Center for Internet and Society
at Stanford Law School

The Berkman Center for Internet & Society
at Harvard Law School

Research Publication No. 2005-16
Fall 2005

Beyond Internet Governance: The Emerging International Framework for Governing the Networked World

Mary Rundle

JEL Classification: F020, K330, O300

BEYOND INTERNET GOVERNANCE: THE EMERGING INTERNATIONAL FRAMEWORK FOR GOVERNING THE NETWORKED WORLD

Mary Rundle*

ABSTRACT

Increasingly, governments are regulating the "Net" – that is, the Internet and people's activities over it. Because the Net is global in nature, governments are turning to intergovernmental organizations to iron out common approaches. Taken together, these international Net initiatives foray into all areas of government traditionally dealt with by domestic regimes – addressing foreign commercial relations, jurisdiction, infrastructure, security, monetary authority, property, relations between private parties, and citizenship.

In agreeing to participate in these federated, power-sharing arrangements, governments are gradually constructing an entire framework for governing the networked world. Given the importance of these rules for the future, those who hold freedom dear must work to build democratic values into this emerging international system.

Keywords: Internet governance, integration, international federalism, networked world, Tunis Agenda

* Mary Rundle is a Fellow at the Berkman Center for Internet and Society at Harvard Law School and a Non-Resident Fellow at the Center for Internet and Society at Stanford Law School. This paper was produced under the Net Dialogue project, which seeks to shed light on international Net governance and help bridge the technology and international policymaking communities.

BEYOND INTERNET GOVERNANCE:

THE EMERGING INTERNATIONAL FRAMEWORK FOR

GOVERNING THE NETWORKED WORLD

Mary Rundle

Table of Contents

FOREWORD

The Tunis Phase of the World Summit on the Information Society in November 2005 formally brought to a close an international process begun seven years earlier to consider challenges and opportunities posed by the Internet. With approximately 19,000 people attending that Tunis meeting, there were naturally a multitude of views on what constituted the most pressing issues. At the Summit's conclusion, governments endorsed the *Tunis Agenda for the Information Society*.[1] Rather than finishing the dialogue, this negotiated document marks the end of the beginning of a process.

As part of this Tunis Agenda, governments agreed to set up an Internet Governance Forum, mandating it, among other tasks, to:

- "Discuss public policy issues related to key elements of Internet Governance…;"
- "Identify emerging issues…;"
- "Discuss, *inter alia*, issues relating to critical Internet resources;" and
- "Help to find solutions to the issues arising from the use and misuse of the Internet…"

While called the "Internet Governance Forum," the Forum's mandate goes well beyond the "Internet" (i.e. the technical core of the network of networks) and includes a much broader set of issues – and so extends to governance of the networked world.

Just what are these issues, specifically? When looking at topics listed in the Tunis Agenda, it is clear the conception includes the topics of cybercrime, spam, privacy and the protection of personal data, e-business, digital divide and opportunity, human rights, and more.

Although the list of relevant issues would appear boundless, it does not defy categorization. In fact these topics may all be viewed as falling under the same, basic areas that governments have dealt with throughout history – only here in the context of the Net.

What is new, and the reason there has been so much attention to WSIS, is the powerfully integrative force of the Net. This force brings the world to a level of integration never before experienced. Ready or not, the networked world has begun.

[1] Document: WSIS-05/TUNIS/DOC/6(Rev.1)-E, 15 November 2005.

INTRODUCTION

The Net – here meaning the Internet and people's activities over it – is becoming an increasingly controlled medium. Driving this regulation are two predominant forces: people desiring certainty in their online activities, and governments striving to exercise sovereignty over this space.

Control of the Net is accomplished through technological and legal means. Software and hardware act as "code," determining what happens to information. For example, through code it is possible to monitor a person's movements, including where he goes with his cell phone, what web sites he visits, what he expresses in email, and what purchases he makes using a credit card. Law in turn can dictate the choice of code, and what uses of information technology are permitted or prohibited. In this way, code and law combine to regulate the Net.

As a country considers its role in steering the Net, it has four main choices vis-à-vis other countries:

1. Assert sovereignty over the whole of the Net;
2. Abdicate any claim to sovereignty over the Net and agree to some form of supranational governance;
3. Assert sovereignty over a specific territory of the Net ("zoning"); or
4. Agree to participate in a federated, power-sharing arrangement that entails a combination of zoning and supranational governance.

For the most part, countries today are choosing the fourth option, as they attempt to maintain sovereignty over some areas of the Net but concede the need to cooperate and share power to an extent.

To work out compromises in specific areas, governments have used the settings of pre-existing intergovernmental institutions that are specialized in the fields at issue. For example, they have treated electronic commerce (e-commerce) in the World Trade Organization (WTO), and electronic banking (e-banking) in the Basel Committee on Banking Supervision (BCBS). In fact, governments have drawn on more than a dozen intergovernmental bodies to iron out rules for a seamless, networked world.

Taken together, these international Net initiatives foray into all areas of government traditionally dealt with by domestic regimes. For example, to provide a backstop for *people's interactions with each other*, governments have established guidelines for consumer protection and have set standard legal terms for electronic contracts; they have provided certain intellectual property protections in cyberspace as well to help define *property rights*. To manage relations on a more macro level, they have negotiated in the areas of *foreign commercial relations* and *jurisdiction.* Finally, to provide a stable and secure Net environment, they have partnered with industry in the areas of *infrastructure*, *security*, and *monetary authority*. The one area of governance that presents perhaps the most difficulty for international arrangements is that of citizenship, or the *relation between a person and the state* in the networked world.

> *Governments have drawn on more than a dozen intergovernmental bodies to iron out rules for a seamless, networked world. Taken together, these international Net initiatives foray into all areas of government traditionally dealt with by domestic regimes.*

Ironically, as governments have attempted to hammer out Net rules on an "as needed" basis only, they have permitted the incremental accumulation of governance functions at the international level. Though almost imperceptible, the ad hoc expansion of these initiatives points toward an entire international governance framework for the networked world.

While impressive in scope, this emerging international regime lacks fundamental mechanisms to prevent government overreach and to safeguard liberties. Instead of reflecting an intrinsic distrust of the accumulation of power, the invisible regime is more a celebration of that power. Notably absent are assurances of subsidiarity,[2] checks and balances,[3] accountability to the public, and effective protections for fundamental freedoms.

