ESPRIT

ORGANIZING INTERNET ARCHITECTURE

Bernard Benhamou
Senior lecturer for the Information Society at the Institute of Political Studies in Paris.
Head of mission "*Foresight and Internet governance*" Agency for the Development of e-Government.

Networks make up the new social morphology of our societies, and the logic of their mapping largely determines the processes of production, experience, power and culture… What is new today is the fact that information technology provides the base of their proliferation to the entire society.

Manuel Castells[1]

Code is law… and architecture is politics.

Lawrence Lessig[2]

The Internet has become, in a few years, one of the sources of the Wealth of the Nations and one of their most crucial infrastructures. It developed in our societies to become an essential element for education, dissemination of knowledge, culture as well as the economy. The Internet, by leveraging all the activities of production, has also become one of the drivers of corporate development. Understanding the architecture of the Internet and its repercussions on business activity covers a strategic

[1] Castells, Manuel , *The Rise of the Network Society (Information Age, 1.)* Blackwell Publishers 1996.
[2] Lawrence Lessig, *Code and Other Laws of Cyberespace*, Basic Books, 1999.

nature for all the stakeholders of what is called the Information Society, but also more widely for the general public. Moreover, questions concerning Internet Governance were at the center of the World Summit on the Information Society (WSIS[3]) organized by the United Nations. Beyond actions that would foster the development of these technologies (especially in emerging countries), one of the challenges posed at WSIS was to establish the "common base" of principles and values that should be, in the years to come, embedded in network architecture.

THE INTERNET: ANATOMY OF AN EXCHANGE NETWORK

The architecture of the Internet is in effect made of several technological, economic and political specifications that are shaping the networks usage. Thus, before being a network, or even "a network of networks," the Internet is at first a set of protocols endowed with specific characteristics. One of the "historic" definitions of the Internet was given by Ed Kroll[4] and summarizes the multidimensional nature of the network:

The Internet is:

1. **a network of networks based on the TCP/IP protocols,**
2. **a community of people who use and develop those networks,**
3. **a collection of resources that can be reached from those networks.**

This definition of architecture relates to the superimposition of "layers" with different functions. Thus for Y. Benkler[6] these three fundamental layers of the Internet are linked first to transport (physical infrastructure), then to applications (logical layer) and finally to information exchange (content layer). One of the characteristics of this architecture is the independence of the different "layers" that

[3] World Summit on the Information Society: www.itu.int/wsis/index.html

[4] Ed Kroll, "What is the Internet?" RFC 1462 from June 24, 1993 (http://mist.npl.washington.edu/internet.txt).

[6] Yochai Benkler, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access", 52 Fed. Comm. L.J. 561, 2000 (www.law.indiana.edu/fclj/pubs/v52/no3/benkler1.pdf).

make up the network.

"TCP/IP," the double protocol fundamental to the Internet, assures a separation of the transport functions and the information processing functions. This separation is one of the essential principles of the Internet: the *end-to-end* principle (or neutrality principle). According to this principle, the "intelligence" of the network is located at the edges of the network's and not centralized in the network itself, the "higher" data processing functions are then processed by computers (and users) located at the edges of the network.

It is this characteristic of the Internet's architecture that allowed "isolated" users to develop technologies which were then adopted worldwide. This was the case with HTML, which gave birth to the *World Wide Web,* and more recently with weblogs[7] as well as *peer-to-peer* systems. These exchange technologies are in fact the most recent translations of the *end-to-end*[8] principle.

This principle of a decentralized network also constitutes a profound break with the "centralized" network systems to which we had previously been accustomed, especially in France with the Minitel. A centralized architecture, in addition to making a network more vulnerable to attacks, relaxes the effort of creating new services on a limited number of players and thereby deprives its users of numerous opportunities for innovation (as beneficiaries but also as contributors as is the case with the development of open source software). On the other hand, networks that adopt the *end-to-end* principle are "neutral" and can only transport information without modifying it (which is why this principle is also called the "neutrality" principle). The network therefore constitutes a platform of common expression, a "commons," which allows

[7] "A web log, which is usually shortened to blog, is a type of website where entries are made (such as in a journal or diary), displayed in a reverse chronological order. Blogs often provide commentary or news and information on a particular subject, such as food, politics, or local news; some function as more personal online diaries. A typical blog combines text, images, and links to other blogs, web pages, and other media related to its topic. Most blogs are primarily textual although some focus on photographs (photoblog), videos (vlog), or audio (podcasting), and are part of a wider network of social media." Definition from the online encyclopedia *Wikipedia* (http://en.wikipedia. org/wiki/Blog). Read also: Bernard Benhamou : "Le projet Proxima. Pour une appropriation de l'internet à l'école et dans les familles" (annex on web logs and syndication, www.educnet.education.fr/ plan/proxima.htm).

