Local Power, Global Reach: The Domestic Institutional Roots of Internet Governance

DAVID BACH AND ABRAHAM L. NEWMAN

Ten years into the Internet revolution it is clear that early claims about power and governance in a digitised world have largely missed their mark. In his 1996 Declaration of the Independence of Cyberspace, John Perry Barlow flatly told governments: 'You have no sovereignty where we gather. … You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear.'[1] Barlow of course was and is a cyber-libertarian, a former songwriter for the Grateful Dead. Other leading legal scholars struck a similar chord. In an influential 1996 essay, law professors David Johnson and David Post argued, 'The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new Phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign.'[2] The Internet, the reasoning went, constituted a separate and independent jurisdictional space, one that required new forms of governance and a unique set of rules.

Even governments bought into the notion that the Internet was somehow different, that its speed, flexibility and global reach meant that cyber-governance was best left to the private sector. In their 1997 *Framework for Global Electronic Commerce*, President Clinton and Vice President Gore said that the United States (US) 'will encourage the creation of private fora to take the lead in areas requiring self-regulation such as privacy, content ratings and consumer protection and in areas such as standards development, commercial code and fostering interoperability.'[3] In response, Europe's then Commissioner for Telecommunications, Martin Bangemann suggested that business should take the lead in developing an international e-commerce framework that would rely heavily on 'market-led, industry-driven, self-regulatory models.'[4] On both sides of the Atlantic, business was near universally seen as more qualified and better equipped to govern digital markets. Because of leading e-commerce firms' global reach, empowering business was seen as a way to ensure consistent global rules, thus avoiding regulatory fragmentation along state lines.

D. Bach & A.L. Newman, 'Local Power, Global Reach: The Domestic Institutional Roots of Internet Governance,' *STAIR* 3, No. 1 (2007): 23-41.

More than ten years into the Internet revolution, we can see that things have turned out quite differently. Early conventional wisdom on Internet governance has been wrong on two important points.[5] First, while private actors have undoubtedly played important roles, governments have been in the driver's seat as far as questions of Internet governance were concerned.[6] This is because the Internet has become a victim of its own success; it penetrated economies and societies more quickly and more thoroughly than even its most enthusiastic advocates expected. This penetration has made the neat separation of online/offline or cyberspace/physical space as envisioned by Barlow and others impossible.[7] Governments have asserted authority over cyberspace to defend existing–often pre-Internet–policies, regulations and interests. Secondly, while the underlying communications networks powering the Internet may be global, Internet governance has not been an exercise in consensus driven global rule-making. Rather, as individual governments have asserted authority, often incompatible or conflictive domestically rooted solutions have been advanced globally, usually through the extraterritorial application of domestic rules.

In this setting, Europe and the US have been most influential, largely to the detriment of developing countries. But the two have frequently been at odds over how to respond to new digital challenges. Whereas European policymakers have favored strict rules protecting personal information, the US has advocated a more market-based approach. Conversely, European countries have been permissive of Internet based gambling whereas the US has aggressively sought to prevent its citizens from visiting online casinos and poker halls. Even in areas where an early transatlantic consensus existed, as in the case of domain name governance, there has recently been a fair amount of discord.

How can we explain policy positions and varying patterns of influence in global Internet governance? This paper argues that much of contemporary Internet governance is the result of domestic political struggles unfolding transnationally. Both policy preferences and power are rooted in domestic political and regulatory institutions. By focusing on the domestic institutional determinants of individual government influence, we can shed light on why Europe has prevailed in some areas, the US in others and why other countries have generally been rule-takers in the field of Internet governance. Domestic regulatory institutions are a critical determinant of power in global governance and Internet governance is no exception.[8] Countries with a clearly defined set of domestic market rules are best positioned to advance their preferences internationally, particularly if they can leverage sizeable domestic markets towards that end.

The next section outlines a domestic institutional argument of global governance. International regulatory influence, we argue, is a function of both domestic market size and the extent of regulatory capacity over that market. Jurisdictions with large and attractive domestic markets can wield extraterritorial influence if they have the capacity to formulate, monitor and enforce a set of domestic market rules despite globalisation. The importance of large domestic markets explains why the US and the European Union (EU) have enjoyed disproportionate influence over Internet governance.[9] The focus on the role of domestic regulatory capacity explains why the US has prevailed in some areas and Europe in others, as domestic regulatory capacity tends to vary across sectors, issues and time. In the second part of the paper, we illustrate the argument through case studies of governance in the fields of data privacy, Internet domain names and online gambling. The final section concludes with thoughts on the future of power and governance in a digitised world.