Adding urgency to this situation is the difficulty of reversing internationally agreed rules and of rewriting computer code once embedded in the Net's architecture…

Of course, people should not expect that a single country's constitutional arrangements would guide the process of international decision-making or the substance of what is decided. Still, people would hope that the rights they have come to expect, and the limits on government they have taken as firm, would remain true in this networked world.

Adding urgency to this situation is the difficulty of reversing internationally agreed rules and of rewriting computer code once embedded in the Net's architecture. Acting first and asking questions later does not serve well in the construction of a global framework to govern the networked world. Since computing will soon be integrated into the environment so that the distinction between the real and virtual worlds disappears, the time is now to ensure a sound foundation.

The sections that follow set out a broad-brush overview of international Net governance from a political-economy perspective. Categorized according to traditional functions of government, the sections explore challenges posed by cyberspace and international initiatives to address them.[4] The paper concludes with a summary of some of the democratic shortcomings of this emerging system and turns to consider practical responses that take into account the intersection of technology and the law.

[2] "Subsidiarity" here refers to the principle of making decisions at the most local level feasible.

[3] As explained on Wikipedia, "In a system of government with competing sovereigns (such as a multi-branch government or a federal system), 'checks' refers to the ability, right, and responsibility of each power to monitor the activities of the other(s); 'balances' refers to the ability of each entity to use its authority to limit the powers of the others, whether in general scope or in particular cases." The phrase "checks and balances" was coined by the French political thinker Montesquieu (Charles-Louis de Secondat, Baron de La Brède et de Montesquieu, 1689 - 1755), whose ideas have been implemented in many constitutions throughout the world. (Wikipedia entry as viewed on December 13, 2005.)

[4] More information on these initiatives and the organizations behind them is available at http://www.netdialogue.org.

GOVERNMENTS FACILITATING PRIVATE INTERACTIONS

When people began transacting over the Net on a wide scale in the 1990s, they found themselves wishing for the same sorts of legal certainties they enjoyed in the real world. Because dealings often carried an international dimension, countries needed to cooperate in order to present parties with a predictable framework for e-commerce. Thus, governments undertook to provide their citizens with international contractual guidance and collaborated in the name of consumer protection and intellectual property protection.

These Net governance developments may be seen as networked world versions of the traditional governance functions relating to "Relations Between Private Parties" and "Property."

- **Relations Between Private Parties**

One of the functions of government has traditionally been to provide a legal backstop for people's interactions with each other. The area of law most closely associated with this governance function is that of contracts and torts, where contracts entail what parties bargain for and torts involve unforeseen circumstances.

Over centuries, contract law has evolved so that certain conventions apply: for example, what constitutes an offer and acceptance, what is a valid signature, and what constitutes performance. So, too, people have had a general sense of which system of law provided the backdrop to their relationship. These characteristics have afforded people a fair degree of certainty in the traditional world.

The Net, however, challenges this sense of confidence. For example, to date it has been difficult for people to verify each other's identities when contracting in cyberspace. Persons harmed by unforeseen cyber events (e.g., denial of service) may find themselves at a loss for recourse. At the same time, people often have scant assurance as to which legal regime will provide a definitive backstop for their relationship. These examples illustrate some of the ambiguities people encounter in their online interactions.

To add clarity for people wishing to contract internationally over the Net, governments have worked through the United Nations Commission on International Trade Law (UNCITRAL) and have agreed on a *Convention on the Use of Electronic Communications in International Contracting*[5]:

> Aimed at enhancing legal certainty and commercial predictability where electronic communications are used in relation to international contracts, the provisions of the convention deal with determining a party's location in an electronic environment; the time and place of dispatch and receipt of electronic communications; and the use of automated message systems for contract formation… The new convention will assure companies and traders around the world that contracts negotiated electronically are as valid and enforceable as traditional paper-based transactions.[6]

From the point of view of facilitating e-commerce, this initiative is important as it will establish uniform legal terms for e-contracts. As such, parties engaging in

[5] UNCITRAL sent the *Draft Convention on the Use of Electronic Communications in International Contracting* to the Sixtieth UN General Assembly in the fall of 2005, where the Sixth Committee (Legal) approved the draft text (Document A/60/17, Annex).

[6] UNCITRAL Press Release announcing the decision to forward the draft Convention to the UN General Assembly for adoption, 15 July 2005.

business will face fewer uncertainties and enjoy lower transaction costs.

On a systemic level, the initiative is highly significant because it marks a deepening in the degree to which countries are harmonizing their laws. Earlier UNCITRAL initiatives in e-commerce have taken the form of "model" laws (which signatories could choose to emulate in domestic legislation). This instrument goes much further in that signatories commit to recognizing the same package of terms in contract law.

> *From the point of view of facilitating e-commerce, this initiative is important as it will establish uniform legal terms for international e-contracts.*

Of course, the UNCITRAL Convention does not cover every online interaction. For example, persons in the networked world will confront unforeseen events that they did not address through a contract. Judicial systems have commonly dealt with such situations in the real world by constructing an arrangement that reflects what the parties would likely have agreed among themselves, had they been able to negotiate beforehand. Or, even when individuals know in advance how they would like to define their relationship, the law may for some purpose step in and impose constraints, preventing these parties from negotiating completely freely between themselves.

A major point of contention in this area – and one that has proved thorny for multilateral agreement – concerns the ownership and control of personally identifiable information. Here, it is useful to recall that both technology and law affect the ownership and control of data: Technology enables the automated processing of personal data, while law can influence the choice of technology, and what uses of information are permitted or proscribed.

It is fairly well known among the public in industrialized nations that companies have been making a business of collecting and selling people's electronic profiles. There has been some debate as to whether such information is tradable or entails something akin to inalienable personhood. For example, the European Union has argued for a personhood conception of personally identifiable information, while the United States has pushed for the notion that individuals may contract away rights to this data.[7]

The Organization for Economic Cooperation and Development (OECD) and the Council of Europe (COE) each foresaw the possibility of personal data being mishandled in the information age and developed rules in the early 1980s.[8] Together, these initiatives cover a number of concerns relating to personal data collection and processing. The OECD Guidelines seek to protect personal data through principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The COE Convention contains similar provisions and adds an anti-discrimination provision. Still, these instruments have not had the impact that some would hope, as the OECD principles are non-binding, and the

[7] To resolve this disagreement while still fostering commerce, in 2000 they reached the Safe Harbor Agreement by which different standards are applied, depending on the jurisdiction. While the United States allows business wider latitude in using personally identifiable information, the European Union has narrower rules but maintains a governmental claim to certain data. The two markets are large enough to allow those differences.

