Growing Up: The Maturing of the Internet and the Implications for Internet Governance

Peng Hwa Ang*

Abstract: This paper aims to sketch a road map for Internet governance based upon the state of development of various aspects of the Internet. The framework for analysis was developed by Deborah Spar in her 2001 book *Prophets, Pioneers, and Pirates*, in which she convincingly demonstrates that new technologies go through four phases of policy development: innovation, commercialization, creative anarchy, and rule-making. The analysis suggests that Internet governance for three of four clusters has reached a level of maturity in policy development. The most developed aspect is the cluster of issues around physical infrastructure or what has been described as the ICANN issues. Two other clusters—Internet use and Internet-related issues—are less developed, with their state of development linked to economic advancement. The least developed aspect of Internet governance is that of the use of the Internet for economic, social, and cultural development. The analysis suggests that development aspects of Internet governance should perhaps not be addressed in the current framework but should be discussed separately, with, however, the same level of importance attached to this venue as to the Internet Governance Forum.

Keywords: Internet governance, Internet regulation, Internet policy development, ICT4D.

INTRODUCTION

This paper aims to sketch a road map for Internet governance based upon the state of development of various aspects of the Internet. The idea is that as the Internet evolves, it will need a more stable state of governance. That is, new rules will be needed to regulate this new technology that has now become a sphere of human activity.

* Peng Hwa Ang is the Director, Singapore Internet Research Centre, and Professor, Wee Kim Wee School of Communication and Information, Nanyang Technological University.

Manuscript received October 20, 2009; out for review November 1, 2009; review completed December 1, 2009; accepted December 10, 2009.

The Korean Journal of Policy Studies, Vol. 24, No. 2, 117-132 (2009)

The central framework for the analysis is derived from Debora Spar's book *Pirates, Prophets and Pioneers* (2001), in which she demonstrates convincingly that when new technologies emerge, they create markets that, at least at first, have no rules and are run by what she calls "pirates." Over time, however, the pirates acquire wealth and property through the technology, and then they want to have rules in place to protect their interests.

Spar first applies her thesis to the case of Portuguese explorers in the fifteenth century. She argues that the development of "frontiers," as she calls them, begins with an innovation. This phase is marked by the presence of inventors, tinkerers, and enthusiasts. It is the "sexiest" (Spar 2001, xix) of the phases because it is marked by exciting imaginations and dreams. Commerce is absent because commercial uses for the technology have not appeared. So business ignored the telegraph and radio at first, seeing them as playthings or else too complicated for public use. Similarly, the Internet was seen as a technology suitable only for academic use; its potential for mass market use was initially ignored.

The lack of mass appeal explains the lack of necessity to regulate the technology. Spar sums up the situation thus:

> During this first phase there are no rules because none are needed: technology hasn't developed to the point where property rights are critical; there are no questions yet of access or unfair competition; and the societal impact of the new technology is minimal. Indeed, because the technology is still so experimental at this stage and confined to such a small group of users, there simply will not be many people outside this community who either understand the technology or have any concerns about its use. (Spar 2001, xx)

This pioneering phase is peaceful but often ends abruptly when the technology leaves the laboratory. Then, commercialization enters the picture as business people see how the technology may be profitable in the marketplace. In this phase, the technology is still ahead of the authorities. This potential for profit combined with anarchy draws more people, and a scramble ensues:

> Speed is essential during this phase, as is a certain ability to see beyond the confines of established business practice. Not surprisingly then, most of the pioneers who rush along the technological frontier are young. Marconi was twenty when he brought his blackbox to London. Marc Andreessen was twenty-three when he founded Netscape. (Spar 2001, xxi)

Fortunes are made and lost. For the Internet, that happened with the dotcom bust of 2000. It was a scenario that resembled that of the printing press in Europe soon after

the Gutenberg press was invented. Many who went into the printing business then failed (Ang and Dewar 2002).

