Securing Internet Freedom

Security, Privacy and Global Governance

Securing Internet Freedom

Security, Privacy and Global Governance

Inaugural address of Prof. dr. Milton Mueller, XS4All Professor,
Technology University of Delft, Information and Communication
Technology section, Faculty of Technology, Policy and Management

17 October, 2008

colofon

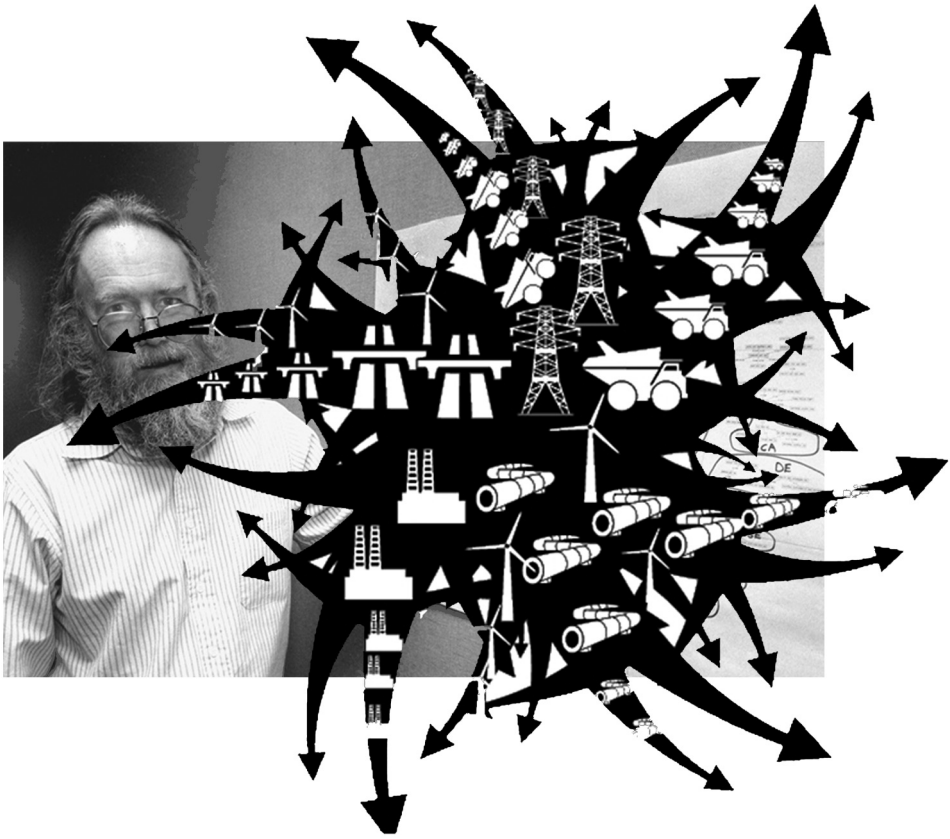
Voorwoord

Vijftien jaar geleden werd XS4ALL opgericht als eerste Nederlandse internetprovider voor particulieren. Internet was toen al mondjesmaat beschikbaar voor bedrijven en universiteiten, maar een groep hackers, programmeurs en techneuten vond dat het netwerk voor iedereen beschikbaar zou moeten zijn. Zij stichtten XS4ALL (toegang voor iedereen) met een duidelijk ideëel doel: voor de oprichters, maar ook voor de eerste medewerkers en klanten waren het vrijgeven en toegankelijk maken van informatie, het delen van expertise en het ontwikkelen van vrije software van groot belang. Ook individuele vrijheid en privacy waren in de hackergemeenschap belangrijke waarden. Toen XS4ALL enkele jaren later van een stichting overging in een BV, veranderde aan die idealen weinig.

Inmiddels is internet sterk verweven in het dagelijks leven. Het netwerk speelt een belangrijke rol in werk en vrije tijd, voor commerciële activiteiten en bij overheidszaken. Internetgebruik groeit nog steeds sterk en het wordt steeds mobieler, waardoor nieuwe security- en privacy-vraagstukken ontstaan. Mobiele telefoons, laptops en PDA's maken verbinding met internet, steeds meer producten worden voorzien van RFID chips en via locatiebepaling middels GPS en gegevens van mobiele telefonie kunnen gebruikers steeds nauwkeuriger getraceerd worden. Doordat steeds meer communicatie via het netwerk plaatsvindt kan netwerkanalyse een zeer gedetailleerd beeld opleveren van internetgebruikers. Dat gegeven is erg interessant voor commerciële partijen, voor reclame- en marketingdoeleinden, maar ook voor overheden, voor opsporing en preventie.