Localising Global Internet Governance

To properly understand global Internet governance, research must re-examine the role that states play in creating the rules for digital markets. Contrary to the predictions of early cyber-libertarians, the state has not relinquished its authority. Internet governance also confounds international relations theories that expect nations to resolve conflict through intergovernmental negotiations. Instead, much of global Internet governance is the result of domestic rules developed on the national level spilling over and affecting other countries. The very trans-territoriality of the Internet allows national rules to reverberate internationally.[10] The prosecution of Yahoo! in French courts for material made available on the company's U.S. website but accessible by French citizens typifies this new global governance of the Internet.[11]

The complexities and perceived messiness of Internet governance notwithstanding, there are clear patterns of influence. When and why a state can shape the rules governing global digital markets thus becomes the critical question. We argue that two factors are decisive. Jurisdictions with large markets have the ability to leverage their market size to induce compliance with their preferred policies. Firms in other countries fear being excluded from such markets and want to minimise the costs of complying with multiple rules.[12] While market size is a necessary condition for regulatory influence, size alone is not sufficient. Markets,

whether in physical or cyberspace, are defined by rules.[13] We argue that regulatory capacity–a jurisdiction's ability to define, monitor and enforce a set of market rules at home–is the other critical determinant of influence over global Internet governance. If both factors are present, a state is well positioned to shape regulation in a digitised world.

Drawing on the realist theories of international relations, political economy research has emphasised the power that large markets have to influence international economic governance.[14] James and Lake termed this 'the second face of hegemony' and argued that great powers leverage trade relations to alter the relative prices of goods in foreign markets.[15] Nations with large markets are thus better positioned to win favorable outcomes in international negotiations. They can also alter the preferences of firms in other jurisdictions so that foreign firms support greater power preferences in their home markets.[16] More recently, Drezner has applied this logic to the case of Internet governance.[17] He argues that the character of global governance can be explained by the positions of the US and the EU, owing to their dominant market size. When the two jurisdictions share a common position, as he claims is the case in Internet protocols and intellectual property rights, a stable negotiated settlement is possible. When they disagree, as in cases such as harmful Internet content or data privacy, governance will be at best a sham or at worst characterised by competing rival standards and fragmentation. While Drezner notes that smaller economic players can influence negotiations, he concludes that lasting international solutions to Internet governance depend on agreements between the great powers.

Drezner's contribution offers an important corrective to earlier work that emphasised the role of private actors, such as firms and NGOs, in global Internet governance. We agree that research on Internet governance must take seriously the role that states play in international bargains. However, the current conception of state power, which looks only at the material character of markets, is both theoretically and empirically unsatisfactory. In many areas, one jurisdiction has prevailed in international debates despite transatlantic discord. In both the case of data privacy and Internet domain name governance, one great power has dominated the debate despite opposition from the other. At several critical moments in these debates, large markets were either absent from formal international discussions or were incapable of formulating a coherent international position. The ability of great powers to exert their influence over Internet governance has varied across sectors and time, variation that is not easily explained by market size alone.

To correct the limitations of existing work, we examine a jurisdiction's regulatory capacity, which encompasses its ability to define,

monitor and enforce a set of domestic market rules.[18] A jurisdiction's regulatory capacity is determined by at least two factors–expertise and statutory authority. Expertise refers to the knowledge that is necessary to formulate an agenda and define a coherent policy solution to a regulatory challenge. Particularly in the arena of Internet governance where many issues lie at the intersection between two highly technical fields–computer science and law–regulatory expertise is crucial. Jurisdictions build up expertise in a field through years of experience, and the creation of policy networks combines experts in that field.

Once a jurisdiction has defined a clear set of market rules, they must have the authority to punish violations. Statutory authority to control market access and fine regulatory breaches provide a jurisdiction with the mechanisms to translate market size into a powerful tool for international regulatory influence. While market size determines the potential costs that great economic powers can inflict on others that fail to abide by their demands, regulatory capacity determines the likelihood that a great power can actually carry out such threats.

Integrating the analysis of domestic regulatory institutions into international Internet governance debates sheds light on state preference formation, issue coherence and bargaining influence. We briefly discuss each in turn. Internal regulatory regimes involve a tremendous amount of institutional-sunk costs for governments and firms. Governments often create intricate bureaucratic structures to administer regulatory regimes,and these bureaucracies invest in and defend their competencies. If challenged–for example by a new technology such as the Internet–they try to defend existing domestic solutions.[19] When the challenge has a transnational character, as is generally the case with the Internet, this often involves promoting international rules that mimic domestic regulation, thereby safeguarding the domestic status quo. Similarly, firms invest considerable resources into domestic regulatory compliance. While some firms may view international challenges as a way to lower regulatory standards, many prefer simply to minimise adjustment costs.[20] Domestic regulatory institutions, then, shape national interests vis-à-vis international governance.

Similarly, domestic institutionally-rooted regulatory capacity affects the ability of a jurisdiction to formulate a coherent international governance position. Once preferences exist, the state must be in the position to define an international agenda. The absence of a regulatory spokesperson with expertise acquired domestically limits a jurisdiction's ability to do this.

Finally, regulatory capacity shapes the bargaining strength that a jurisdiction can wield in formal or informal international debates. While

great powers rely on the size of their domestic markets to incentivise foreign adjustment, they depend on their regulatory capacity to back up demands with credible threats of non-compliance costs. In cases where great powers cannot enforce their domestic market rules, foreign firms have little to fear from great power blustering.

