimes limit their citizens' access to websites, email, and other forms of communication that advocate democracy, or that are critical in other ways. Contrary to the prediction that governments would not be able to censor the spread of information on the Internet, governments can and do censor the spread of information, with a reasonable degree of success. Shanthi Kalathil and Taylor C. Boas argue that there is evidence to suggest that "the Internet is not necessarily a threat to authoritarian regimes," and examine how various repressive regimes have limited their citizens' access to the Internet.[17] Many authoritarian states require ISPs to route all access to the Internet through proxy servers, which allow them to filter access to content that criticizes the regime, advocates democracy, or is objectionable to them in some other way (pornography). Frequently, access to non-local news sites is limited too. It is extremely difficult for these states fully to block access to this content, and as they develop new technologies of censorship, democracy activists and others develop new ways of circumventing these blockages. Even so, authoritarian regimes have shown themselves far better able to cope with the challenge of open communication on the Internet than might have been expected. Indeed, some authoritarian states have shown themselves adept at using the Internet in order to disseminate their views (or even hack the websites of regime opponents).

Nor has this behaviour been confined to authoritarian regimes. Many democracies too impose limits on the websites that their citizens can reach. Many Western European democracies maintain blacklists of websites that their ISPs are asked – or required – to block access to. Many of these websites advocate political positions (neo-Nazi party platforms, racist hate) that it is illegal to publish in the countries in question. Continental European states such as France and Germany are especially concerned with neo-Nazism, for historical reasons, and have taken a very pro-active stance. Even the US, which

[17] p.3, Kalathil, Sahnthi and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington DC: Carnegie Endowment for International Peace, 2003).

opposes the censorship of political arguments and most other forms of content, seems willing to countenance action at the state level to censor child pornography.

Second, and perhaps most interesting from the point of view of international relations theory, states are using private actors not only to insulate themselves, but to extent their international influence. Again, two examples may serve to illustrate a more general trend. First, France, Germany and other countries have taken steps to prevent their citizens accessing neo-Nazi material that go beyond the forms of domestic censorship that have already been described. They have sought to sway important international e-commerce firms such as eBay (a specialized Internet auction house) and Yahoo! to implement their preferences, by banning all users of their services from distributing objectionable materials. France, for example has acted to prevent Yahoo!'s customers from buying or selling neo-Nazi paraphernalia through Yahoo!'s auction website. Such material is illegal in France, yet French customers of Yahoo! could buy it relatively easily from people who lived in other jurisdictions such as the US, where it is perfectly legal to own it. After activists took a court-case in France, French courts ruled that Yahoo! had a legal responsibility to prevent French citizens from accessing this material through Yahoo!'s website, although it allowed Yahoo! some discretion in deciding how to implement this policy. Yahoo!'s immediate response was to declare that it was not bound by the French ruling, and to seek a ruling in a US court that the French judgement was unenforceable. After going through the motions of declaring that it had no need to comply with French courts, Yahoo! nonetheless banned *all* its customers, whether they were French citizens or not, from buying or selling this material. Simultaneously, it claimed, rather implausibly that this new policy had nothing to do with France's legal threats. eBay has been more forthright – in the wake of pressure from Germany, it too acted to ban the sale of Nazi-related paraphernalia through its website, noting that many eBay users were banned by their own home country from buying or selling such material. Both Yahoo! and eBay complied with European authorities because they stood to loss more than they could gain if they did not comply. Both firms had a strong interest in developing their presence in European markets, through European subsidiaries that might very possibly have been subject to substantial fines and other legal penalties. If eBay and Yahoo! had not had these important economic interests, it is doubtful that France and Germany could have done anything to persuade them to comply. Certainly, US-based ISPs that host neo-Nazi sites have shown no particular desire to comply with German demands that they shut down or otherwise limit access to these sites.

Second, the US has acted to try to prevent its citizens from accessing off-shore gambling sites, through pressuring financial intermediaries. The regulation of gambling in the US is a complex topic – federal law is murky in important respects, and regulations vary from state to state. Some US states ban gambling completely, while others allow it (and indeed prosper greatly from it). As the WWW became more easily accessible, operators began to set up gambling operations in offshore locations that were effectively beyond the reach of US jurisdiction. These sites allowed US citizens living in states where gambling was banned to evade the law with ease – by gambling on-line, they could flout the law. The small Caribbean state of Antigua and Barbuda was an especially popular base for offshore operations – at the end of the 1990's, a substantial portion of its GDP flowed directly from Internet gambling operations that were aimed at the US. Because these activities were offshore, and because previous US regulatory decisions made it difficult for US authorities to force ISPs to block access to these offshore sites, it appeared that the US had little choice but to acquiesce to the unravelling of its domestic gambling regime.