[8] OECD members adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. The Council of Europe adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS 108, in 1981. These organizations have adopted subsequent instruments to reinforce these principles.

signatories to the COE Convention are European only.[9]

> *For these OECD initiatives truly to reduce uncertainty for private parties interacting in cyberspace, they must be reinforced with a way for people to seek redress in the event of problems.*

OECD members together have continued to craft guidelines to respond to technological developments. For example, they drafted the *Guidelines for Consumer Protection in the Context of Electronic Commerce* and other texts to deal with threats to individuals in an increasingly connected world. Reflecting a more recent trend to shift some responsibility for security to computer users themselves, the OECD has offered a program called "Creating a Culture of Security" to provide guidance on this front.[10]

Of course, for these OECD initiatives truly to reduce uncertainty for private parties interacting in cyberspace, they must be reinforced with a way for people to seek redress in the event of problems. Partly to answer this call, governments in the 1990s began negotiating a *Future Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters* ("Judgments Project") through the Hague Conference. At the moment, negotiations for the treaty as initially envisioned have stalled.[11] If this treaty were to go through, however, it could provide a useful judicial arrangement[12] for the resolution of private, cross-border disputes relating to the Net.

Since technology has proved nimble in responding to problems to date, it will likely step in to resolve some of the challenges in private party relations even as law falters – for example by continuing to provide increasingly sophisticated reputation systems, spam filters, and the like.

- **Property Rights**

A clear system of property rights lets people know what is owned by whom and what options people have for using that property. Such a system is said to be essential for going about daily life in a society, for example by providing predictability for people conducting business or enjoying a public space.

Likewise, a clear property system is important for cyberspace. While a country may have its own domestic arrangement for protecting property rights, the Net opens the door for people elsewhere to make use of this property without necessarily observing these rights. On its own a government is limited in its means to address this problem and to ensure that its country's property system remains effective – hence, the need for an international approach.

To date most of the discussion on property in cyberspace has centered around digital copyright, which includes digital inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. Theoretically, governments grant intellectual-property ownership and usage rights to offer incentives for creativity

[9] Signatories include 38 European countries, 33 of which have ratified the Convention.

[10] Many technology experts contend that the best way to promote computer security is to target vulnerabilities where they lie – that is, with computer owners and software vendors, whose machines and products allow computer worms and viruses to spread.

[11] Due to difficulties in negotiations, the scope of this draft Convention has been dramatically reduced, with the narrower initiative now renamed the Hague Conference's *Draft Convention on Exclusive Choice of Court Agreements*.

[12] Still, a dispute would be brought to a national-level court, with an arrangement in place for other countries to honor that country's judgment. (The question then becomes, "Which country's law applies?" if disputing parties have not arranged this choice of law in advance contractually.)

and innovation, while ensuring that benefits accrue to the general public.

> *The WIPO Internet treaties require signatories to bolster intellectual property rights by granting legal protection to technologies that enforce these rights through computer code…*
>
> *One could say that policymakers are apt to underestimate the effect their rules have on technology, and the resulting effects then on society.*

Given the global nature of the Net, international collaboration appears the most obvious way to use the law to protect intellectual property and maintain an incentive system for creators in the digital environment. Governments have therefore turned to intergovernmental bodies to devise a system for recognizing and enforcing these property rights in cyberspace.

The "Internet treaties"[13] of the World Intellectual Property Organization (WIPO) translate traditional conceptions of copyright law into the digital realm. Some observers argue that the WIPO protections go further than domestic regimes had previously, in that they erode principles of "fair use" or "fair dealing."[14]

To help prevent the need for extensive litigation, the WIPO provisions favor technological tools for enforcement. Hence, in addition to projecting traditional conceptions of intellectual property law onto the Net, the WIPO Internet treaties require signatories to bolster intellectual property rights by granting *legal protection to technologies that enforce these rights through computer code* (e.g., digital rights management, or DRM, tools). These treaty clauses are known as the "anti-circumvention" provisions.

Though intended for purportedly good purposes, the anti-circumvention provisions have been criticized for crimping scientific innovation. Specifically, some countries implementing them have criminalized the creation of technologies that might possibly be used to circumvent DRM tools, even if their primary purpose involved other applications.[15]

If one were to generalize from the experience with the WIPO anti-circumvention provisions, developments in DRM technologies, and citizens' responses, one could say that policymakers are apt to underestimate the effect their rules have on technology, and the resulting effects then on society. By favoring some technologies over others and mandating computer scientists to build them into the Net's architecture, policymakers may inadvertently affect other areas when they intend to target one set of issues. In this governance area as with others, Net governance would be better served by increased dialogue among technologists and the drafters of international rules.

[13] The *WIPO Copyright Treaty* (WCT) and the *WIPO Performances and Phonograms Treaty* (WPPT) of 1996 together are referred to as the "Internet Treaties."

[14] As described on the Wikipedia website (as visited on 10 August 2005): "The fair use doctrine is an aspect of United States copyright law that provides for the licit, non-licensed citation or incorporation of copyrighted material in another author's work under certain, specifiable conditions. The term 'fair use' is unique to the United States; a similar principle, 'fair dealing', exists in some other common law jurisdictions…"

[15] The Electronic Frontier Foundation (http://www.eff.org) explains regarding U.S. implementation of WIPO commitments: "[T]he 'anti-circumvention' provisions of the Digital Millennium Copyright Act ('DMCA')… have not been used as Congress envisioned. Congress meant to stop copyright pirates from defeating anti-piracy protections added to copyrighted works... In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright piracy. As a result, the DMCA has developed into a serious threat to several important public policy priorities…"

GOVERNMENTS ATTENDING TO FOREIGN RELATIONS

When governments started encouraging e-commerce in the 1990s, they confronted the need to clarify how multilateral market-access commitments applied in the electronic realm. Suddenly, the Net opened channels for trade in an unprecedented way, enabling products delivered electronically to flow freely across borders.

Because countries had made certain commitments to let trade flow, new questions arose as to the degree to which a country had domestic dominion over what is acceptable Net content – and whether content regulations must yield to market access commitments in the event of a clash.