XS4ALL vindt dat de privacy van internetgebruikers gewaarborgd moet zijn en dat al die gegevens goed beveiligd moeten worden tegen misbruik. De XS4ALL leerstoel aan de TU Delft is daarom opgericht om onderzoek te doen naar de privacy- en security-aspecten van huidige

en toekomstige technologische ontwikkelingen. Zowel met het oog op de technologie zelf, als op bestuurlijke en ethische aspecten van die ontwikkelingen. Milton Mueller heeft zijn sporen meer dan verdiend als wetenschapper op deze gebieden, XS4ALL is dan ook zeer verheugd met zijn aanstelling als eerste XS4ALL Internet Professor.



1. *The Dream*

I want to begin by killing off a dream. I don't conduct this murder casually, because it is my own dream.

In this dream the internet behaves the way it was designed to behave: as a robust method of exchanging information among any digital device, anywhere. No governments or corporations interfere with that. There are no more filters and chokepoints. The end to end principle reigns supreme. The bearded wizards of computer science rule the root once again. People use the Internet responsibly and don't abuse each other. The dream involves nothing less than a restoration of the Golden Age of pure liberty and cooperation on the Internet.

It could actually come true, this dream. Isn't freedom part of the Net's *original design*? (Lessig, 2001) If only we stopped blocking and censoring web sites; if only spammers and criminals didn't abuse its openness; if the world's governments would just leave it alone; if the big media conglomerates stayed away from it; if we could only legislate net neutrality; if only the Russians and the Chinese would moderate their dictatorships, if, if … but you can already see what is wrong with this dream. The list is getting too long, and increasingly implausible.

Let this dream now come into full contact with reality. The Internet is a mess. It is an organism infected by viruses and worms; a planet invaded and colonized by alien botnets. For every innovator, there is an imposter. The more it brings us together into social networking sites, the more we discover how bizarre and even horrifying social relations can be. All of our contemporary and historical social problems are manifest there: war, hate, discrimination, cruelty, perversion and domination. And yet we cannot escape it because it is invading our pockets through our mobile telephones.

Most of all it is an internet to which governments have woken up. Ambitious politicians move to 'save' us from its problems. New forms of crypto-armor are added to the Net as states define it as 'critical infrastructure' and make plans to use it as a weapon. Governments

assert a blanket right to watch, record and data-mine everything ordinary people do online. The U.S. insists on retaining control of its central coordinating functions. China and Russia react by exploring national internets. Europe jostles for position in the emerging internet of things. The simple act of internetworking is now geopolitical.

In short, it does not matter how the Net was designed or what the intent of the designers was, the best and the worst of what human beings are capable exist there, and will never be eliminated online anymore than they will be finally eradicated offline. We might say of it, as Norman Mailer said of America, "It grew by itself. Like a weed and a monster and a beauty and a pig."

So the dream is dead. Bang! You are now a witness to the murder.

What kept this dream alive for so long? I think it was that initial taste of freedom associated with the earliest days of the Internet. It still haunts us. It was more than just the absence of restraints but the kind of freedom associated with the acquisition of powerful wings by a flightless animal. It put you in control; it threw the authorities off balance. It inspired utopian visions. The flood of creativity and innovation it unleashed stands as a lasting rebuke to the overly controlling institutions that preceded it.

Some kind of dream like that is worth keeping, of course. But I have to kill off the old one first. Not because I want to give aid and comfort to the enemies of internet freedom. No, it has to be put to death because it has become a siren that pulls the Odyssey of Internet governance off course. The astonishing truth is that the simpler, earlier freedom of the Internet was an accident. It rested on its spontaneous emergence from a sheltered, noncommercial environment, and from the inattention and ignorance of established authorities. That kind of freedom is forever gone. The strange claim that freedom is engineered into the technology lends credence to the falsehood that we could preserve it by fending off all attempts to change it. It also lends support to the belief that freedom itself is responsible for our problems. As long as we cling to that fallacy we will lose what is worth keeping about the original dream.

So what does 'Internet freedom' mean in this new context? That, in my view, is the question that defines the research agenda of the XS4ALL Chair. To answer it we have to look forward, not back, and dedicate ourselves to a new conception of Internet freedom attuned to contemporary conditions.