This second phase does not last long. It gives way to the third phase, which Spar calls "creative anarchy." Those who have made their fortunes from the technology soon discover that the very anarchy that enabled them to make their fortunes is also destabilizing their businesses. The technology is maturing and the market is growing; but technical standards and rules for property rights and fair competitive play are not in place. This is the phase with the most frustrations. These frustrations, however, are critical to the development of the use of the technology because they highlight the cost of anarchy. The frustrations inevitably boil over and yield to the fourth phase, rule-making:

> When a technology is new, it usually looks so radical, so untameable, that those closest to its creation can't conceive of it being governed. This is particularly true—as with oceanic trade, radio or cyberspace—when the technology reveals a space that, for practical purposes at least, hadn't been there before. How could anyone in Europe ever hope to impose order on the vast and unruly seas? How could anyone own the air? Or patrol the reaches of cyberspace? During the innovation and commercialization phases, the very idea of governance seems absurd. (Spar 2001, xxv)

Spar (xxv) argues that although governments and societal groups sometimes clamor for rules, it can be said that the rules are promulgated at the instigation of "prophets" in the private sector.

In sum, the four phases may be characterized as follows:

- Phase 1: the pioneer creates the technology.
- Phase 2: the entrepreneur popularizes the technology.
- Phase 3: the "pirates" fight to maintain their business and keep others away.
- Phase 4: the "prophets" call in government regulators.

The four phases described above fit very well with the trajectory development of the Internet and the policy-making around it. At first, the Internet was restricted to military and academic use. In the early 1990s, it became publicly available. Soon, it was proclaimed a new medium independent of law, a claim that will be investigated in some detail below. In 1995, Netscape made its initial public offering of shares and made multimillionaires of its investors at a time when its revenues were negligible. That led to the equivalent of a land grab in cyberspace. In April 1999, a survey by *Wired* magazine found that of 25,500 standard dictionary words, only 1,760 had not been registered as a dotcom name (McCullagh 1999). Meanwhile, there were rumblings about the governance of the Internet, and in 2005, the Working Group on Inter-

net Governance, appointed by the UN secretary general, released its final report recommending the establishment of the Internet Governance Forum.

What predictions can be made, based on Spar's model, for the future of Internet governance? The next section of this article addresses that question.

THE RISE OF INTERNET GOVERNANCE

Some history is necessary to appreciate the development of Internet governance. In the early days of the Internet, there was speculation that it was beyond the reach of governments to regulate. Johnson and Post (1996) have given what may be considered as the best example of what has been called Scholarship 1.0 (Engel 2002). Just as the first versions of software tend to be flawed, so was Johnson and Post's attempt to outline the development of law of the Internet. Johnson and Post predict that the Internet will generate new laws that are separate from current laws that are based on geographical territory. In a more recent work, they have adopted a similar stance on how goods created in virtual worlds should be handled, arguing that a separate set of rules should be created for virtual worlds (Johnson and Post 2006). Such a position was effectively rebutted by Easterbrook (1996) who pointed out that there is no "law of the horse" in the physical world. Easterbrook observed that general principles from sound law should apply to the Internet, in the same way that general principles of law applied to the use of the horse. Just as there is no separate "law of the horse", so there should be need for a separate law of the Internet.

The most popular lay rendition of the idea that the Internet is separate from the offline world may be found in John Perry Barlow's *Declaration of the Independence of Cyberspace* (1996). It was a bold proclamation made on February 8, 1996, one day after the Communications Decency Act was signed into law in the United States. Within nine months of his pronouncement, some 40,000 sites had carried the Declaration and a virtual court had been set up. But the offline world was more dismissive of the Declaration. Larry Irving, assistant secretary of commerce in the Clinton administration, who was tasked with promoting the Internet for economic development, observed that the absence of rules could "slow down the growth of what is likely to be a major boon for consumers and business" (Yang 1996).