This evolution in Net governance may be viewed as involving the traditional areas of "foreign commercial relations" and "jurisdiction."

- **Foreign Commercial Relations**

As described above, governments have attempted to provide a predictable environment for people's international interactions over the Net. For large-scale, global e-commerce, these efforts would be meaningless without the broader promise of market access.

This aspect of e-commerce echoes the past: Throughout history, government has intervened in relations between persons in its territory and persons or governments elsewhere – particularly in commercial relations, where a government says it is looking after general economic and security interests. Typical intervention has included securing market access for exports, protecting domestic competition from imports, and collecting revenue in the form of customs duties or tariffs. Countries have sometimes agreed to accord each other market access, for example by committing to admit imports or by lowering tariffs. In recent decades, governments have bound themselves to such arrangements through the multilateral trading system – with agreements negotiated and administered today through the World Trade Organization (WTO).

The Net poses challenges for governments as they wrangle over how existing market access commitments apply in the digital era. One principle often cited in WTO discussions is that of "technological neutrality," which holds that market-access commitments apply regardless of the technology used in carrying out trade. In this light, this medium can be viewed as turning traditional market access on its head: Instead of the conventional dynamic of governments' taking down barriers to trade, products traded electronically can now stream across borders relatively undetected.

This medium can be viewed as turning traditional market access on its head…

With this effective opening for imports, governments must adjust to losses in tariff revenue[16] and to new competition facing domestic suppliers. To alleviate these pressures, they must emphasize the benefits of cheap imports and the potential of boosted exports; meanwhile, they must find the right balance in redistributing gains derived from e-commerce and must enable economic restructuring.

An obvious strain here will come from strong reactions by people in high-wage countries against services provided by people in low-wage countries via electronic means. While international e-commerce promises economic gains, it also ushers in serious political tensions as the ability to trade electronically gives rise to protectionist tendencies. From a free-trade perspective, if the global trading system is to

[16] Losses stem either from the moratorium on customs duties currently practiced by WTO members, or simply from the practical difficulties of collecting such revenue.

prevent entrenched interests from squelching new entrants in the networked world economy, it will need to rest on institutional capacity like that of the WTO's dispute settlement system to enforce rules through panels and the possibility of sanctions.

- **Jurisdiction**

A basic measure of a country's sovereignty is its government's ability to exercise jurisdiction – that is, the ability to set, interpret, and enforce laws throughout the country's territory.

Because cyberspace does not correspond to traditional geographical space, it is unclear what portion of the Net any given country has the right to treat as falling under its jurisdiction. A major way this uncertainty manifests itself today is with respect to online content. Here, principles that one country holds sacrosanct may be viewed as suspect by another. For example, free speech is championed in some jurisdictions but considered a threat to morality in other locales. Clearly, it would seem impracticable for each country to apply its own legal regime to the whole of the Net.

The implication is that future trade panels could rule illegal a country's move to ban online content if the ban were to run up against a trade interest.

It is plausible that a country's attempt to take action against objectionable content would be considered a violation of its WTO market-access commitments. In a WTO case in which Antigua and Barbuda challenged U.S. restrictions on the supply of gambling and betting services via the Internet,[17] for its defense the United States relied in part on Article XIV(a) of the WTO's General Agreement on Trade in Services (GATS). This Article permits countries to go against their market-access commitments if taking measures "necessary to protect public morals or to maintain public order."

In the final report for this case, the Appellate Body held that the measures imposed by the United States fell within the scope of the exception. However, this ruling was not really a victory for governance at the local (national) level.

In explaining how "necessity" was determined, the Appellate Body noted:

> The standard of "necessity" provided for in the general exceptions provision is an objective standard. To be sure, a Member's characterization of a measure's objectives and of the effectiveness of its regulatory approach – as evidenced, for example, by texts of statutes, legislative history, and pronouncements of government agencies or officials – will be relevant in determining whether the measure is, objectively, "necessary".
>
> A panel is not bound by these characterizations, however, and may also find guidance in the structure and operation of the measure and in contrary evidence proffered by the complaining party. In any event, a panel must, on the basis of the evidence in the record, independently and objectively assess the "necessity" of the measure before it.[18]

The Appellate Body then elaborated how it applies this standard: "The process begins with an assessment of the 'relative importance' of the interests or values furthered by the challenged measure. Having ascertained the importance of the particular interests at stake, a panel should

[17] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Appellate Body Report (WT/DS285/AB/R) of 7 April 2005.

[18] *Id.*, para. 304.

then turn to the other factors that are to be 'weighed and balanced'." In most cases a panel will consider two main factors as it continues in its determination of a measure's necessity: "One factor is the contribution of the measure to the realization of the ends pursued by it; the other factor is the restrictive impact of the measure on international commerce."[19]

To paraphrase, a WTO panel is to pay deference to a member's domestic decision to invoke an exception in the name of public morals or public order. Ultimately, however, it is the WTO panel itself who determines whether or not the member's chosen course is justified, in light of the panel's own evaluation of the importance of the problem, as well as its assessment of the measure's effectiveness in addressing that problem as weighed against the measure's trade restrictiveness.[20]

Extrapolated, the implication is that future trade panels could rule illegal a country's move to ban online content if the ban were to run up against a trade interest. So, for example, China's use of filters to prevent its citizens from accessing websites displaying the word "democracy" could be struck down if a panel did not find the purpose of the ban compelling and the approach appropriate, given the degree to which it crimped trade.

By this same logic, the "right" of a country to revert from participating in the global Net could also be called into question. For example, in recent years China has made noises to suggest that it might set up its own Internet so as to have more control over infrastructure and content. However, doing so could result in significant economic injury to other countries wishing to reach the Chinese market through the global Internet; as such, it is foreseeable that a WTO panel would find such action unwarranted.[21]

In this instance, one could argue that the multilateral trading system supports free speech. While a nice effect, the focus is on market access – a value that governments have embraced at the international level, whether or not they intended for WTO panels to assess Net content policies.

What, then, is the extent of a country's jurisdiction to set, interpret and enforce laws relating to cyberspace? Will this authority be tempered by market-access obligations? This thorny issue is not likely to go away as it demands attention for the sake of predictability in e-commerce, and, more deeply, for the exercise of basic freedoms (…or, seen from other vantage points, for the sake of governmental authority and the shepherding of public morals).