Re-conceptualizing Internet freedom is simultaneously a normative-philosophical and a scientific enterprise. Let's begin with the normative.

2. *Rights*

Freedom, security and privacy are not technical concepts. They are human and social objectives that technology and governance can be used to realize – or threaten. Thus, I would not begin the discussion with talk about the security of *infrastructures* or the security of *nations* and I would reject the rhetoric of securitization.[1] I prefer to talk about the security of human beings.

The relationships between privacy, security and freedom are double-edged. Privacy and security can enhance and protect freedom of action and freedom of thought, but both concepts are also invoked frequently in calls for greater regulation of behavior on the Internet. One can only hint at the complexities here, but consider privacy first. Anonymity can liberate you to do and say things that you might otherwise be afraid to say or do. But anonymity can also allow one to evade

1 The term 'securitization' here refers not to finance but to the process of actively constructing something as a security problem through descriptions and rhetoric. The concept, which originated with the Copenhagen School (Waever 1995), explains how once topics or policies are successfully defined as security problems actors can legitimize extraordinary means to address problems, such as suspending civil rights, mobilizing the military or attacking another country.

accountability for harms to others. Protection of your personal data can mean freedom from unwanted forms of attention and from abuse, or the ability to move beyond past mistakes. But shielding data about yourself from others can deceive them and impinge on their ability to learn and to make decisions that protect their interests.

Security too has a complex and double-edged relationship with freedom and privacy. To lack security in one's person and property is be unfree, to be manipulated, to lose the fruits of your labor. At the same time, efforts to safeguard security can create barriers and roadblocks to others' (and even your own) freedom of action. Giving central authorities an unrestricted ability to pursue 'our' security can ultimately threaten our security. It is ridiculous to believe that the gigantic collections of sensitive data assembled by governments will never be mishandled; that the computers controlling wiretapping intercepts will never be a target for capture; that the removal of oversight and due process protections from surveillance will not produce political abuses.[2]

The dualism associated with the concept *security*, and with *privacy*, may seem obvious, but in public policy research and discourse there is still no clear resolution of their contradictions. We speak vaguely of 'balances' and 'trade-offs.' But that kind of talk merely turns decisions over to the vagaries of politics or to business calculations. And in those

2 For Americans, the generation of insecurity from an overly aggressive, rights-indifferent pursuit of global security is most evident from the foreign policy blowback they have experienced recently. The 1988 bombing of Pan Am flight 103 over Scotland, for example, resulted in the deaths of 259 passengers – over 100 of them Syracuse University students. The attack is now known to be retaliation for the Reagan administration's aerial bombing of Libya, which killed the Libyan President's stepdaughter. Whatever the objective of that foreign policy adventure, it clearly did not make us more secure. Worse, incidents of blowback can be and often are exploited by those who caused them to expand extraordinary powers, creating a vicious cycle.

situations generalized concerns about abstract rights and freedoms yield too easily, unless there are major legal or institutional safeguards standing in the way. So in addressing security and privacy issues thoroughly, one is led inexorably to higher levels of abstraction – to ethical theories and political philosophy.

If we assert that people have a *right* to privacy and security, what do we mean by rights? What is the best way for society to resolve conflicting claims about protections or limitations of rights? When is it admissible to sacrifice individual security and privacy for the sake of collective security? In the context of the Internet these are not just philosophical questions, but practical ones we face every day.

I conclude that one cannot talk sensibly, much less scientifically, about privacy and security on the Internet without grounding the discussion in a commitment to clearly defined individual rights. By 'rights' I mean strong, categorical claims that set firm boundaries on what governments or other actors can do to individuals. Rights are claims that regulate and limit the use of coercion by governments and others. They are substantially different, stronger and more important than ordinary policy claims that assert that certain actions will bring about public benefits. Rights should take priority over all such claims.

One useful theoretical guideline to the definition of rights can be found in the classical concept of isonomia. Isonomia is composed of the Greek words for equality, ἴσος, and law, νόμος, and means equality of individual rights under the law. In a deeper sense, it encapsulates the celebrated formula of Immanuel Kant that freedom for all can be achieved only if the freedom of each does not extend further than was compatible with an equal freedom for all others.

The idea of reciprocal and equal freedom imposes a strong and useful discipline on our notion of rights and on the exercise of power. It confines our rights lexicon to individual rights of the most basic and universal sort. It directly links individual freedom to responsibility to others. It prevents us from manufacturing rights claims specific to groups or situations, creating a tangled and inconsistent skein that

allows political might rather than the right principles to rule.