Internal regulatory capacity is particularly critical for global Internet governance as many regulatory debates take place outside traditional intergovernmental fora. While nations have engaged United Nation (UN) agencies and the World Trade Organisation (WTO) in several high profile areas, most notably intellectual property, Internet governance on the whole has evolved in other institutional settings. In contrast to those that predicted a new field of global cyberlaw, great economic powers have worked to externalise their domestic regimes through extraterritorial provisions of national law. The global architecture of the Internet amplifies this change as decisions taken in one jurisdiction quickly appear on the policy-making agenda in others.

To illustrate the argument, we explore in the next section three cases–data privacy, Internet domain names and online gambling–that demonstrate the importance of market size in conjunction with domestic regulatory capacity for global Internet governance.

Data Privacy

Starting in the 1960s with the advent of computer technology, societies have long confronted concerns dealing with the collection and processing of personal information. In response, governments enacted data privacy laws. These laws enforce a set of basic data privacy principles on the use of such information. While advocates of privacy legislation made similar appeals across the globe, national legislation varied across countries. Some countries, including Germany and France, adopted comprehensive regulations covering both the public and the private sector. These laws were overseen and enforced by independent regulatory agencies–data privacy authorities. In other countries, such as the US and Japan, legislation was restricted to the public sector. Regulations applied primarily to government bureaucracies with some additional application in sensitive sectors such as health-care and banking. In general, however, industry-led, market-based efforts defined the governance strategy for business use of personal data. Other countries ranging from Italy to Argentina adopted no regulations at all throughout the 1990s. As

a result, the world entered the digital era with a wide array of strategies and a high degree of regulatory fragmentation.[21]

This changed, however, with the passage of the European data privacy directive in 1995. In addition to requiring all E.U. member states to adopt comprehensive rules and to create formal regulators, the directive included an extraterritorial provision. This provision prevents the transfer of personal information to countries that have failed to implement 'adequate' privacy safeguards.

The European privacy directive has had significant international ramifications. A number of countries ranging from Albania to Argentina that did not previously have data privacy legislation have adopted comprehensive rules. Another set of countries, including Japan, Canada and Australia, which had previously relied on limited public sector regulations, extended coverage to the private sector to meet European demands. Altogether over 30 countries have adopted the European approach since the passage of the data privacy directive.[22] Even the US was strong-armed into signing an international accord, the Safe Harbor Agreement, which requires U.S. firms active in European markets to safeguard data processed in the US by European rules.[23] The US signed the agreement even though it was the most vocal supporter of self-regulatory solutions for global Internet governance, including data privacy. Similarly, multinational corporations have moved to comply with European rules in their global data management systems to minimise the regulatory costs of complying with multiple regulatory regimes.[24]

Why was Europe able to export its domestic regime? Regulatory capacity played a critical role in the international spread of European privacy rules. First, Europe had a coherent strategy regarding the international governance of privacy that it leveraged in international fora. Parallel to internal European debates on privacy during the early 1990s, the European Commission pushed for a privacy exemption in international trade rules. While negotiating the General Agreement on Trade in Services (GATS), the Commission team found that the US offered no resistance to its demand for a cultural exemption for privacy.[25] The US, at the time, did not have the regulatory competence to foresee what such an exemption could mean. It was only after the adoption of the privacy directive that the US argued that privacy rules breached international trade law.[26] Owing to the earlier negotiation, however, Europe had already constructed institutional protection for its approach.[27]

Similarly, Europe has used its statutory authority to control market access. It has done this to persuade foreign jurisdictions to adjust their

domestic regulatory policies. In three cases–Hungary, Switzerland and Canada–the Commission ruled that national reforms met E.U. standards. In other cases, the EU has refused to confer adequacy status, forcing national governments to further reform their national policies. Australia is an important example. After years of following a limited regulatory path, Australia reformed its national legislation to cover the private sector in 2000. Despite this reform, the EU identified a number of loopholes in Australian legislation. A regulatory network of national data privacy regulators in Europe, the Article 29 Working Party, released an opinion that found the Australian regulations inadequate.[28] The EU has worked with the Australian government to amend its law and Australia has passed several reforms that have addressed the most critical problems.

In the case of data privacy, Europe has thus relied on internal regulatory capacity to shape international Internet governance. With the passage of national legislation in the 1970s, Europe created independent regulatory agencies with considerable expertise and statutory authority. European regulation expanded both of these resources in the 1990s. The EU, combining its market size with its regulatory capacity, externalised its internal regulatory regime, forcing global harmonisation around its preferred policy.