However, lawyers working for the New York state attorney-general's office hit upon an unorthodox solution – holding financial institutions such as banks and credit card agencies responsible for facilitating illegal transactions between New York state citizens and offshore gambling operations. Through fining or threatening to fine, New York state succeeded in making financial institutions stop allowing these transactions to take place. Other authorities – including authorities at the federal level – appear to be following suit. The results have been striking - the size of the Antiguan online gambling industry halved over a few years, in large because of the US crackdown. Antigua's response was to take an action against the US at the World Trade Organization – at the time of writing, Antigua has succeeded in winning a preliminary judgement that the US action was probably illegal under world trade law.

In both of these cases, states have used their influence over certain key private actors (Internet auction houses, financial institutions), to exert extra-territorial control over other private actors' activities on the Internet. Nor are these the only cases of this phenomenon – states are increasingly using influence over private actors to achieve their political goals for Internet regulation – even in the absence of agreement from other states. This is an unexpected result. Contrary to the predictions of some, private actors are not replacing states as the key sources of Internet governance. Nor, for that matter, are states reasserting control through traditional instruments (international agreements, direct action) in many important areas of Internet policy. Instead, what we are seeing is the creation of a new set of relationships between states and private actors, as states begin to use private actors as proxies to achieve policy goals that they otherwise couldn't achieve. This has important implications for the international regulation of the Internet, which I will turn to in the next and final section of this chapter.

Conclusions

In this chapter, I have argued that the Internet's consequences for international politics are not at all what might have been expected. Private actors, rather than replacing states and transforming the international system, are becoming proxies for states in many instances. This is not unique to the Internet– states have used other private actors (standard setting organizations, for example) to achieve their aims in other – and less sexy – areas of politics than Internet regulation. This said, international relations theory has had very little to say about the sources and consequences of these state-private actor arrangements to date. Thus, these emerging forms of Internet regulation may have interesting lessons for Internet policy more generally.

Most prominently, it is clear that the ability of states to persuade private actors to do their bidding varies. In particular, where states have few bargaining tools vis-à-vis private actors (they cannot make credible threats or credible promises to sway these actors) they will have little success in making these actors do their bidding.[18] Thus, for example, France and Germany succeeded in persuading Yahoo! and eBay to implement France and Germany's preferences for the censorship of certain material rather than the US's preferences (for the free dissemination of political material, even if it's offensive). They were able to threaten adverse consequences (fines, effective legal sanctions) if

[18] I develop this point in forthcoming work.

Yahoo! and eBay did not comply. In contrast, however, Germany did not succeed in persuading US-based ISPs to take down neo-Nazi material – because it could not threaten effective punishments (these ISPs were beyond its reach), its influence over the relevant actors was negligible.

This has interesting implications for US bargaining power. Because of the early choices that were described in the beginning sections of this chapter, the US has tied its hands behind its back in important areas of Internet policy. It has voluntarily foresworn Internet regulation – and thus has few effective ways of threatening many private actors who do not do its bidding. For example, it is highly difficult for US authorities to make ISPs block access to certain kinds of content – even when they would prefer to do so, or to share certain kinds of content with government enforcement authorities. It is important not to exaggerate this problem. The US has managed in many instances to exert control, either by using actors not directly involved with the Internet (financial institutions) to extend its extraterritorial grip, or by invoking urgent security needs in order to make private actors comply. Still, the US now enjoys less influence over many aspects of Internet policy than one might reasonably have expected five years ago, or even today, if one looks at the enormous importance of the US market.

It also is likely to have important implications for the existing international structures governing international exchange, even if these implications are still rather difficult to discern. Existing international institutions such as the WTO rely on definitions of goods and services that are increasingly adrift from reality, and fail explicitly to regulate categories of activity (such as the kinds of influence through private actors that I have discussed), which are demonstrably important to the world economy. It is difficult to predict how well they will adapt. If the last five years of discussion on the international regulation of the Internet has focused on broad questions about the role of states and private actors, the next five is likely to be much more closely concerned with the particular impact of the Internet – and the state-private actor relationships associated with it – for a variety of issues in international politics.

Suggested Readings

Drezner, Daniel H., “The Global Governance of the Internet: Bringing the State Back In.” Forthcoming in *Political Science Quarterly*. Also available at http://www.danieldrezner.com/research/egovernance.pdf (checked April 26 2004).

Farrell, Henry, ‘Constructing the International Foundations of E-Commerce: The EU-US Safe Harbor Arrangement’, *International Organization* 57, 2 (Spring 2003): 277-306.

Kalathil, Sahnthi and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington DC: Carnegie Endowment for International Peace, 2003).

Spar, Debora L., *Ruling the Waves* (New York: Harcourt and Brace 2001).