While agreeing with Barlow that the Internet would transform society, *Economist* magazine called his utopian view "absurd: just another example of the 1990s hype that produced the dotcom boom and bust" (2003). Barlow himself seems to have come around to the view that his Declaration was unrealistic. When he was asked in a recent magazine interview if he had sounded a lot more optimistic in the early 1990s, "with a

much more 'nothing can stop us now' attitude," he replied: "We all get older and smarter" (Doherty 2004, 5). More recently, Barlow's Declaration has been criticized for "contradictions and misdirections: newness is rooted in history; revolution is effected by commercial transaction; and liberal democracy becomes libertarianism" (Morrison 2009, 53).

Nevertheless, some still cling to the mistaken notion, literally of the previous century, that the Internet is impossible to regulate and should be left that way. Three points are made in Barlow's 850-word Declaration that are relevant for Internet governance and still believed and even advocated by some: (1) globalization by the Internet makes it difficult for governments to regulate, (2) where technical experts agree and lead, governments will follow, and (3) globalization enhances the power of nonstate actors (Morrison 2009).

All three statements have a kernel of truth in them, but they cannot be taken at face value. First, governments have demonstrated that they are able and willing to collaborate when there is agreement that there is harm being perpetrated on its citizens via the Internet—for example, in cases of child pornography and consumer fraud. There have been simultaneous multicountry raids on the homes of purveyors and consumers of child pornography (Ang 2005). As this article was being completed, the European police agency Europol reported that Operation Typhoon, a two-year, 19-country operation, had led to the arrest of 115 people for child pornography offences (BBC 2009). In the area of consumer fraud, there are annual sweeps of the Internet coordinated by the International Consumer Protection and Enforcement Network (http://www.icpen.org), a network of consumer protection and law enforcement agencies of more than more 40 countries and regional groups. There are costs in running such a network, just as there would be other costs if there were no such network. The important point is that it is possible for governments to collaborate if they agree that there is harm.

Barlow asserts that where technical experts agree and lead, governments will follow, and it is true that on technical matters, the experts will have to lead. But it is not true, as may be mistakenly extrapolated, that the opinions and advice of technical experts are necessarily decisive, even on highly technical matters. There are examples of superior technical standards being overtaken by other functional but inferior standards for various reasons. The defeat of Sony's Betamax standard by Matsushita's VHS standard is a textbook illustration (Lardner 1987). The current Internet Governance Forum under the auspices of the United Nations shows that governments will not easily relinquish their role as regulators in significant areas of human activity.

Barlow is on target when he asserts in his third point that the power of nonstate actors is rising at the expense of the power of governments. For the most part, governments have been willing to let nonstate actors have a role in the development of the

Internet. The dotcom boom and bust have shown the importance of the private sector not only in running for-profit enterprises but also in rule-making and enforcement. Service providers such as Yahoo, Google, and Amazon, for example, comply with the laws in Germany and France not to sell Nazi memorabilia (Ang 2005). Nonprofit and civil society groups in turn have a role to play in the development of the Internet to ensure, for example, that the concerns of those overlooked by the private sector are taken care of. Gender, poverty, and economic and social equity are some of the issues that fall more naturally into the ambit of such groups. The importance of both the private and civil society sectors in Internet governance has been recognized in the final report of the Working Group on Internet Governance (2005).

It is possible to argue that it is the governments who delegate some of their power to these nonstate actors. That argument is at best a legal fiction. The lesson is that governments cannot be the primary actors on the Internet governance stage. The governance of the Internet is now in the hands not only of governments but also of nonstate actors.

KEY ACTORS

States are still the primary actors in Internet governance, but not the only actors. Chief among the reasons for this is the intent of the United States government, which has dominance over the Internet, to have greater private sector involvement in the running and governance of the Internet. Even under the Democratic Clinton administration, Ira Magaziner, then senior advisor for policy development, who later developed the e-commerce policy initiative, supported private-sector involvement:

> As the Internet grows up and becomes more international, these technical management functions should be privatized, and there should be a stakeholder-based, *private international organization* set up for that technical management" (Magaziner 1999; emphasis added).

The innovation in the governance process is the multistakeholder approach, which had been mentioned many years before but was more formally reported by the Working Group on Internet Governance. In its final report, the Group (2005) called for a multilateral (many countries) and multi-stakeholder (government, private sector, and civil society) approach to Internet governance. This thread runs throughout discussions on how Internet governance should be informed.