Internet Domain Names

Since 1998, global governance of the Internet's Domain Name System (DNS) has been officially in private hands.[29] That year the U.S. government delegated administrative authority over the DNS to the Internet Corporation for Assigned Names and Numbers (ICANN), a California non-profit organisation. ICANN performs this role under a contract with the U.S. Department of Commerce, a contract that is periodically reviewed and can be cancelled unilaterally by the U.S. government. For at least the past five years, a growing coalition of governments–especially from developing countries and emerging markets–has sought to place DNS governance under international governmental oversight.[30] Many even demand the transfer of all ICANN responsibilities to the International Telecommunications Union (ITU), a U.N. affiliate in Geneva. In the run-up to the 2005 World Summit on the Information Society (WSIS), the European Union joined the camp of ICANN skeptics, leaving the US isolated as the current system's only major proponent.[31] Nevertheless, at the WSIS meeting, efforts to change the status quo failed

yet again. Why did the US opt for private domain name governance in the first place and how has it upheld its preferred policy internationally?

From its inception in the early 1980s, the DNS had been run by a small group of computer scientists and network engineers led by Jon Postel, an Internet pioneer who coordinated the system under a contract with the U.S. Department of Defense through an entity he called the Internet Assigned Numbers Authority (IANA). When authority over the Internet moved from the military to the civilian research community in the early 1990s, the National Science Foundation (NSF) awarded a contract to manage registered domain names and to run the system's authoritative 'A' root server to Network Solutions, Inc. (NSI), a small company in Virginia. The explosion of domain name registration following the Internet's commercial breakthrough raised the stakes, turned NSI into a multi-million dollar enterprise, and eventually led to a rupture between NSI and Postel's IANA.[32] The resulting uncertainty about who was in charge of such a critical asset prompted the Clinton Administration in 1997 to step in, assert regulatory authority over the DNS based on prior Internet funding and contracts and to draw up plans for a new order.

To the U.S. government, private sector governance of the domain name field had two decisive advantages. First, as U.S. Internet firms, including NSI, had thrived in an environment characterised by little government intervention, creating a new national or international bureaucracy was seen as contrary to U.S. interests. This was especially true given that the DNS–as one of the Internet's few central access points–could in theory be used to enforce all kinds of policies, even those wholly unrelated to domain names. Secondly, private governance offered an opportunity to ensure considerable U.S. influence while avoiding the charge that the U.S. government was taking over a global resource. The White House directed an Interagency Workgroup to draw up a plan for a 'contractually based, self-regulatory regime.'[33] A new private body was to coordinate the DNS under a U.S. government contract and was also to enter into contractual relations with domain name registrars, registries, and other stakeholders around the world.

Despite rhetoric that private governance was by definition global, the ensuing process was heavily US-focused. Of the 400 comments received on the initial proposal, only seven percent came from outside the US.[34] The European Commission was the only non-U.S. governmental entity that officially commented on the proposals, and it only stressed the need to take the views of European stakeholders into account.[35] In the words of one ITU official at the time, 'it was simply impossible to find high-ranking government officials in Europe who were interested

in this."[36] Most governments were still trying to come to terms with the Internet as a whole, let alone something as seemingly mundane and technical as domain name administration. The way Postel had previously run the DNS was an important reason for foreign governments' ignorance. As self-appointed head of IANA, the job of delegating authority over particular domain suffixes–including country code domains such as .uk or .nl–fell to him. Yet his method of delegation 'tended to bypass completely the institutions in other countries that historically had possessed authority over communication, such as government ministries or post, telephone, and telegraph monopolies.'[37] Foreign regulatory expertise thus formed in the private sector and local research communities, not among governments.[38]

With international concerns largely sidelined, the focus of U.S. policy deliberations shifted towards reconciling two sparring domestic camps–the old Internet's engineering elite led by Postel and the new commercial interests represented by NSI. The resulting ICANN based global governance structure reflects the domestic political bargain brokered by the U.S. government. The Department of Commerce picked ICANN to administer the DNS and appointed Postel as its head. However, it also guaranteed NSI a privileged position in the new system of registries and left it in charge of the critical 'A' root server, thus depriving ICANN of important leverage from the start. Ostensibly to 'keep the peace' and thus safeguard the Internet's stability, the Commerce Department retained policy authority over the DNS and reserved the right to intervene or overrule ICANN. Subsequently, the U.S. government backed away from its stated intention to eventually transfer all policy authority to ICANN, prolonging regulatory uncertainty and considerably irking non-U.S. stakeholders who had since awoken to the issue's importance.

While the Clinton Administration made much of the claim that private governance was truer to the character of the Internet, by definition global and inclusive, and in any event superior to government regulation, domestic political and economic considerations were the principal source of policy preferences. The domestic arena is also the source of U.S. power in this area because it is there that regulatory capacity building occurred. It is true that the U.S. domestic market for domain names was considerably larger than any other during the critical period–it accounted for roughly 50 percent of the world total and was more than ten times as large as the UK and Germany, number two and three respectively.[39] Likewise, even after its monopoly on .com, .net, and .org registrations had fallen in 1999, NSI remained by far the world's largest domain name registrar with more than two-thirds of the market.[40] However, just as important as market share has been domestic regulatory capacity. Before anybody

else, the US began the process of building governmental regulatory expertise in this area and laid the legal foundation to exercise authority over the DNS. Once it had formally asserted policy authority, the Commerce Department barred ICANN and NSI from making any changes to the 'root zone file'–the information stored on the 'A' root server that directs inquiring computers toward their target–without its written approval. The U.S. Commerce Department thus holds de-facto market exclusion power over the domain name market, not just for the US, but essentially worldwide in an extraterritorial fashion.