Most importantly, this principle suggests that at the normative or ethical level of analysis security, privacy and freedom are not antagonistic. Once grounded in a consistent notion of individual rights, security and freedom are mutually supportive concepts. Individual autonomy or freedom is the overriding value; security is a derivative of that, and privacy is merely an extension of concepts of security and freedom to the domain of reputation and the disclosure of personal information. They are not opposing forces that need to be arbitrarily traded off against each other in the exigencies of the moment.

You cannot be free without security in your person and property; any claims to guarantee collective security at the expense of individual rights will only produce new forms of insecurity. Likewise, privacy is of interest only insofar as it protects and preserves human freedom. As an extension of your personal freedom you have a right to withdraw from public scrutiny and to anonymity in the pursuit of lawful and peaceful action. But unless we put freedom first, privacy law can easily slip into a paternalistic attempt to comprehensively regulate how information is used.

3. *Order*

How do you actualize rights? How do you build freedom? Is it somehow embedded in the way the technical system is built? Or is it in the laws and institutions around it? Here I want to contrast two visions or approaches to this problem: law professor Lawrence Lessig (L. Lessig, 1999) and the late economist Friedrich Hayek (Hayek, 1973).

Lessig's phrase 'code is law' has become a common aphorism. It implies that it is the *design* of information technology itself that has the deepest influence on the control of users. His worldview is based on an architectural metaphor; the effect of designs is to construct the spaces and flows of online society to shape behavior in ways that the

designers intend. In its most extreme form, behavior is shaped the way that laboratory rats are guided through a maze – by putting technological barriers where you don't want people to go and automated rewards where you want them to go. A liberal, Lessig is compelled to advocate designing freedom into the system somehow(L. Lessig, 2001), but his concept of order remains intrinsically hierarchical: code and law express the power of some people over others.

I want turn away from this all-too-popular paradigm and raise the possibility of another. In Hayek's worldview, the rules that govern society should not be designed to shape behavior to someone's purpose and dictate specific outcomes. Rather, they should create a secure and orderly framework within which people can act to pursue their own ends.[3] Ideally, rules enable cooperative interaction, and constrain only in order to protect and preserve the freedom or rights of the actors involved. We are back to the isonomia principle.

Hayek's basic metaphor for social order is not architecture but language. Languages commit their users to specific patterns of grammar and to shared conventions about the meaning of words. These rules and conventions are constraints, yes, but by accepting and working within them we gain more freedom, more power to think, cooperate and act than we would have without them. In other words, rules can liberate and not just control; they can *enable* freedom, they do not necessarily conflict with it.

Furthermore, no hierarchical authority promulgates the rules of language; grammars and vocabularies emerge and evolve through negotiated interactions and gain acceptance over time. Hayek would have no trouble recognizing and accounting for the existence of de-

---

3 '... it is necessary to free ourselves wholly from the erroneous conception that there can be first a society which then gives itself laws. ... It is only as a result of individuals observing certain common rules that a group of men can live together in those orderly relations which we call a society.' Hayek (1973), p. 95.

signed spaces in the online world, private properties where code is law in Lessig's sense. But he distinguished between designed social orders oriented around a specific purpose, which he called 'organizations,' and the larger space that encompasses the interdependent actions of all these intentional actors. This he called a spontaneous order, and viewed it as a product of human action but not of anyone's design. The distinction between organization and wider social order is important (even if it is slippery). Society is not something that can be 'designed.'

The global adoption of Internet protocol provided a powerful demonstration of the simultaneous ordering and liberating effect of impersonal, universally applicable rules. TCP/IP provided software instructions for compatible data exchange between any of the world's networks and computers. The 'code' of TCP/IP was indeed *law* – not in Lessig's sense but in Hayek's. It enabled orderly and constructive interactions among its users, and so provided the framework for an emergent, global spontaneous order in the communication-information economy, an order profoundly subversive of the *status quo ante*.

In our overly legislated society, we are much too comfortable with the notion that everything and anything is subject to top-down public policy; we have lost sight of the elegant power of rules that enable people to do what they want to do rather than pressure them to do what others want them to do. A Hayekian conception of order serves as a useful counterweight to the paradigm of architectural design. It makes it clear that we need to show some deference to rule systems that have evolved in a bottom up fashion because of their coordinative ability. It also suggests that our approach to governance needs to give people the space to work out their own solutions – assuming that their negotiations take place within a framework in which their basic rights are not violated – and that we should not resort instantly to hierarchical legislation.