In theory, such an approach would be highly inclusive and would afford opportunities to discuss significant issues and, more importantly, to bring out the best ideas and

practices to resolve them. After all, it would be democratic and would allow the maximum of participation. In practice, there are many problems to be overcome to reach that ideal stage, beginning with issues of legitimacy and representation. The private sector may consider business associations to be representative. But civil society groups do not have so ready a response. Invariably, questions of "whom do you represent?" have cropped up in meetings on Internet governance that this author has attended. By definition, membership of civil society groups tends to be open; that is, anyone who is sufficiently interested in the mission and activities of the group pays the requisite fees and joins. Business groups have the profit motive as a single common issue that all groups can subscribe to. In contrast, the diversity in the interests of civil society groups means that it is difficult to coalesce their wide-ranging interests into a single overriding umbrella issue.

It seems that the appearance of civil society groups on a governance stage changes the question that can be asked of representation. Taken together, civil society groups do not represent any one distinct constituency. Instead, each group acts to further the interests of its membership. In the case of Internet governance, it means that civil society as a grouping may not represent, say, the marginalized, or children, or the disabled, but it raises their concerns. In that way, the quality of discussion and debate rises with the addition of civil society into the governance process.

Civil society can play the role of an *amicus curiae* (friend of the court) who helps the judge make better sense of a complicated case. But the analogy goes only so far. The amicus curiae in a legal process is an impartial contributor to the case and has no decision-making power. In the Internet governance process, civil society groups highlight problems that should not be overlooked. The solution to these problems may conflict with the interests of business and government. The conflict with business is readily evident: the issues highlighted by civil society groups tend to be social in nature, the very type of issues that tend to be overlooked in the commercial logic of business. Conflicts between civil society and government are more complex. Governments are supposed to protect citizens' interests. But there may be conflicts with civil society groups in terms of prioritizing those interests in the face of limited resources. Then there may be conflicts at the operational level of the bureaucracy. That is, while the cabinet may approve a plan, mid-level officials at the local or national level may get in the way of implementing it.

At the international level, therefore, it is understandable that a private international organization would seem an attractive structural solution to the governance of critical Internet resources. Such an organization would not be commercial in nature and so would avoid the problems of being a commercial organization. But it would not overcome the twin issues of legitimacy and representation and perhaps the additional mat-

ter of efficacy for the following reasons.

On paper, such a private international organization would have the sole task of advancing the interests of the use of the Internet. To his credit, Magaziner talks about having an international—as opposed to a U.S.—organization as the Internet becomes more international. Nevertheless, the question still arises: to what extent can technical decisions be made on purely technical grounds? The answer, as discussed earlier, is that technical decisions do not spring forth without nontechnical considerations and other (for want of a better word) political concerns. The word "political" is used here in the broadest sense of government and regulation.

If technical decisions cannot be made on purely technical grounds, then the issue of representation arises—the stakeholders will want to ensure that their respective interests are taken into account during decision-making. The problem with representation per se is that often enough, the representative may not be the most knowledgeable in contributing to the discussion and debate. Instead, the representative is more likely to be chosen based on factors such as diplomatic skills and rank in hierarchy. To that extent, representation as the most significant criterion for participation in a decision-making body undermines the efficacy of that body.

There is one other major obstacle in the path of an international organization set up to oversee the Internet. This is the issue of the power to police. By its very nature, international organizations do not have such power. In the end, they have to rely on existing enforcement authorities—specifically, the police—to enforce rules and regulations. In short, even from a structural (as opposed to operational) perspective, there are no easy solutions to governance issues. Instead, the above analysis of the role of various stakeholders highlights the importance of governments in the Internet governance process. Even from the perspective of new regulatory regimes, such as self-regulation, it can be argued that it is governments that empower these new regimes through delegation. That is, the Internet cannot regulate itself without government help. It is governments that have decided to delegate the power of regulation to the regulatory body; any government can, at any time, intervene in any self-regulatory regime and thereby directly regulate and enforce rules as it deems fit.