Because of its sweeping authority over the DNS and associated extraterritorial reach, the US has been able to largely ignore foreign pressure, at times even overtly snubbing its critics.[41] In light of a united front at the November 2005 WSIS meeting pressing for change, the US made some small concessions and agreed to the establishment of an Internet Governance Forum under U.N. auspices to advise on critical questions of Internet governance.[42] But it again refused to commit to relinquishing unilateral U.S. oversight over the DNS. This seemingly changed a few months later when the Department of Commerce and ICANN presented the latest iteration of their Memorandum of Understanding (MOU). Indeed, the U.S. government suggested ICANN could obtain independence by 2009, but observers were quick to denounce the move as merely rhetorical. According to a group of ICANN experts, 'The US and ICANN have responded to these concerns by dressing up their MOU relationship in new clothes. The object seems to be to strengthen the public's perception that ICANN is relatively independent. But the basic relationship between the US [government] and ICANN is fundamentally unchanged.'[43] Some countries, including China, are now openly toying with the idea of setting up an alternative root.[44] But for those unwilling to risk a root split and potentially parallel and incompatible Internets, pressuring the US to share DNS oversight with other governments is the only option. So far this has been to no avail.

Online Gambling

In both data privacy and domain names, global governance has converged around a set of policies. In the former case they were set by the EU and in the latter by the US. The case of online gambling is different because global rules remain unclear and contested. For domestic political and regulatory reasons, the US has banned online casinos and poker halls within its jurisdictions. But because the Internet enables U.S.

citizens to just as easily place bets with offshore websites in Antigua, Bermuda or Gibraltar, stamping out online gambling by U.S. citizens has required stringent new regulation with extraterritorial reach. This has angered not only online casino operators and authorities in prominent offshore locations but increasingly also irks governments in Europe and Australia where an online gambling industry is taking hold.

Gambling has always been a controversial issue in the US.[45] After a complete ban in the early decades of the 20th century, Nevada became the first state to legalise gambling in the 1930s. By the mid-1970s, other states began to open their market and by 2004, about half had legalised gambling. Gambling has also been legalised in self-governing Native American reservations. Several decades before the Internet, communication technologies posed a fundamental challenge to the federalist approach of letting individual states set gambling policy. The diffusion of household telephones enabled Nevada bookmakers to accept bets from outside the state by phone, and two-way wire transfers took care of the financial side. In response, Congress enacted the Interstate Wire Act (also known as the Federal Wire Act) in 1961, which made it a crime to place or receive a bet via a wire communications service.

The rise of Internet based online casinos, poker halls, and sports betting services posed an even more formidable challenge to U.S. efforts to restrict gambling to certain locations. This is because U.S. consumers have turned out to be among the world's most avid online gamblers. In 2006, an estimated 23 million Americans played poker over the Internet every day. Since 1998, the number of Americans gambling online has grown about twenty percent a year, piling up more than US$6 billion in revenue in 2006.[46] The U.S. market thus represents about half the world's total, estimated at about US$13 billion.[47] Not surprisingly, several leading online gambling companies such as BetOnSports, 888 Holding and PartyGaming depend to a very large extent on revenues from the US.

After the Bush Administration took office in 2001, the U.S. Department of Justice took the position that the 1961 Interstate Wire Act also applied to the Internet and that Internet based gambling was therefore illegal. Leading online gambling firms catering to the U.S. market thus moved their operations offshore, especially to the Caribbean. The policy change did not have much of an effect as U.S. gamblers continued to use their credit cards to place online bets. That the receiving institution was based offshore was hardly noticeable to them. To enforce its ban, the Justice Department therefore decided to crack down on U.S. payment service providers. After some initial resistance, even the largest credit card

providers such as Citibank bowed to government pressure and pledged not to permit transfers to known offshore gambling sites.[48]

While offshore gambling providers as well as U.S. gamblers found ways around the new enforcement measures, the industry nevertheless suffered. By 2004, the number of Antiguan jobs in the offshore gambling industry, for instance, had fallen by more than half. Antigua and Barbuda, a tiny island nation of 68,000, thus charged the US with breach of international trade in services rules and extraterritorial application of U.S. law, and took the case to the WTO.[49] The EU, Japan, Canada, Mexico and Taiwan all filed briefs in Antigua's support.[50] Defending its measures as legal, the US referred to escape clauses in existing trade agreements that permitted exceptions to uphold public morals. While the WTO agreed in principal that a defence of public morals could indeed be invoked in this case, its dispute resolution panel nevertheless found in favour of Antigua.[51] In 2000, the US enacted the Internet Horseracing Act which explicitly legalised placing bets via the web on horse races, provided such betting was legal in the states of both transacting parties and provided such bets were placed with U.S. firms. In its ruling, the WTO found dual discrimination–Antiguan firms were excluded from the U.S. horse racing market and the US permitted some forms of Internet based gambling but not others. Nevertheless, in the spring of 2006, the US let a deadline lapse to comply with the WTO finding.[52]