This approach assumes, however, that people already possess the appropriate levels of autonomy and freedom needed to negotiate and adapt. That assumption is not always true. In this world injustice and

domination are rampant. So while it is clear that we cannot place our hopes for internet freedom in some top-down design, it is just as clear that we cannot just sit back and allow evolution to take its course. The simple ordering principle of TCP/IP is not sufficient. Free interaction via Internet protocols cannot by itself guarantee the basic human rights to freedom and security, and we have to stop pretending that it can. Something must be done about that, but what? Here we have to engage with questions about governance, policy and institutions. That leads us to the scientific part of the research agenda.

4. *Institutions*

My research agenda is based on a social science approach that can be broadly labeled *institutionalism*. Institutionalists are those who try to explain the emergence and effects of the systems of socially constructed rules that channel human action. In these theories, the term 'institution' refers not to organizations, but to the rules and roles that structure the interactions among purposive actors. Institutionalization implies that parties involved in regular interactions understand and accept certain norms, conventions and explicitly formulated rules governing their interaction. This results in what game theorists call equilibrium outcomes, or stable patterns of interaction that reproduce and reinforce the rules as the precondition for action.

Institutionalism is the best way I know of to integrate the technological, economic, political and organizational aspects of the study of Internet governance. 'Technologies' are really socio-technical systems. The characteristics of the system are shaped by the economic and political incentives of corporate and individual actors, by laws, regulations, politics and social norms, as well as the design and capabilities of the technologies deployed. Because path dependency is a prominent feature of the way socio-technical systems evolve and adapt, an awareness of historical process is critical as well. There is rarely a

single process or a 'thing' that can be designed here, but there is always a discoverable order. This approach draws on the accomplishments of the literature on law and economics, property rights and transactions costs, as they contributed to the development of the new institutional economics. (Alston, 2008) It also draws on the more recent body of scholarly literature developing around the economics of security in information systems.[4] (Anderson & Moore, 2007)It is a mode of analysis that lends itself to the analysis and development of policies as well.

Within this broad methodological approach, two major problem areas define the contour of the scientific research agenda. The first is the problem of the nation-state versus transnational or global governance. The second is the problem of intermediary responsibility as it applies to the Internet service provider. I will describe these problem areas and then discuss two research projects related to them that are already underway under the XS4ALL Chair.

4.1 THE NATION-STATE

For centuries, national governments have been the most authoritative platforms for defining and enforcing the rules that condition society. The study of internet governance, however, takes us beyond the normal boundaries of institutional analysis. The internet disturbed the institutional equilibrium in information and communication. This put pressure on the nation-state in four ways. First, its distance-insensitive cost structure and non-territorial addressing and routing architecture made borderless communication the default; any deviation from that requires additional (costly) interventions. Second, as an open network of networks it distributed authority over networking and ensured that the decision making units are no longer aligned

4 The existing research on the economics of information security, however, tends to focus on economic incentives and has little to say about the political and institutional dimensions of the problem.

with political units. Third, de facto decision making authority over standards and critical Internet resources rests in the hands of a transnational scientific/technical community that emerged independently of national states and their derivative institutions. These relatively young but maturing institutions, such as the Internet Engineering Task Force (IETF), the Regional Internet Address Registries, and ICANN, provided a new locus of authority over governance processes affecting Internet standards and virtual resources. We are only just now beginning to figure out how governments can and should relate to these 'native' institutions. Finally, the sheer volume of transactions and content on the internet and the speed with which it changes exceeds the regulatory and dispute resolution capacity of traditional governmental and judicial/regulatory processes.

While disruptive technologies shuffle the deck in the short term, it is only a matter of time before things settle down again into a more stable pattern of interaction. So what kind of a global governance regime is the internet settling into? Do we have any new ideas about how to intervene in that process to make the outcome better? Relating back to our normative agenda, how can we secure freedom in this transition?

There is an ongoing debate in political science over the role of the state in Internet governance. (Drezner, 2007; Goldsmith & Wu, 2006; Mueller, 2002; Reidenberg, 2005) While it is clear that the Internet does not threaten to overthrow the nation-state, as some idealists asserted, it does *problematize* its power and its mode of operation in the sector, and demand adjustments. Its globalizing effect also highlights and makes more contentious some of the extreme differences among the world's nations with respect to individual rights. It is clear that states – including the U.S., not just undemocratic once – constitute some of the biggest threats to Internet freedom. In the international arena they are concerned mainly with their own power and security more than with individual rights. At the same time we may need state-like powers to prosecute and incarcerate criminals, ensure due process of law, counter private aggregations of power, or to formalize indi-

vidual rights and sanction violations of them by states or other actors. How to harness power to secure freedom? This is a hard problem.