Meanwhile, in their quest to retain control, governments have looked into technologies that "map" the real world onto cyberspace, for example through location aware tools. Such "zoning" technology will allow parties to know what jurisdiction(s) they are subject to in their interactions on the Net.

In turn, this type of technology could spur further harmonization of legal systems: To keep transaction costs at a minimum, companies will likely reach out only to those online markets where they can be relatively certain of conforming to local law. Hence, there will be market incentives for those wishing to engage in e-commerce to use electronic "tags" to signal which jurisdiction they belong to online. The corollary to this is that small economies will feel pressure to align their legal systems with those of others for legal economies of scale.

[19] *Id.*, para. 306.

[20] This approach loosely embraces the principle of subsidiarity (i.e. governance at the most local level practicable) as the panel checks that the member applying an exception has itself used a process to determine that the interests or values that the measure is protecting are important.

[21] Of course, even if China could justify this action on the grounds of protecting public morals or the public order, the expected economic loss in terms of online exports could be deemed too great for the government to attempt such a fiat.

GOVERNMENTS PARTNERING WITH BUSINESS FOR STABILITY

Given the prominent role of the private sector in developing the Net, governments have been partnering with industry to achieve a stable networked environment. Of course, private companies have different constituencies than government – namely, shareholders instead of the public generally. Nonetheless, the vital expertise offered by business renders this partnership necessary.

Specifically, Net governance in the name of stability involves the traditional governance roles of overseeing infrastructure, security, and monetary authority – now, of course, at the international level.

- **Infrastructure**

Government is often expected to provide the infrastructure necessary for citizens in a society to conduct their daily affairs smoothly. Examples of infrastructure include the transportation system, the energy system, and the communications system, as well as shared resource arrangements for health, education, and the environment.

With the advent of the Net, citizens have looked to government to pave the way for this mode of communication. Because the Net is a global network of networks, countries must use common technical standards for it to function well.

> *As governments are appreciating the critical importance of the Internet for their infrastructures, there has been pronounced disagreement over which country or countries should exert influence.*

Meanwhile, there is the need for quick and expert decision-making to accommodate technology's rapid changes. Governments for the most part recognize this need and are partnering with industry to manage the Net's infrastructure. Non-governmental bodies dealing with Internet infrastructure include the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and the International Organization for Standardization (ISO), among others. The Internet Corporation for Assigned Names and Numbers (ICANN), which coordinates the Internet's domain name and addressing system, was supposed to be a hybrid, involving a mix of governmental advice and high-tech expertise.

As governments are appreciating the critical importance of the Internet for their infrastructures, there has been pronounced disagreement over which country or countries should exert influence over these bodies, particularly ICANN. For example, in the months leading up to the November 2005 Tunis meeting of the World Summit on the Information Society (WSIS), countries like China, India, and Brazil charged that ICANN's responsibilities should be transferred to a multilateral body. In a meeting that was supposed to be the last on the subject of Internet Governance prior to the Tunis event, the European Union joined the ranks of those calling for a multilateral body to oversee public policy issues pertaining to the Internet, leaving the United States essentially isolated. Eventually countries agreed to a process to explore how to strengthen involvement of governments in public policy issues relating to ICANN, as well as a forum for considering broader issues of the Information Society.[22]

While governments are mindful of politics, they nevertheless are committing to greater infrastructure collaboration in the networked

[22] See, e.g., statements by these governments at the Preparatory Committee meetings ("PrepComs") for WSIS in 2005 (appearing at http://www.wgig.org/PrepCom-Statements.html) and the *Tunis Agenda for the Information Society*, adopted by governments at the conclusion of the Tunis Phase of WSIS (appearing at http://www.wsis.org).

world. For example, the Next Generation Networks (NGN) initiative of the International Telecommunication Union (ITU) has governments working with some members of the private sector (e.g., Cisco) to design a way to distinguish between types of communications passing over the Internet. The idea is to have an intelligent network that can tell if a transmission is voice, video, or other data, and that can then adjust service to the particular demands of that communication (in the name of "quality of service"). Many technologists object to this initiative on the grounds that it will disrupt the clean "end-to-end" architecture of the Internet, where the intelligence is at the ends and the core of the network is purposefully simple.[23] Nevertheless, an NGN Focus Group and its affiliates have gone ahead and formulated standards,[24] and the ITU will apparently be moving full steam ahead.

Initiatives like these go unnoticed by the popular media and are unknown to the public. Nonetheless, they lay the foundation for internationally federated control over the world's information infrastructure.

Another big but fairly unnoticed intergovernmental initiative is the Group on Earth Observations (GEO),[25] which was established in 2003. GEO has a mandate to "improve coordination of strategies and systems for observations of the Earth and identify measures to minimize data gaps, with a view to moving toward a comprehensive, coordinated, and sustained Earth observation system of systems," and to "exchange observations recorded from *in situ*, aircraft, and satellite networks," among other tasks.[26] The *10-Year Implementation Plan* for its Global Earth Observation System of Systems (GEOSS), adopted in early 2005, institutes a major but relatively unnoticed process: "The vision for GEOSS is to realize a future wherein decisions and actions for the benefit of humankind are informed via coordinated, comprehensive and sustained Earth observations and information."[27]

An additional effort to coordinate infrastructure is being propelled by the European Organization for Nuclear Research (or "CERN", Europe's scientific consortium where the World Wide Web was born). CERN's Large Hadron Collider Computing Grid project includes a plan "to integrate thousands of computers worldwide into a global computing resource," or Grid. The project's most enthusiastic proponents contend: "The Grid goes well beyond simple communication between computers and aims ultimately to turn the global network of computers into one vast computational resource."[28]

Initiatives like these go unnoticed by the popular media and are unknown to the public. Nonetheless, they lay the foundation for internationally federated control over the world's information infrastructure.

[23] See, e.g., IETF notes from the ITU-IETF meeting of May 2005, at http://www.ietf.org.

[24] See "ITU Focus Group Announces Release 1 NGN Standards," ITU-T Newslog, 21 November 2005, at http://www.itu.int.

[25] As of August 2005, GEO consisted of 47 members and 29 participant international organizations.

[26] *Declaration of the Earth Observation Summit*, Washington, DC, July 31, 2003. "*In situ*" connotes measurements taken through direct physical contact; other mechanisms covered by the agreement entail remote measurements.

[27] Group on Earth Observations, *Global Earth Observation System of Systems: 10-Year Implementation Plan,* February 2005, p.1. The *10-Year Implementation Plan* was endorsed by nearly 60 governments and the European Commission.