THE STATE OF INTERNET GOVERNANCE

Given the above, where does Internet governance stand, in view of the likely increase in regulation over time? This part of the article uses four broad Internet governance issues and Spar's (2001) four phases of development as a framework for understanding Internet governance policy formation.

The Working Group on Internet Governance (2005) identified four clusters of issues:

1. physical infrastructure, which covers ICANN-related issues such as Internet protocol (IP) addresses, domain names, and root zone servers,
2. use of the Internet, which includes such issues as spam, network security, and cybercrime
3. issues related to the Internet but with wider impact, such as competition policy, e-commerce, and intellectual property rights
4. the development aspects of the Internet

As described earlier, Spar (2001) sees new developments as going through four phases: innovation, commercialization, creative anarchy, and rule-making. Being able to pinpoint the phase of policy development will be helpful in determining the extent to which rule-making may successfully be used to help improve the regulatory environment and thereby spur further innovation and development.

Physical Infrastructure

The physical infrastructure of the Internet has reached the stage of rule-making. The Internet has been commercialized since 1995 and has seen explosive growth in the number of users since then (Frischmann 2001). So explosive has been the growth, with investors pouring funds into online ventures, that by the time of the first dotcom boom, there were fears that domain names based on English words would run out (Middleton 2000).

At the level of physical infrastructure, much of the Internet bypassed the "creative anarchy" phase because the architectural design required a central authority to assign unique IP addresses. There was a brief period during which someone did attempt an alternative Internet registry called AlterNIC (Diamond 1998). That experiment was very quickly halted. But it, along with the mushrooming of online ventures, highlighted the need for regulation. There was a bottom-up attempt by Internet users to come together to establish a governing body to "coordinate the administration of domain names and IP addresses" (Domain Name Handbook 2000). In the end, the governing body was taken over by the U.S. government with the formation of the Internet Corporation for Assigned Names and Numbers (ICANN).

Although the fiction is that ICANN does not make policy, there is recognition that its "coordination" will inevitably impinge on policy and rule formation. Vinton Cerf, one of the founders of the Internet, was quoted as saying, "In some sense, the policy issues surrounding the Internet are more important than the technological ones, and they're harder to solve" (Davis and Seib 2000, A1).

Use of the Internet

Policy issues related to Internet use are especially difficult. They can be divided into two categories based on whether they are directly or indirectly related to the Internet. In the first category are issues such as spam, network security, and cybercrime. Cybercrime is a broad category that encompasses a range of new mischiefs, such as cyberstalking and identity theft, that would not exist without the Internet. One reason for categorizing the issues in this way is to allow new approaches to rule-making concerning the Internet.

By new approaches is meant the emphasis on modes of regulation: instead of resorting to the use of legislation immediately, other modes should be attempted. Lessig (2006) has observed that there are four modes of regulation: legislation by government—including self-regulation, because that is a form of delegated governance; markets; social norms, including etiquette; and architecture, by which is meant the design of the environment. These four modes existed before the Internet. The novel element introduced by the Internet is the emphasis on self-help and community-based bottom-up regulation and governance, as opposed to the traditional reliance on government action. For example, self-regulation, which means regulation of industry by industry, is advocated as the preferred mode of regulation of Internet content (Ang 2005), because it allows for greater speed of action and is more responsive to an industry that changes quickly.

Lessig's (2006) major contribution is to point out that the design or architecture of a product or service can direct human behavior. He discusses the case of low bridges that are put across roads so that wealthy seaside residents can keep out buses that would otherwise bring visitors to the public beaches near their homes (Lessig 2006). Such architecture of a product or service could not be considered rule formation unless it was deliberately intended. Otherwise, by definition, every innovation by sheer fact of having been created would be rule-making.