The international debate over online gambling came to a head in the fall of 2006. First the British CEO of BetOnSports was arrested in Texas on his way to Costa Rica where his company is based,[53] and then, in a move that surprised even industry insiders, the still-Republican Congress passed the Unlawful Internet Gambling Enforcement Act, elevating previous Department of Justice policy to the level of federal law.[54] Under the new law, banks are formally prohibited from allowing payments by U.S. residents to online gambling services. The regulation sent shockwaves through the industry, crashing share prices of online gambling services, prompting several leading providers to issue new rules to explicitly exclude U.S. gamblers, and setting off a process of industry consolidation.[55] While some experts predict that ways around the new payment ban will be found, the industry outlook in the aftermath of losing its largest market is still quite gloomy.

Meanwhile Britain in particular is becoming increasingly hospitable to the idea of online gambling and especially to providers of online gambling services. Almost all publicly listed online gambling firms trade on the London Stock Exchange and British offshore locations such as Gibraltar or the Isle of Man host a fair number of websites. British authorities are ready to legalise online gambling under strict rules aimed

at protecting minors and stamping out financial fraud. Indeed, Britain has hosted an international summit of the sector to evaluate options for a global approach to legalisation.[56] For the time being, however, other European governments have refused to go along with this. France and Germany are trying to protect their domestic gambling monopolies and the European Commission consequently sees no immediate future for efforts to harmonise gambling regulation throughout the EU.[57]

While far from settled, the case of online gambling regulation is consistent with our domestic institutional framework for Internet governance. Global rules are not resulting from an internationally coordinated public policy process. Rather, global governance is shaped by domestic regulatory politics in the largest and most influential markets playing out transnationally. The U.S. position on online gambling is a mix of commercial and political interests. U.S. land based casinos, and especially those collecting taxes on land based casino operations, see online gambling as a threat. Moreover, the strong general opposition to legalised gambling in part of the US mixes with special concern for minors and fraud victims in the case of online gambling. The U.S. government has thus applied existing, pre-Internet rules to the new medium. Its global influence in this area is rooted on the one hand in the size and importance of the U.S. gambling market and on the other hand in conscious efforts to strengthen already considerable regulatory capacity in this area. European countries' positions are similarly shaped by domestic political trajectories. Britain, where a competitive betting industry has long flourished, views legalisation more favourably than countries such as Germany and France that are concerned about the implications for state monopolies. Europe could shape global Internet governance in this area if it rallied around a common position and built the regulatory capacity to effectively regulate legalised online gambling, including services provided from offshore locations. It is too early to tell how the matter will end, but it is clear that governments embedded in domestic political contexts have been calling the shots, not private actors operating in an allegedly borderless cyberspace.

Conclusion

Taking stock of global Internet governance a decade after the onset of the digital revolution, it is clear that something remarkable has happened. The state has reasserted itself by defining and enforcing the rules for digital markets. Contrary to early predictions of a sweeping new field

of global cyberlaw, however, Internet governance has been driven primarilyby local decisions. The three cases examined–data privacy, domain names and online gambling–demonstrate several intriguing features of global Internet governance. Domestic regulations reverberate internationally through the trans-territorial nature of the underlying communications networks. Large markets are best positioned to externalise their domestic regulations by using control over market access to affect the preferences of firms and governments in other jurisdictions. Large markets do this by employing domestic regulatory capacity to activate latent power vested in domestic markets.

This finding has a very practical implication. It suggests that governments and firms have an interest in building up their domestic regulatory institutions. These are the agencies and organisations that defend national interests in international regulatory debates over emerging Internet governance questions. To the extent that political efforts in the US to undermine government regulation of the economy have succeeded, the US may well be in a weaker position to shape the next round of Internet governance questions. At the same time, Europe has invested heavily in the creation of a regulatory state and many other countries have come up to speed with the Internet and are building regulatory capacity.[58] Perhaps the most significant developments in this respect are recent Chinese efforts to develop powerful domestic regulatory institutions in the field of information and communications technologies. While still in its infancy, China's regulatory state has already become a source of influence in global technology governance.[59]

On a more theoretical level, our argument calls on scholars of Internet governance to ground their analysis in historical legacies. Discussions of most technological innovations assume a tabula rasa environment that allows total governance experimentation. As this paper shows, nations confront new technological challenges with an existing palette of resources. The weakness of the US in current privacy debates, for example, dates back to decisions made in the 1970s; its opposition to online gambling is deeply rooted in federalism and the power of moral politics in some states. To get a fuller picture, we need to look at how national regulatory trajectories interact with one another over time and thereby produce global regulatory outcomes.