[28] Grid Café, "What is the Grid?" as viewed at http://gridcafe.web.cern.ch/gridcafe/whatisgrid/whatis.html on August 15, 2005.

- **Security**

A fundamental function of government is to ensure the security of the land. Indeed, in customary international law, this security is considered one of the hallmarks of sovereignty.

This mix brings underlying tensions since the players involved – that is, governments and private enterprises – naturally have different interests.

The conception of security in cyberspace has undergone dramatic change in its short history to date. Just a few years ago, cybersecurity was construed as protecting the information infrastructure for the sake of that infrastructure itself.[29] Now, however, cybersecurity is viewed as central to general security. No doubt, a disabling of the Internet would wreak havoc on industrialized societies.

A single government is inadequate on its own to ensure the security of the Net and to prevent people from using it for criminal purposes. Seeing the need to cooperate on cybersecurity, governments are coordinating legal and technological responses.

An added complexity stems from the need for governments to partner with the private sector in providing cybersecurity. The private sector offers technological expertise and controls many of the Net's critical processes. Moreover, the high-tech sector is fast and flexible.

Still, this mix brings underlying tensions since the players involved – that is, governments and private enterprises – naturally have different interests. Governments agree that they must protect the "order", but they do not agree on basic values that should underlie that order. A business, meanwhile, has to focus on its own competitiveness and profitability and must answer to shareholders rather than the public at large.

Despite differences, one area of cooperation concerns risks posed by countries' varying abilities to counter threats to this vital infrastructure. Essentially, some developing countries lack the resources (and perhaps the desire) to confront vulnerabilities in network security. These regions are sometimes viewed as the "weak link" in the chain of international cybersecurity. Recognizing this strain, the World Bank recently tempered its rush to roll out technology in developing countries, balancing this obvious requisite for infrastructure development with attention to cybersecurity concerns. At the same time, companies like Sun Microsystems see developing countries as good testing grounds for new, inexpensive technologies, whose administration can be handled remotely.

Perhaps the need to solve security problems will induce governments of wealthier countries to fund infrastructure development in poorer regions. Beyond solving the weak-link problem, infrastructure investment in developing regions would allow these countries to participate more effectively in e-commerce; the improved economic welfare in turn would likely pay dividends in political stability.

Meanwhile, countries with greater capacity to carry out cybersecurity are forming alliances despite differing interests. For example, forty-five European countries, Canada, Japan, South Africa and the United States all signed the *Convention on Cybercrime*. This treaty commits these countries to using common definitions of what constitutes cybercrime, and common procedures for criminal enforcement; in addition, signatories have agreed to establish a "fast and effective regime" for international cooperation, including

[29] Of course, the Internet had its beginnings with the U.S. military. Still, the focus has shifted from the Net's being vital for communications (whether military or civil) to its being crucial for society's general workings.

information sharing among different countries' enforcement agencies. The treaty places a burden on Internet service providers (ISPs) by requiring them to capture and retain communications data for use in criminal investigations.

In an initiative under the International Civil Aviation Organization, 188 governments have pledged to follow common standards to embed biometric information (e.g., photos, fingerprints, or digitized eye scans) in travel documents.[30] Since machines will be able to read this data without contact, future readings could be taken not just at immigration checkpoints but anywhere that programmed sensors were placed (e.g., at entrances to buildings).

On a systemic level, it is unclear what the lines are in terms of international enforcement – and whether the blurring of enforcement boundaries will erode domestic curbs on government power.

Who will have access to this data? How will its proper care be ensured? How will such matters be decided? Questions abound.

In sum, joint cybersecurity efforts are helping to ensure a safe and predictable networked world, but at the same time they carry serious tensions. On a systemic level, it is unclear what the lines are in terms of international enforcement – and whether the blurring of enforcement boundaries will erode domestic curbs on government power.

- **Monetary Authority**

Another area of governance associated with a country's sense of sovereignty is the ability to wield monetary authority. Ideally, a country's monetary authority is capable of (a) managing the supply of money and credit; (b) enabling money to flow smoothly, freely, and without obstruction; (c) keeping the currency stable; and (d) promoting the safety of the banking system by licensing, supervising and regulating institutions in the financial sector.

In the wake of the Asian, Russian, and Brazilian financial crises of 1997 and 1998, government officials active in the Basel Committee on Banking Supervision set up the Electronic Banking Group (EBG). This group aims to:

- Develop guiding principles for the prudent risk management of e-banking activities;
- Identify if and where existing Basel Committee guidance needs to be adapted to facilitate the sound supervision of cross-border e-banking activities; and
- Promote co-operative international efforts within the banking industry and between the public and private sectors to identify e-banking risk issues and sound practices to deal with them.[31]

The EBG has found that one of the new dilemmas for monetary systems is the fact that technology enables unregulated players to provide financial services over the Internet.[32] By acting remotely, non-traditional banks can avoid regulations that come with a local presence, but still enjoy effective market access. The danger is that an unregulated private supplier of electronic money will establish enough credibility to operate apart from the government reserve system – in essence, serving as a private central bank. With this new force, the ability of a country to exercise monetary oversight will diminish, with the consequence of weakened ability to foster stable prices, maximum stable employment, and steady economic growth.

[30] See Press Release of the International Civil Aviation Organization (dated 28 May 2003).

[31] *Electronic Banking Group Initiatives and White Papers*, Basel Committee for Banking Supervision, October 2000.

[32] *Id.*

Although relatively small at present, digital communities that create wealth represent new models of private central banks. For example, in the user-created digital world of Second Life,[33] "residents" may generate wealth through their activities. This wealth is expressed in an internal currency (Linden dollars), which can be exchanged for real currency.[34] In November 2005, 50,000 Second Life residents participated in transactions valued at US$4 million in the internal economy, and they exchanged US$400k worth of Linden dollars with the external economy. Meanwhile, the average value of transactions has been growing at a rate of approximately 100% annually.[35] In light of such figures, Second Life and similar communities should not be overlooked by monetary authorities.

The danger is that an unregulated private supplier of electronic money will establish enough credibility to operate apart from the government reserve system – in essence, serving as a private central bank.