Looking at the mischiefs surrounding the use of the Internet, it is arguable that there are large swathes of activities that are already being regulated. The Council of Europe promulgated the Convention on Cybercrime (2001), which was signed and ratified by the United States to take effect on January 1, 2007 (Espiner 2006). Because the Convention takes into account some of the cultural differences that exist even among countries in Europe, and because the law is in force in the United States, it is expected that more countries will ratify it.

The Convention is the world's first treaty on crimes committed using the Internet and other computer networks. It has an Additional Protocol that covers "acts of a racist and xenophobic nature committed through computer systems" (Council of Europe

2003). The Convention sets up processes to handle offences both domestically and internationally. Substantively, it addresses computer-related fraud, child pornography, copyright infringements, and network security violations such as illegal access. It does not, however, deal with all cybercrimes; for example, it does not address cyberstalking or identity theft. As of December 2009, 46 countries had signed the Convention, and 26 had ratified it (Council of Europe 2009). Still, many countries are left out. Further, because not all offences that are committed using the Internet are captured by this international treaty, the rule-making in this area only goes part way, as reflected in table 1 below.

Internet-related Issues

A similar situation exists for Internet-related issues that have a wider-ranging impact. Into this cluster fall a host of issues such as intellectual property rights, competition law, e-commerce, and e-government applications. This cluster contains a complex mix of offline and online issues. This means that any resolution of the online regime must also consider the extant offline regime. For example, in order for e-commerce to be possible, the law must be amended to admit electronic evidence. That is, the law must specify under what conditions the evidence from an email may be admitted in a trial. Such an amendment would benefit not only cases involving the Internet but also cases involving computers in general (Ang 2005). Similarly, competition law to foster a more competitive environment for the Internet will have an impact on non-Internet businesses as well.

From this perspective, therefore, it should be evident that some rules are being made in the cluster area. For the most part, the rules introduced are intended to facilitate activities on the Internet while minimizing any impact offline. One legal example would be the liability of intermediaries on the Internet for third-party content. For example, book reviewers provide third-party content for Amazon.com. To what extent should Amazon be held liable for those reviewers' material if, for example, it violates copyright or defamation law? In the offline world, there is no question of affixing liability on the host of such content. Thus, a newspaper, magazine, television, or radio station would be liable for content that infringes on copyright or is defamatory. But merely transposing the offline law to the online world would impose an intolerable burden of inspection on the content hosts. Worse, it would expose an entire range of intermediaries—such as proxy servers and Internet service providers—to similar liability. It is therefore only sensible to amend the online rules to immunize content hosts from liability for third-party content with the proviso that the hosts act reasonably when the offending content is pointed out (Ang 2005). Interestingly enough, there is

no push to offer a similar form of limited immunity to media in the offline space.

In summary, the rapid diffusion and pervasive nature of the Internet has necessitated the promulgation of rules to facilitate its development. New rules, such as those that immunize intermediaries, and the amendment of extant rules, such as those governing electronic evidence, suggest that the model proposed by Spar may need some modification. In the cluster under discussion, rule-formation has happened rather quickly. In fact, some of the rules concerning electronic evidence and immunity were made in 1996, even before ICANN was established. Some suggestions for further research in this area are made below.

Development Aspects

Of all the issue clusters in Internet governance, the thorniest in practice is development. "Development" in this context means the use of the Internet for economic, social, and cultural betterment of less economically developed countries. The irony is that while development was the early driver of efforts to establish Internet governance, it has been the least discussed issue. This is evident from the references in the final report of the Working Group on Internet Governance (2005) to meetings in which most of the time was devoted to addressing issues around Internet resources. As table 1 sums up, development aspects are the least developed in Internet governance.

One of the reasons for this is that development is difficult if not impossible to commercialize. By their very nature, it is rarely possible to show a profit for development projects. After all, if there was profit to be made, private enterprise would be first in the queue. To be sure, there are many innovative ways that the Internet and other information and communication technologies can be used for development. Often, they are not intended to turn a profit, even though they may benefit the community at large, because in many cases the community cannot afford to pay for them.