[8] David D. Clark and Marjory S. Blumenthal, "Rethinking the design of the Internet: The end-to-end arguments *vs*. the brave new world,"25th Telecom Policy Research Conference, 2000 (www.tprc.org/abstracts00/rethinking.pdf).

all users to develop new content and new services.[10]

This principle also has consequences on the economic functioning of the network. In fact, by encouraging competition at the "edges" of the network, it maintains equality of access to the network for new entrants while preserving the unicity of the network's basic functions. This principle notably protects the network from appropriation by certain corporations or sectors to the detriment of all its users.

It is also this principle that gave the Internet its flexibility in developing content and applications, and allowed it to become, in the space of several years, the most important network of people and content. To allow networks to develop, one must preserve the unity of the Internet without imposing a uniformity of uses of services or technologies. It is also important to note that for the first time during the WSIS process, the 25 countries of the European Union explicitly wished to protect, at the United Nations, the three fundamental principles of the architecture of the Internet, which are interoperability, [11]openness and the *end-to-end* principle.[12]

PERSPECTIVES ON THE INTERNET ARCHITECTURE: UNICITY OR UNIFORMITY?

The current architecture of the Internet is not at all an immutable fact related to the "nature" of the network. The temptations to change this architecture for economic

[10] Howard Shelanski, "Three Constraints on Net Neutrality Tradeoffs with the 'End-to-end' Principle," Berkeley, University of California, February 8, 2004 (www.pff.org/weblog/Shelanski_ Boulder04.pdf).

[11] "Interoperability is the ability of products, systems, or business processes to work together to accomplish a common task. The term can be defined in a technical way or in a broad way, taking into account social, political and organizational factors." *Wikipedia* (http://en.wikipedia.org/wiki/Interoperability). As recent debates on authors' rights with the draft of the DADVSI law in France have shown, the interoperability of software and file formats is a critical issue for all the stakeholders of the Internet. Thus, the legal obligation of interoperability, which aims to make downloaded music readable by all players, sparked an intense debate on industry evolution of the Internet and the evolution of network cultural practices. Read the editorial by David Lazarus, "Apple not happy, but French may be on right track," *San Francisco Chronicle*, March 26, 2006 (www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/03/26/BUG4CHTPEF1. DTL). In the future, activities connected with the interoperability of software and data formats must be the "hard core" of the regalian functions of the States concerning the architecture of the information society.

[12] See the proposal by the presidency of the European Union during the preparation for WSIS (www.itu.int/wsis/docs2/pc3/contributions/sca/EU-28.doc).

or political ends are many, and they come from both the industry players most involved in the management of the Internet[13] and certain governments[14] who see it as a convenient way to reestablish political control over the networks.

In fact, the network, which was originally designed to resist certain forms of localized attacks, could not (in its current form) withstand a change of its fundamental protocols[15]. Any change of the architecture of the Internet, partial or local, could have heavy consequences on the future development of the network and further on the progress of all our societies.

The *end-to-end* (or "transversal") architecture of the Internet was at the origin of its success, but centralized (or "vertical") architectures have undeniable economic advantages for their promoters when it comes to controling the "value chain" [16]. These integrated networks allow to control each step of the services offer and extending such control to areas previously separated from the Internet (television, fixed and mobile telephony and also video distribution). This is why many companies wish to implement such "integrated" [17] networks, which allow to link and control, in a given geographic area, the infrastructure and the offer of services and content. [18] This integration would be a critical change in the general dynamic of the network.