Entities engaged in transmitting money may be affected by international initiatives to stem money laundering and the financing of terrorism. In this area again, governments find themselves in a position where they must cooperate to deal with Net-related problems, and they are again turning to international organizations to coordinate policy. With the Financial Action Task Force (FATF), they have drawn up recommendations with heavy involvement of the private sector.[36]

In particular, the FATF's Special Recommendations on Terrorist Financing[37] address the loophole that had previously allowed non-traditional financial institutions to go unsupervised. Recommendation VI reads: "Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions..."

Additionally, Recommendation VII requires the entity transmitting money to verify the identity of senders and receivers of funds and to keep this information on file.[38]

Given technological developments and society's declining use of cash, these FATF recommendations may signal the increasing surveillance of transactions generally as payments over the Net become the norm and costs of data storage and analysis fall.

While private sector entities may bemoan the fact that the burden is placed on them to implement a secure financial system, this sector may offer the best model of a successful partnership between private-sector competitors and multilateral government bodies – with competition at all levels driving players to keep abreast of technology.

[33] See http://secondlife.com.

[34] Linden dollars may be exchanged on Second Life's official currency exchange site (LindeX) and on third party sites.

[35] Presentation by Cory Ondrejka, Vice President of Product Development for Second Life, at the Berkman Center for Internet and Society, Harvard Law School, November 29, 2005.

[36] FATF member states include 28 of the world's leading economies. By prescribing "best practices" and designating non-conforming areas as "Non-Cooperative Countries and Territories" that require extra due diligence, this group wields substantial power in financial geopolitics.

[37] Financial Action Task Force on Money Laundering, *Special Recommendations on Terrorist Financing*, October 31, 2001.

[38] Recommendation VII: "Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain."

CITIZENS ADRIFT

As the above account tells, governments have responded quickly to meet challenges in cyberspace: They have set certain parameters for people's online dealings. They have kept the doors open for e-commerce. They have let an international trade court review national rules on Net content. They have pooled resources for infrastructure development. They have set up cybersecurity arrangements. They have even cooperated to safeguard the financial stability of the networked world.

However, in letting the framework for Net governance evolve in an ad hoc way, policymakers have focused on surface problems, at the expense of deeper, more fundamental questions of democracy. Sooner or later, the networked world must confront an issue facing all societies: that is, the relationship between the state and its citizens.

- **Relation Between Person and State**

For better or worse, states traditionally have made distinctions among persons and have applied different sets of rights and responsibilities to different groups. In places that have high regard for the rule of law, there are usually criteria spelling out when a person fits into a given category – such as a person enjoying citizenship or a company receiving treatment as a "juridical" person.

However, acting independently, a single government is unable to guarantee that a person will be accorded rights in cyberspace.

Zoning the Net according to citizenship spheres at first glance might seem a sensible way to maintain the modern world's citizenship lines. However, such a practice will encounter problems, not the least of which is citizens' dissatisfaction with differential treatment based on nationality.[39] As in the other areas of governance, a global approach is needed here.

Theoretically, the *Universal Declaration on Human Rights*, agreed by the UN General Assembly in 1948,[40] could serve as a global standard for citizen rights in cyberspace. Governments reaffirmed their support for these principles at the World Summit on the Information Society.[41] Provisions with a clear Net nexus include the following:

Article 12.

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation...

Article 18.

> Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 19.

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 20.

> (1) Everyone has the right to freedom of peaceful assembly and association.
> (2) No one may be compelled to belong to an association.

[39] See also discussion under "Relations between Private Parties" and "Jurisdiction", above.

[40] Resolution 217 A (III) of 10 December 1948.

[41] *Tunis Commitment*, WSIS-05/TUNIS/DOC/7-E, 18 November 2005, para. 2.

According to the principle of technological neutrality (discussed above), it would seem these freedoms would automatically extend to cyberspace.

> *In letting the framework for Net governance evolve in an ad hoc way, policymakers have focused on surface problems, at the expense of deeper, more fundamental questions of democracy.*

Of course, the exercise of these freedoms must be considered in light of technology. Take, for example, the following:

- Identity management will soon allow the exchange and automatic processing of personal data with unprecedented speed and precision.

- Biometric readers are enabling the increasingly accurate identification of individuals through fingerprints, irises, gait, and other unique features.

- Location based services can pinpoint a mobile phone user's location, even to within a few yards in urban areas.

- Ubiquitous computing integrates computation into the environment (e.g., grafting it into the walls of a building), so that computers are all around.

- Sensors bring the miniaturization of computing appliances, e.g., through nanotechnology and radio frequency identity (RFID) tags that are readable without contact.

- Mesh networking will soon allow the spontaneous formation of networks, for example among tiny devices sprayed across a geographic area.

While these developments may conjure up sci-fi images, they are very real and fast approaching. Despite their quick onset, it is not yet clear how the emerging framework for governing the Net will apply – and at what level decisions will be made concerning the ownership and control of information they transmit.

With the combination of technology and international Net governance, the citizen faces many uncertainties. How will he know if he can rely on the rights he has come to expect under his own country's constitutional arrangement? Who will have say over his personally identifiable information as it flows around the world? Will he have the right to freedom of expression on the Net? Will he enjoy the freedom to manifest his religion online, or might there be consequences for his beliefs? Will he be guaranteed the right to associate or assemble with others via the Net? Will there be anything to keep him from being discriminatorily blocked from accessing the Net? How will he be recognized in the networked world, other than as a consumer and non-threat?

More than ever before, the citizen needs to know his rights in the networked world and have effective recourse if prevented from exercising them.

- **Accountability to the Public**

Meanwhile, in terms of accountability to the public, there is a basic disconnect between organizations making Net policy and member countries' citizens.

To bridge this gap, governments wishing to foster freedom should press for democratic channels in intergovernmental institutions. In strategizing how this might be done, it is useful first to consider how these institutions function.

Intergovernmental institutions may be viewed as analogous to administrative agencies that operate within a country. Administrative agencies are typically set up to deal with policy areas that require regulatory expertise and flexibility. They are specialized in a given subject area and can exercise all three functions of government – that is, making, interpreting, and enforcing the law – doing so in a rather streamlined fashion.

Of course, administrative agencies operating within a country are often structured to prevent arbitrariness and overreach. Checks to control and limit agency powers include (a) procedural avenues for public participation through notice of proposed rule-making and opportunities for public comment, as well as (b) substantive supervision by a country's legislative, executive, and judicial branches.