In the book *Powers of Freedom* (1999), Nicholas Rose observes that liberalism was not the first political movement to proclaim the right of individuals to be free; its innovation was that it was the first to successfully link that claim to a specific system of governance. The 19th century liberal-democratic state created a particular historical realization of a system of rights and it did this by distributing the responsibility for government to individual citizens qua citizens. The democratic nation-state, however, doesn't scale to global proportions. We need to find ways to translate liberal rights and freedoms into a governance framework suitable for the global internet. This is the institutional problem that drives our research agenda.

4.2 NETWORKED GOVERNANCE OF INTERNET SECURITY

We are now attacking one small piece of this big problem. One of our research projects is investigating the organizational arrangements that have evolved to support responses to security incidents on the Internet –problems such as spam, viruses, phishing and denial of service attacks.

Security and crime are traditionally domains where states play a major role as both legislators and enforcers of rules. But the governance of Internet security seems to follow a less state-centric model. It takes place mainly through informal, cooperative relationships among technical experts in the nonprofit and private sector. In some ways they are analogous to a globally distributed volunteer fire department that mobilizes around emergencies but also maintains an ongoing network of exchanges of data and specialized knowledge. They generally involve actors with direct operational control of some form of access to the Internet (servers, routers, bandwidth, domain names). Governments and law enforcement agencies are involved and there are applicable national and international laws, but most of the day-to-day work of identifying, preventing and responding to threats seems to

be done by non-state actors relying on cooperative frameworks and norms developed independently of states.

The methods and actions of this global network of security governance have never been systematically documented in the scholarly literature, and the implications such arrangements might have for organizational theory and the larger problems of Internet governance have not been adequately explored. There is an applicable scientific literature – or rather multiple literatures from different disciplines that don't articulate all that well. In political science there are concepts of 'policy networks,' (Fritz W. Scharpf, 1997; Scharpf, 1993) 'networked governance' (Kahler, 2008; Sørenson & Torfing, 2007) and 'transgovernmental networks' (Raustiala, 2002; Slaughter, 2004). In management and organizational sociology there is the concept of the 'network form of organization' (Podolny and Page, 1998; Powell, 1990). In law and economics there is the concept of 'commons-based peer production' (Benkler, 2006; Weber, 2004).

The terminology here can be confusing. 'Networks' in this case does not mean the technological communication networks but what we might in layman's terms call social networks; that is, regularly communicating clusters of people and organizations. These connected individuals, to use Benkler's words, can be seen as 'a new modality of organizing production … based on sharing resources and outputs among widely distributed, loosely connected individuals who cooperate with each other without relying on either market signals or managerial commands.' (2006 p. 60)

Can this kind of an arrangement square the circle of global governance, overcoming the limitations of territorial sovereignty while retaining the freedom and flexibility of nonhierarchical cooperation? Maybe, maybe not. We must analyze networked governance critically. Forging networked relations across organizational boundaries does not by itself resolve questions about how much authority these organizations have in relation to each other and what rights the 'citizens' of cyberspace can claim against them. As an example, the Anti-Phishing

Working Group,[5] one of these new network organizations devoted to fighting cybercrime, acts to take down web sites that prey on banking customers as rapidly as possible. But what if they make a mistake, and disable an innocent business's facilities? Thus it is important to understand how the new networks of actors thrown together by the problems of Internet security answer questions about who makes binding decisions and who has what rights. We must also explore the relationship between networked collaboration and the more traditional forms of state power, such as inter-governmental conventions, government agencies and national laws. In connection with that, we will explore which factors make the traditional inter-governmental laws and treaties ineffective responses to Internet security issues, and what kinds of problems or changes might trigger more direct and formal involvement by states. Finally, we will investigate whether the information security practices of private actors pre-empt or supersede the more traditional law enforcement activities of governments, or whether they supplement or complement them (e.g., see the theses of Raustiala 2002).