This evolution towards the "vertical convergence" of networks would sanction

---

[13] On this point, see the report given on the *WildCard* change provided by Verisign. "The Site Finder Report: Dr Stephen Crocker, Chair of the Committee", *CircleID*, July 15, 2004 (www.circleid.com/article/647_0_1_0_C/).

[14] See Shanthi Kalathil and Taylor C. Boas, *The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution*. CEIP report, July 2001 (www.ceip.org/ files/pdf/21KalathilBoas.pdf).

[15] It is important to note that several times, industry or government stakeholders wished to change this architecture. See in particular the controversies with the Chinese authorities regarding protocol IPv9: "Explaining China's IPv9" in *CircleID* July 6, 2004 (www.circleid.com/article/646_0_1_0_C/). See also "Towards a Common Understanding of the Roles and Responsibilities of all Stakeholders in Internet Governance," text by the Workgroup on Internet Governance (WGIG) put in place by the United Nations (www.wgig.org/docs/WGIGpaperStakeholders.pdf).

[16] Carl Shapiro and Hal Varian *Information Rules*, Harvard Business School Press, 1998).

[17] On this point, see controversial issues of Next Generation Networks in Ross Rader, "Internet to ITU: Stay Away from my Network", *CircleID*, December 21, 2004 (www.circleid.com/article/842_0_1_0_C).

[18] One of the recent examples of these conflicts on the principle of neutrality concerns the installation of "tiered Internet" by certain telecom operators for certain added-value services like video. This debate, which was taken up again in the American Senate, should determine the limits and the nature of the regulatory activities of the States on the architecture of the Internet. Dossier News.com, "Net Neutrality Showdown," April 2006 (http://news.com.com/ Net+neutrality+showdown/2009-1028_3-6055133.html).

a transformation from a two-way exchange architecture to a one-way broadcast architecture. This could lead to questioning certain types of applications and therefore certain uses of the network, but it could also lead to instituting the concept of "privileged" broadcasters and "passive" receptors. We could therefore witness a "televisualization" or "broadcastization" of the Internet.[19] These new architectures could also have major macro-economic consequences, because they could lead to a fragmentation of the Internet and thereby reduce the global value of the network for all economic players.[20]

In fact, up to this point, the Internet has been a "neutral" platform and has benefited from financing shared by all the industry stakeholders. The fragmentation of the Internet could also lead to a rethinking of this financing model for the benefit of only the most profitable "infrastructure segments" of the network.

The other fundamental characteristic of the Internet that could be challenged by these evolutions is its plasticity, and therefore its ability to generate new links between the various "nodes" of the network. The current set-up of the network offers the advantage of allowing permanent re-combinations between user groups and between applications that are located on the network. Programmers and users of the network can thereby experiment directly on a large scale with new social, cultural and economic practices. As the phenomenon of fragmentation of the Internet sets in, those re-combinations could become increasingly difficult. This rigidification (or ossification) of the network would encourage the breaking down of the Internet into a series of islets. These islets and archipelagoes could become self-sustaining, with the

[19] But unlike television, the economic engine of these evolutions is not only the "massification" of audience, but also a more elaborate form of collecting and handling personal information. These networks would provide users with low-cost personalized content and services; it's the principle of "mass customization." One of the last evolutions in online audiovisual broadcast concerns *podcasts*, which are now used by all traditional radio stations to air their broadcasts and by the internauts who produce and broadcast their own audio or video programs. "Podcasting " differs from radio broadcasting and webcasting in the broadcast of sound or video, not by a centralized mechanism that sends a stream to its listeners, but by the actions of listeners who look for audio files themselves. The authors of these broadcasts publish audio files that are similar to classic radio broadcasts. It is then up to individuals to create their own reading list through their various subscriptions. The downloading of programs, from the various sources they have chosen, is then automatic. *Wikipedia* (http://fr.wikipedia.org/wiki/Podcasting).