And because there is no profit to be made, the rough-and-tumble creative anarchy that is present in the other clusters where commercial logic pervades is absent here. The issue of rule-making also does not arise because of the absence of contestation. It would appear that development aspects do not fit so easily into the Internet governance framework.

Summary and Suggestions for Further Research

Table 1 below summarizes the foregoing discussion. The four issue clusters are assessed in terms of the four phases of policy development. The first three clusters are well past the phase of commercialization and into the policy- and rule-making phase.

The "physical infrastructure" cluster is well on the way to maturity in policy development. The second cluster, "use of the Internet," needs further policy development as the international cooperation it requires currently extends to a limited number of countries and a limited number of issues. The third cluster, "Internet-related issues," has also reached a sophisticated level in policy development, although this cannot be said to apply to less developed countries. From discussions and conversations with officials from South and Central Asia and parts of the Middle East and Africa, it is clear that much work lies ahead. This may be a form of digital divide in that it is only through addressing a number of the key Internet-related issues that it is possible to develop the use of the Internet.

In the "development aspects" cluster, Spar's four-phase framework (innovation, commercialization, creative anarchy, and rule-making) does not fit as well. Because development is often not susceptible to commercial logic, it may be that this framework is not suitable for discussing it. However, it is also worth considering the possibility that development issues should addressed separately from other Internet governance issues. Their uneasy fit may explain why development is often treated as a stepchild in Internet governance discussions. Even the Digital Solidarity Fund has received very little funding support. Its 2009 budget was 2.7 million Swiss francs, or about US$2.7 million (Digital Solidarity Fund Foundation 2009).

The advantage of taking development out of the Internet governance discussions and therefore out of the Internet Governance Forum is that it would not be treated as a stepchild. As the subject matter is important, it should be given due attention in a separate forum similar in importance and recognition to the Internet Governance Forum. A possible disadvantage of this approach is that because the Internet Governance Forum is such a high-profile event, moving development out of it could lead to an erosion of its status and recognition. As development was one of the motivations behind the rise of Internet governance concerns, this is a radical notion that should be further researched.

Table 1. Internet Governance and the Four Phases of Policy Development

	Innovation	Commercialization	Creative anarchy	Rule-making
Physical infrastructure	X	X	X	X
Use of the Internet	X	X	X	X
Internet-related issues	X	X	X	X
Development aspects	X			

CONCLUSION

Governments cannot be excluded from the Internet governance process. This may seem obvious, but there continue to be those who argue in favor of a mostly, if not purely, bottom-up and community-driven approach to Internet governance. This article has shown that this is not possible or even desirable.

Adopting the above position does not mean that governments have the sole role, or even a majority role, to play in Internet governance. The private sector and civil society have roles to play, as has been highlighted in the final report of the Working Group on Internet Governance (2005). The private sector, with more readily available financial resources, is playing a major role at the international level in Internet governance. Civil society groups have some way to go. These roles, however, are permitted and even encouraged by governments because of the pace of technological advancement. It is just not possible for the law to keep pace with the rapid development of technology.

Perhaps more importantly, it is possible to use different modes of regulating the Internet. This enables greater flexibility in Internet governance, thereby preserving the ability to adapt to technological change while providing sufficient stability for widespread use. The different modes of regulation may also portend the regulation of all things in the future.

Different areas of Internet governance are in different states of policy development. The developed countries, particularly those that have signed the Council of Europe's Cybercrime Convention, are well on their way to maturity in the policy development phase of the Internet. Less developed countries will not only have to address cybercrime and other online afflictions but will also have to look at Internet-related issues that have wider offline implications.

Among the four clusters of issues in Internet governance, development aspects sit uneasily in the framework used above. It may be that the framework is not suitable. On the other hand, it may be that issues in development do not sit easily with Internet governance. This is such a radical notion in the light of the current global discussion that it must be thought through more carefully.

The framework used in this analysis does go some way to explain the trajectory of Internet policy development. Perhaps the Internet developed more quickly than earlier technological innovations, but rules governing it have been developed very quickly too. However, there are still gaps, and so the need for rule-making continues.