4.3 ISP's and the problem of intermediary responsibility

ISPs are the site where human rights to communication and information on the internet are actualized. Many want the road to the internet to be as transparent and neutral as possible – a taken-for-granted, generalized capacity for communication driven by end users' own choices of applications, content and services. This is the argument for network neutrality, which implies a clean separation between conveyance and content. Moving in parallel are efforts to exploit the ISP's intermediary position to facilitate social control. ISPs are routinely asked to block access to illegal content. There are pressures to require

5 http://www.apwg.org

ISPs to assume more responsibility for catching or removing malware.[6] Copyright holders want them to police illegal downloads by their users.[7] Still others want to extend notice and takedown procedures to objectionable comments or photos. (Solove, 2007) Aside from external pressures, there may also be commercial pressures on the ISPs to spy on their customers or manage and control their activities.

The politics of Internet governance now tend to push more responsibility for monitoring and policing Internet conduct onto ISPs. (Lichtman & Posner, 2006) This can be a strategy for scaling up and making more efficient the policing function by harnessing the incentives and resources of private actors who are closer to the action. But it puts private parties in the position of judge and executioner. And it imposes major burdens on the ISPs, raising the cost of access and lowering the diversity of supply models. (Harper, 2005)

So we need more transnational comparative research about ISP regulation that carefully analyzes the relationship between the freedom and innovation fostered by making ISPs a neutral conduit, and the alleged benefits of exploiting their potential to act as a gatekeeper or control point. Such research needs to be sensitive to institutional variation at the national level, but must remain focused on the workings of the global internet as a whole. And in keeping with the normative ideals outlined earlier, it must not lose sight of the way policies and commercial practices affect the universal rights and freedoms of the individual.

---

6 See, for example, the UK House of Lords Select Committee on Science and Technology Fifth Report, http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm.

7 See Nate Anderson, 'MPAA head wants deeper relationship (read: content filtering) with ISPs' ArsTechnica September 19, 2007, and UK Department for Business Enterprise and Regulatory Reform (BERR) Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-sharing, July 2008.

4.4 ISP's and deep packet inspection

In line with this problem, our second research project focuses on ISPs and their use of a new technological capability, Deep Packet Inspection (DPI). DPI is specialized hardware with powerful and fast information processing capabilities. Once DPI is embedded in a network its operator can analyze what is inside the individual packets that constitute internet traffic and take action on them according to defined policies.

DPI has profound implications for the freedom, privacy and security of Internet users. Before this, ISPs were more or less passive movers of Internet datagrams, reading only the header information needed to deliver the packet to its destination. It was considered technically impossible for certain kinds of control to take place. As an integrated technology of control, DPI can be used for a number of different purposes. It can be used to catch malware in transit, to manage bandwidth and to identify and regulate the type of files end users are sharing with each other.

Our research will explore how regulatory institutions in different parts of the world are reacting to actual or prospective DPI implementations by internet service providers, and how those legal and regulatory reactions in turn affect the ISPs' deployment and use of DPI. In other words, we will be examining the mutual influence of technology on institutions and of institutions on the deployment of technology. The study should allow us to detect how effectively different rule-systems respond to user rights and regulatory problems inherent in the use of DPI.

5. *End*

Let me close with a sardonic vignette. You are probably all familiar with the growth of virtual worlds such as Second Life. These are online environments based on three-dimensional computer graphics where

people create alternate identities – avatars – and construct their own territories and behaviors.

In February of this year, the U.S. National Security Agency (NSA) leaked a report to the *Washington Post* expressing concerns that virtual worlds are becoming a haven for terrorists.[8] NSA is 'convinced that the qualities that many computer users find so attractive about virtual worlds – including anonymity, global access and the expanded ability to make financial transfers outside normal channels – have turned them into seedbeds for transnational threats.'

Let us overlook for the moment the unsurprising but still chilling fact that governments are not comfortable until they can spy even on our dreams. Consider this instead: even as it issues reports suggesting that online anonymity breeds criminality, the NSA keeps its budget, the names of most of its staff, and most of its activities secret. There is an obvious paradox here. If the secrecy of civilians or loose networks of transnational actors interacting in a virtual space can lead to social harms, then surely anonymity can also be abused by organizations with guns, large tracts of real estate and multi-billion dollar budgets. No doubt the NSA's advocates believe that secrecy is essential to the performance of their mission. But it obviously raises the same questions about accountability and abuse as the online actors. Who watches the watchers? This duality, which I have referenced before, goes to the heart of the problem.