[20] Thus Metcalfe's Law (from the name of the inventor of the "Ethernet" protocol) states that the value of a network is proportional to the square of the number of users of the system.

risk of permanently isolating whole sections of the Internet. These phenomena could also lead eventually to an actual stagnation of the exchanges between the islets thus created and consequently restrict the variety of content and usage of these networks. The consequences of these evolutions will not only be technical or economic, but also political. In addition to changing the physionomy of the network, these transformations would have an impact on the very idea of the power of control of the Internet. Their impact on the circulation of ideas could be particularly intense. In fact, users of these islets would only come in contact with people and ideas that are already familiar to them and become more and more impervious to unfamiliar ideas. This is what makes constitutionalist Cass Sunstein predict that the radicalization of political opinions expressed on the Internet, the "group polarization"[21], could intensify while this fragmentation would become a reality.

The risks of fragmentation or of rigidification of the Internet will therefore have to be taken into account on every level, and on an international scale. Generally, the preservation and development of the Internet will require the implementation of an international coordination among the stakeholders and regulators of the Internet.

MAPPING THE INTERNET: THE NEW "SCIENCE OF PRINCES?"

Another key element of the architecture of the Internet is linked to one of the rare centralized structures of the network: the management of domain names (*Domain Name System* or DNS). Each computer connected to the Internet is in fact identified by a numerical address (for example 143.126.211.220). Rather than using a numeric

[21] "First, people should be exposed to materials that they would not have chosen in advance. Unplanned, unanticipated encounters are central to democracy itself. Such encounters often involve topics and points of view that people have not sought out and perhaps find quite irritating. They are important partly to ensure against fragmentation and extremism, which are predictable outcomes of any situation in which like-minded people speak only with themselves. I do not suggest that government should force people to see things that they wish to avoid. But I do contend that in a democracy deserving the name, people often come across views and topics that they have not specifically selected." Excerpt from Cass Sunstein, *Republic.com*, Princeton University Press, 2001.

identifier, as is still the case with telephones, Internet users type in domain names (like www.airbus.com). The DNS then converts the domain names to numeric addresses, thereby making sense of the numeric addresses of the machine connected to the network. The first architects of the Internet designed this system around thirteen machines, called "root servers," which sustain several thousand relay servers all over the world. It is these DNS machines (root servers and secondary servers) that respond to requests from users who want to visit a Web site or send an email.

The distribution of root servers is still very unequal since ten of them are located in the United States and only two in Europe. All of the architecture of the DNS is currently managed by Icann[22], a California not-for-profit corporation established by the United States government in 1998. It is the "root A" server that controls the distribution of the different domains according to their geographic zone (for the codes of different countries, like the root ".fr" for France or "de" for Germany) or according to their general type of activity (com, net, org, aero, etc.). But it should be noted that since the creation of Icann, the "root A" (or Root Zone File) is still directly controlled by the United States Department of Commerce.

The management of the DNS, then, is the thematic and functional mapping of the Internet. The concepts of Internet governance and DNS governance have long been confused. In fact, current forms of Internet governance are directly linked to the architectural specificities of the Internet and in particular of the DNS. If the architecture of DNS had been designed from the outset to facilitate the operations of setting up and maintaining the network, this centralized architecture became the target of much criticism when it proved to be the base of a political power on the networks. In fact, this architecture would in theory enable the administrator of the DNS to "erase" the resources of an entire country from the map of the Internet. [23]

So one of the essential objectives of the WSIS was to establish the management of these critical infrastructures in a multilateral, transparent and democratic framework. With this in mind, the countries of the European Union presented a

[22] Internet Corporation for Assigned Names and Numbers (www.icann.org).

[23] Similar concerns were raised about the control of satellite navigation systems. It is in fact possible in the United States to change (for example in times of war) the data transmitted to all GPS users (*Global Positioning System*). See "U.S. concerned China plans its own satellite navigation system," *Computer World*, June24, 2003 (www.computerworld.com/printthis/2003/0,4814,82464,00.html).

unified position that aimed to place the management of these critical resources of the Internet under the joint control of the States and no longer under the sole jurisdiction of the United States Department of Commerce. This "middle ground" proposal was at equal distance from the position of *status quo* supported by the United States and that of countries like China or Iran who wished to place the entire Internet under state control. The idea of a possible loss of control over these critical resources drew the hostility of the the United States, as was made clear by the intense diplomatic and media campaign that was mounted against the European proposal.[24] However, a compromise on Internet governance was established at the end of the Summit.[25] A double process was thereby established to allow all States to cooperate on equal footing to manage these infrastructures, which are critical to their economies and sovereignty. The first phase of the initiatives established by the United Nations is "enhanced cooperation", which will support the supervision of the critical infrastructures of domain names. The second initiative will be the creation of a Forum on Internet governance, which must encourage exchanges, debates and information sharing on important questions of Internet usage.