[1] See John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996).

[2] David R. Johnson and David Post, 'Law And Borders - The Rise of Law in Cyberspace,' *Stanford Law Review* 48 (1996): 1367-78.

[3] William J. Clinton and Albert Gore, *A Framework For Global Electronic Comerce* (1997).

[4] See Commission of the European Communities, *Globalisation and the Information Society: the Need for Strengthened International Co-ordination* (1998).

[5] 'Internet governance' means many different things to different people. See William J. Drake, 'Defining ICT Global Governance,' Working Paper for the Social Science Research Council's Research Network on IT and Governance' (2004). In line with recent thinking on the subject, we use the term 'Internet governance' broadly to refer to the governance of new markets and other social spaces enabled by the Internet.

[6] See Daniel W. Drezner, 'The Global Governance of the Internet: Bringing the State Back In,' *Political Science Quarterly* 119 (2004): 477-98, and Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

[7] See, for example, Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), Christopher T. Marsden, ed., *Regulating the Global Information Society* (New York: Routledge, 2000), James N. Rosenau, 'Information Technology and the Skills, Networks, and Structures that Sustain World Affairs,' in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, ed. James N. Rosenau and J.P. Singh (Albany, NY: State University of New York Press, 2002), and Henry Farrell, 'Governing Information Flows: States, Private Actors and E-Commerce,' *Annual Review of Political Science* 6 (2006).

[8] David Bach and Abraham L. Newman, 'The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence,' *Journal of European Public Policy* 14:6 (2007).

[9] Daniel W. Drezner, 'Globalisation, Coercion, and Competition: The Competing Pathways to Policy Convergence,' *Journal of European Public Policy* 12:5 (2005): 841-59.

[10] Abraham Newman and John Zysman, 'Frameworks of Analysis for the Political Economy of the Digital Era,' in *How Revolutionary was the Digital Revolution?: National Responses, Market Transitions, and Global Technology*, ed. John Zysman and Abraham Newman (Stanford, CA: Stanford Business Books, 2006).

[11] 'Yahoo!'s French connection,' *The Economist*, 20 November 2000.

[12] See David Vogel, *Trading Up: Consumer and Environmental Regulation in a Global Economy* (Cambridge: Harvard University Press, 1995), and Elizabeth DeSombre, 'Baptists and bootleggers for the environment: The origins of United States unilateral sanctions,' *Journal of Environment & Development* 4:1 (1995): 53-75.

[13] Karl Polanyi, *The Great Transformation* (New York: Farrar & Rinehart Inc., 1944).

[14] See, for example, Albert O. Hirschman, *National Power and the Structure of Foreign Trade* (Berkeley: University of California Press, 1945), Stephen D. Krasner, 'State Power and the Structure of International Trade,' World Politics 28:2 (1976), 317-47, and Robert Gilpin, *Global Political Economy: Understanding the International Economic Order* (Princeton: Princeton University Press, 2001).

[15] Scott C. James and David A. Lake, 'The Second Face of Hegemony: Britain's Repeal of the Corn Laws and the American Walker Tariff of 1846,' *International Organisation* 43:1 (1989): 1-29.

[16] This is the mechanism underlying what Vogel describes as the 'California Effect.' See Vogel.

[17] Drezner, 'The Global Governance of the Internet'.

[18] Bach and Newman, 'The European Regulatory State and Global Public Policy'.

[19] David Andrew Singer, 'Capital Rules: The Domestic Politics of International Regulatory Harmonisation,' *International Organization* 58:3 (2004): 531-66.

[20] Elizabeth DeSombre, *Domestic Sources of International Environmental Policy: Industry, Environmentalists, and U.S. Power* (Cambridge: MIT Press, 2000).

[21] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).

[22] See Abraham L. Newman, *Creating Privacy: the Politics of Personal Information in the United States and Europe*, PhD Dissertation, University of California, Berkeley, 2005.

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

[24] Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Boulder: Lynne Rienner Publishers, 2005).

[25] Interview with the Commission official responsible for data privacy in the Internal Market Directorate during the GATS negotiations.

[26] Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, D.C.: Brookings Institution Press, 1998).

[27] Newman, 'Frameworks of Analysis'.

[28] See Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment Act 2000* (Brussels: European Community, 2001).

[29] The DNS is a hierarchical, inverted tree-like database that links domain names such as sant.oxford.ac.uk to numerical computer identifiers (so-called IP addresses) and thereby allows users to 'locate' content or other users on the Internet.

[30] See Frances Williams, 'Pressure grows on US over control of internet,' *Financial Times*, 7 October 2005. See also contributions to William J. Drake, ed., *Reforming*

Internet Governance: Perspectives from the Working Group on Internet Governance (New York: United Nations ICT Task Force, 2005).

[31] Tom Wright, 'EU and U.S. clash over control of Net,' *International Herald Tribune*, 30 September 2005.