Many of the international institutions dealing with Net policy today resemble domestic agencies in that they are specialized and fairly flexible. However, in these international settings, more needs to be done to promote public participation and allow oversight by elected officials from the three branches of government.[42]

In terms of participation, the public is presently ill equipped to follow Net rule-making at the international level and thereby hold decision-makers accountable. If a person wants to track developments through the organizations' official websites, he must consult the sites of over a dozen different bodies and sift through myriad web pages within those sites, as he attempts to decipher what are the actual rules being negotiated. As a result, the effects of many Net policies are appreciated only after decisions have been made, when it is too late to affect them.

To address this problem, the burden could be placed on the actors most able to make a difference – that is, the intergovernmental bodies themselves. If so mandated by their government members, these organizations would provide public notice of proposed rule-making and would solicit public comment. A lightweight way for them to do so would be to collaborate in a one-stop-shop web portal that consolidates information on their rule-making and offers online discussion tools.[43]

What really is at issue here is the fact that the Net is being governed by global arrangements that look increasingly federal – with the center at the international level.

The question of oversight by elected officials from three branches of government is more complex. Direct participation by different countries' legislatures at the international level would multiply the difficulties of reaching consensus, and judicial review by diverse countries' courts would splinter the interpretation of rules.

What really is at issue here is the fact that the Net is being governed by global arrangements that look increasingly federal – with the center at the international level. As decision-making tilts to the executive branch operating internationally, domestic checks and balances are thrown into disequilibrium, with the legislature and judiciary unable to correct poor choices made at that level.

For example, the legislature or judiciary in a given country might disagree with international requirements for travel documents to contain machine-readable biometric data. However, by the time these officials have become aware of the international standards, it is too late to influence them: With other countries uniformly applying them, it is difficult for one country to negotiate a waiver for its citizens.

[42] Most countries participate in international institutions through their executive branches, with legislative and judicial branches dealing with matters only after they have been brought home for approval and implementation.

[43] The Net Dialogue website, which maps Net rule-making by intergovernmental organizations, provides a working model of how transparency and an online forum could be achieved. See http://www.netdialogue.org.

International cooperation begins to evolve into integration, with institutions at the center no longer serving simply as forums for negotiations but now also as enforcers of rules forged there. They employ technology to carry out this enforcement, with the effect that it is even harder to scrutinize policies since the tools of control are obscure to the average person.

To continue with the example of biometrics in identity cards: In the event of a global pandemic, governments might decide through an international process to place sensors in key places (e.g., transportation hubs) to monitor people's temperatures and signal when individuals carry fevers. These individuals are identifiable by their remotely readable biometric identity cards. The identity information is then transmitted to a centralized administrative body (e.g., the World Health Organization) via GEOSS (the "system of systems"), where the decision is taken to quarantine individuals deemed to pose a risk. A particular country's courts or legislature may disagree with the policy, but if the country goes against the international decision, it will be subject to sanctions (e.g., trade embargos or travel bans).[44]

Of course, technology can also be used to empower citizens, bringing them together to debate and pursue collective action. Still, even organized citizens will have their voting power diluted by the layers between elected government officials and delegates at the international level.

The question of direct representation is a prickly one that will take time to settle. In the meantime, checks and balances that prevent government overreach and corruption should be built into the system as soon as possible.

Since democracies are usually founded by people eager to ensure that government is accountable to the public, technologists who resist government regulation could be recruited as vigilantes for democracy. They could vet proposed rules that intend to use computer code to control behavior, testing them for effects on freedoms enshrined in the *Universal Declaration on Human Rights*. Others could be invited to help write computer code that (i) accomplished the ostensible aim of a proposed rule (e.g., facilitating e-commerce), but that (ii) did so in a way which incorporated checks and balances into the code – for example by separating governance functions; by pitting entities against each other; and by providing for electronic audits.

[44] GEOSS applications already envisioned include the tracking of "pathogen occurrences, as well as patterns of human activities," with forecasts allowing "public-service and environmental managers to modify behaviors ... to avoid exposure." Group on Earth Observations, *Global Earth Observation System of Systems: 10-Year Implementation Plan – Reference Document*, February 2005, p. 45.

CONCLUSION

Rules dealing with an expanding set of Net-related topics are being crafted in numerous forums – with over 18 different international bodies now hosting negotiations and administering rules. In fact, international Net governance is delving into all the areas that a domestic regime typically does, so that topics like security, infrastructure, property, contracts, and money are all treated at the international level.

Though negotiated on an "as needed" basis and designed to address real needs, these agreements are being crafted with little attention to the cumulative effect – that is, the emergence of an international framework for governing the networked world.

The average citizen has no knowledge of the fact that his moves are governed by these international arrangements, or of who is deciding these rules and where. Government accountability to the public is thus tenuous in this arena today.

In other words, the system points to international federalism for the networked world, even as the public is largely unaware of its existence.

Once agreed the rules are exceedingly difficult to change – after all, international bodies usually require consensus (in this context, unanimity) to amend provisions. At this point a country cannot really "opt out" since the arrangement has become an international standard.

If this system were of a strictly legal nature, there would be time for the situation to run a natural course, where the public could learn of its importance and demand greater oversight. However, the system employs technology as an enforcer. Since technology is generational, choices at one point in time may dictate dominant traits for the future, with long-lasting legacy effects. Hidden from the public eye, the computer code giving force to law may become integral to the Net's workings from this point forward.

Moreover, as the distinction between the real and virtual worlds fades over time, the international Net regime will likely spill over to regulate previously local activities. Even simple actions like buying groceries may trigger the application of international rules.[45] In other words, the international framework for governing the Net could signal the early stages of a global federation.

Perhaps most troublesome, there is no guarantee – legal or technological – that free and democratic principles will reign in the networked world.

Given the importance of the governance framework for the future networked world, those who hold freedom dear must work to build democratic mechanisms into the legal and technological structure. Specifically, law and computer code should be designed to promote:

- Subsidiarity (preference for local decision-making);
- Checks and balances;
- Accountability to the public; and
- Protections for core freedoms.

The time for technologists and government officials to embed these principles in Net governance is now, while they are constructing the framework for the future networked world.

[45] In U.S. Constitutional terms, this dynamic resembles that of the "Commerce Clause", where seemingly local actions have been found to have consequences for interstate commerce, with the effect that Federal law trumps local law. The European Union has experienced similar dynamics, and Member States' laws have had to yield to the central "*acquis communautaire*".