There is actually some good news behind this hypocrisy. It shows that even the sworn enemies of privacy recognize the intimate relationship between the ability to be unidentified and their own security and freedom. Those who propose to eliminate or limit those rights for others, but assert it for themselves in critical circumstances, are paying

8 Robert Harrow, 'Spies' Battleground Turns Virtual; Intelligence Officials See 3-D Online Worlds as Havens for Criminals.' The Washington Post, Wednesday, February 6, 2008; Page D01.

the cause of security, freedom and privacy a backhanded compliment. Further, they prove that this is really a negotiation over how each individual's freedom is conditioned by others' freedom. It is clear that some individuals and organizations are asserting a special, privileged status in these negotiations. But it is not clear – morally, logically or practically – what entitles them to such a status.

It is of course a long and complex trek to translate the simple ideal of isonomic individual rights into large-scale governance institutions and the operational practices of Internet service providers. But we must make sure that that journey is guided by clear and well-founded principles, else we get lost along the way.

To conclude, let me express my thanks to some important people. First, to the managers and employees of XS4ALL, thank you again for being the kind of company I am proud to have associated with my academic title; special thanks in particular to Doke Pelleboer, who sits on the Chair's review committee; to Marion Koopman, the CEO; to Neil Huijbregts, an outstanding diplomat for and guide to the company; and to Scott McIntyre as an embodiment of the best of the Internet technical community. I want to recognize also Dr. Margot Weijnen, Program Director of the Next Generation Infrastructures Foundation for her support and interest in the work, and for NGI's support for the Ph.D. projects. Special thanks go to Dr. Harry Bouwman for his essential role in connecting me to TU Delft and for his constant efforts to provide the administrative and sometimes personal support needed to navigate the system here. I am also pleased to acknowledge the importance to me of colleagues from other sections of the Faculty for making this a collegial and collaborative place. There are many, and I hope there will be many more, but I must mention Dr. Michel van Eeten, Dr. Wolter Lemstra and Dr. John Groenewegen.

References

Alston, L. J. (2008). New institutional economics. In S. Durlauf, & L. E. Blume (Eds.), *The new palgrave dictionary of economics* (2nd ed.,) Palgrave Macmillan.

Anderson, R., & Moore, T. (2007). Information security economics – and beyond. *Fourth Bi-Annual Conference on the Economics of the Software and Internet Industries*, Toulouse, France.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Drezner, D. (2007). *All politics are global: Explaining international regulatory regimes*. Princeton, NJ: Princeton University University Press.

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? illusions of a borderless world*. New York: Oxford University Press.

Harper, J. (2005). Against ISP liability. *Regulation*, *28*(1), 30–33.

Hayek, F. A. (1973). *Law, legislation and liberty*. Chicago: University of Chicago Press.

Kahler, M. (Ed.). (2008). *Networked politics: Agency, structure and power*. Ithaca, NY: Cornell University Press.

Lessig, L. (2001a). The internet under siege. *Foreign Policy*, *127*, 56–65.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, L. (2001). *The future of ideas: The fate of the commons in a connected world*. Vintage Books.

Lichtman, D. G., & Posner, E. A. (2006). Holding internet service providers accountable. In M. F. Grady, & F. Parisi (Eds.), *The law and economics of cybersecurity*. Cambridge: Cambridge University Press.

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.

Podolny, Joel M. Page, Karen. (1998). Network forms of organization. *Annual Review of Sociology*, *24*, 57–76.

Powell, W. W. (1990). Neither market nor hierarchy: Network forms of organization. *Research in organizational behavior* (pp. 295–336) JAI Press.

Raustiala, K. (2002). The architecture of international cooperation: Transgovernmental networks and the future of international law. *Virginia Journal of International Law*, 43

Reidenberg, J. (2005). Technology and internet jurisdiction. *University of Pennsylvania Law Review*, 153(6), 1951–1974.

Scharpf, F. W. (1993). *Games in hierarchies and networks: Analytical and empirical approaches to the study of governance institutions*. Boulder: Westview Press.

Scharpf, F.W. (1997). *Games real actors play: Actor centered institutionalism in policy research*. Boulder: Westview Press.

Slaughter, A. (2004). *A new world order*. Princeton, NJ: Princeton University Press.

Solove, D. J. (2007). *The future of reputation: Gossip, rumor and privacy on the internet*. New Haven, CT: Yale University Press.

Sørenson, E., & Torfing, J. (Eds.). (2007). *Theories of democratic network governance*. Basingstoke, Hampshire: Palgrave McMillan.

Waever, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), *On security* (pp. 49). New York: Columbia University Press.

Weber, S. (2004). *The success of open source*. Cambridge: Harvard University Press.