[32] The best account of DNS governance, up to and including the creation of ICANN, is Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge: The MIT Press, 2002).

[33] See William J. Clinton, *Presidential Directive on Electronic Commerce: Memorandum for the Heads of Executive Departments and Agencies* (1997). This Presidential Directive was issued at the same time as the previously cited Clinton and Gore paper outlining a framework for electronic commerce.

[34] The data come from Marc Holitscher, *Die Regulierung des Internets zwischen technischer Koordination und politischer Steuerung: Eine explorative Einzelfallstudie am Beispiel der Internet Corporation for Assigned Names and Numbers zur Rolle privater Akteure in den internationalen Beziehungen*, PhD Dissertation, University of Zürich, 2004.

[35] On the European Commission's role in this process, see Volker Leib, 'ICANN-EU can't: Internet governance and Europe's role in the formation of the Internet Corporation for Assigned Names and Numbers,' *Telematics and Informatics*:19 (2002): 159-71.

[36] Interview with ITU official involved in issues of domain name governance.

[37] See Mueller, 'Ruling the Root,' 88.

[38] See, for example, Daniel J. Paré, *Internet Governance in Transition: Just Who is the Master of this Domain?* (Boulder: Rowman & Littlefield, 2002) for an account of the British case.

[39] Data from Matthew Zook, [Available Online] UC Berkeley and Zooknic [cited 2001]; Available from http://www.zooknic.com/Domains/international.html.

[40] Data from Matthew Zook, [Available Online] UC Berkeley and Zooknic [cited 2001]; Available from http://www.zooknic.com/Domains/market.html,

[41] Declan McCullagh, 'U.S. to retain control of Internet domain names,' [Available Online] *CNET News* [cited June, 2005]; Available from http://news.com.com/U.S.+to+retain+control+of+Internet+domain+names/2100-1028_3-5770937.html.

[42] Declan McCullagh, 'U.S. reaches Net detente with U.N.,' [Available Online] *CNET News* [cited November, 2005]; Available from http://news.com.com/2100-1036_3-5955245.html.

[43] 'ICANN's New MoU: Old Wine in a New Bottle,' [Available Online] Internet Governance Project, [cited September 30, 2006]; Available from http://www.internetgovernance.org/news.html#ICANNoldwine_093006

[44] Mark Ward, 'Big push for Chinese net domains,' [Available Online] *BBC News* [cited March 3, 2006]; Available from http://news.bbc.co.uk/1/hi/technology/4767972.stm.

[45] For an overview of the history and politics of gambling regulation in the US, see Denise von Herrmann, *The Big Gamble: The Politics of Lottery and Casino Expansion* (Westport, CT: Praeger, 2002).

[46] Justin Berton, 'Online poker players face new Prohibition,' *San Francisco Chronicle*, 27 August 2006, A1.

[47] Shelley Emling, 'New law deals devastating blow: U.S. ban on money transfers hurt,' *The Atlanta Journal-Constitution*, 10 November 2006.

[48] Matt Richtel, 'Citibank Bans Credit Cards From Use in Web Gambling,' *The New York Times*, 15 June, 2002, C2.

[49] Jonathan Fowler, 'Antigua asks WTO to condemn U.S. ban on Internet gambling,' *Associated Press*, 24 June 2003.

[50] 'Antigua and Barbuda welcomes WTO ruling on challenge against US,' *BBC Monitoring Americas*, 31 October 2003.

[51] See 'Antigua beats odds: WTO confirms ruling against US on web gambling,' *Agence France Presse*, 10 November 2006, and Liz Benston, 'WTO ruling provides scope for U.S. online gambling ban,' *Las Vegas Sun*, 7 April 2005.

[52] Alan Beattie, 'Antigua hits at US over WTO ruling,' *Financial Times*, 20 February 2006.

[53] Stephen Foley and Julia Kollewe, 'US charges online gaming chief,' *The Independent*, 18 July 2006.

[54] 'Busted flush,' *The Economist*, 5 October 2006.

[55] 'Online gambling bosses forecast consolidation,' *Reuters News*, 3 October 2006.

[56] Eric Pfanner and Heather Timmons, 'U.K. seeks global rules for online gambling,' *International Herald Tribune*, 1 November, 2006.

[57] Huw Jones, 'McCreevy says no hope of pan-EU gambling approach,' *Reuters News*, 15 November 2006.

[58] On the rise of the regulatory state in Europe, see Giandomenico Majone, *Regulating Europe* (New York: Routledge, 1996) and Michael Moran, 'Understanding the Regulatory State,' *British Journal of Political Science* 32:2 (2002): 391-412. On other governments coming to terms with the Internet, see Taylor C. Boas, 'Weaving the Authoritarian Web: The Control of Internet Use in Non-Democratic Regimes,' in Zysman and Newman.

[59] See David Bach, Abraham L. Newman, and Steven Weber, 'The International Implications of China's Fledgling Regulatory State: From Product Maker to Rule Maker,' *New Political Economy* 11:4 (2006).