REFERENCES

Ang, P. H. 2005. *Ordering chaos: Regulating the Internet.* Singapore: Thomson.

Ang, P. H., and J. Dewar. 2002. Back to the future of the Internet: The printing press. In R. Mansell, R. Samarajiva, and A. Mahan (ed.), *Networking knowledge for information societies: Institutions and intervention*, 249-53. Delft, Netherlands: Delft University Press.

Barlow, J. P. 1996. *A declaration of the independence of cyberspace.* http://homes.eff.org/~barlow/Declaration-Final.html.

BBC. 2009. Europol announces arrests of 115 "child sex offenders." December 10, 2009. http://news.bbc.co.uk/2/hi/europe/8407093.stm.

Council of Europe. 2001. *Convention on cybercrime.* http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

Council of Europe. 2003. *Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.* http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm.

Council of Europe. 2009. *Convention on cybercrime: CETS No. 185.* http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

Davis, B., and G. Seib. 2000. Policing a wildfire: Technology will test a Washington culture born in Industrial Age. *Wall Street Journal*, May 1.

Diamond, D. 1998. Whose Internet is it, anyway? *Wired*, April. http://www.wired.com/wired/archive/6.04/kashpureff.html.

Digital Solidarity Fund Foundation. 2009. *Budget proposal 2009.* http://www.dsf-fsn.org/cms/documents/en/pdf/members/CF_Doc_007_09_en.pdf.

Doherty, B. 2004. John Perry Barlow 2.0: The Thomas Jefferson of cyberspace reinvents his body—and his politics. Reason, August/September. http://reason.com/archives/2004/08/01/john-perry-barlow-20.

Domain Name Handbook. 2000. *International forum on the white paper.* http://www.domainhandbook.com/ifwp.html.

Easterbrook, F. H. 1996. Cyberspace and the law of the horse. *University of Chicago Legal Forum* 207.

Economist. 2003. Digital dilemmas. January 23.

Engel, C. 2002. Organizing co-existence in cyberspace: Content regulation and privacy compared. Max Planck Institute Collective Goods Preprint No. 2002/12. papers.ssrn.com/sol3/papers.cfm?abstract_id=325360.

Espiner, T. 2006. U.S. joins European cybercrime convention. *CNET News*. http://news.cnet.com/2110-7348_3-6121760.html.

Frischmann, B. 2001. Privatization and commercialization of the Internet infrastructure: Rethinking market intervention into government and government intervention into the market, *2 Columbia Science & Technology Law Review 1*. June 8. http://www.stlr.org/cite.cgi?volume=2&article=1.

Johnson, D. R., and D. G. Post. 1996. Law and borders: The rise of law in cyberspace. *Stanford Law Review* 48: 1367.

Johnson, D. R., and D. G. Post. 2006. The great debate: Law in the virtual world. *First Monday*, February 2-6. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1311/1231.

Lardner, J. 1987. *Fast forward: Hollywood, the Japanese, and the onslaught of the VCR*. New York: Norton.

Lessig, L. 2006. *Code: Version 2.0*. New York: Basic Books.

Magaziner, I. 1999. Creating a framework for global electronic commerce. *Future Insight*, July. http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomic commerce.html.

McCullagh, D. 1999. Domain name list is dwindling. *Wired*, April 14. http://www.wired.com/science/discoveries/news/1999/04/19117.

Middleton, J. 2000. Dotcom domains are running out. *VNU Business Publications*, August 9. http://www.v3.co.uk/other/news/2047425/dotcom-domains-running.

Morrison, A. 2009. An impossible future: John Perry Barlow's "Declaration of the independence of cyberspace." *New Media Society* 11(1-2), 53-71.

Spar, D. L. 2001. Pirates, prophets and pioneers: Business and politics along the technological frontier. London: Random House Business.

Working Group on Internet Governance. 2005. *Final report*. Bogis-Bossey, Switzerland.

Yang, C. 1996. Law creeps onto the lawless Net. *Business Week*, May 6, 58-64.