POLITICAL, ECONOMIC AND CULTURAL ISSUES...

Long considered a "central and intangible" element of the Internet, the DNS now appears to be one of the network services on par with the Web or email. Other navigation structures of research and data exchange on the Internet would be able to place themselves next to existing systems. On the Internet, "commercial" navigation tools thus become key elements of architecture of the network. Like search engines such as Google, new navigation systems on the Internet could even claim one day to

[24] In a letter addressed to the British presidency of the European Union, Secretary of State Condoleezza Rice "asked the European Union to reconsider its recent position on Internet governance," and did so in terms deemed "unusually strong" by well-informed diplomats. See : Read the letter that won the internet governance battle (The Register 2nd December 2005) (*http://www.theregister.co.uk/2005/12/02/rice_eu_letter/*)

[25] See TUNIS AGENDA FOR THE INFORMATION SOCIETY http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

replace the DNS.[26] Search engines will soon index all forms of expression and transmission of human knowledge. At this point, they have become so critical on an economic and strategic level that they could even become the subject of specific new regulations.[27] It is important to note that it was Google's project for the digitization of literary heritage (Google Book Search project) that was the deciding factor for the launch of a European digital library by the countries of the EU. In their letter to the President of the European Union, the heads of State and of Government of the six signing countries (France, Germany, Spain, Poland, Italy et Hungary) recalled, again with a "geographic" metaphor the cultural issues of this project: "*If it is not digitized and made accessible online, this heritage could, tomorrow, fail to fill its just place in the future geography of knowledge."* [28] But, as Bibliothèque nationale de France President Jean-Noël Jeanneney[29] pointed out, in the face of a constantly evolving network, choices regarding the technological architecture of the European project will be crucial to insure both its validity and durability.

As innovations come to light, in terms of naming or addressing services[30] on the Internet or in search engines[31], navigation tools on the Internet will have to evolve, and with them the processes for the regulation of the Internet. In the same way, the increasing importance of mobile uses of the Internet, the diversification of connected

---

[26] This is the case with the new identification system for "digital objects" (*Digital Object Identifier* or DOI) designed by one of the inventors of the Internet, Dr Robert Kahn (http://en.wikipedia.org/wiki/Digital_object_identifier).

[27] "Should abuses grow, search services could find themselves under increased public pressure for government scrutiny or facing more disputes and criticism concerning such activities from other commercial entities." See the report by the National Research Council, *Signposts in Cyberspace: The Domain Name System and Internet Navigation* (http://www7.nationalacademies.org/cstb/dns_prepub.pdf).

[28] Excerpt from a letter dated April 28, 2005 to European Council President Jean-Claude Juncker, and European Commission President Jose Manuel Barroso, to jump-start the European digital library project.

[29] "Does Europe need to mount its own search engine or several that enable it, on a planetary scale, to insure enduring a competition in this capital domain? Or should it only aspire to a powerful digitization effort that gives it the possibility of imposing its conditions upon entry?" in Jean-Noël Jeanneney, *Quand Google défie l'Europe*, Paris, Mille et une nuits, 2005, see also "Une grande bibliothèque virtuelle?" interviews from *Libération*, May 3, 2005 (www.liberation.com/page.php?Article= 293886).

[30] John C. Klensin, "*Role of the Domain Name System (DNS)*" (www.ietf.org/internet-drafts/draft-klensin-dns-role-05.txt).

[31] Sergey Brin and Lawrence Page, "*The Anatomy of a Large-Scale Hypertextual Web Search Engine*" (www-db.stanford.edu/~backrub/google.html).

devices or even the development of peer-to-peer systems could also have a significant impact on the architecture and the governance of the Internet. This is why the United Nations now favors a wide (and necessarily dynamic) definition of Internet governance. This definition integrates both new uses of the Internet and aspects of security and trust on the networks. [32]

TRUST: THE CORNERSTONE OF INTERNET DEVELOPMENT

At a time when, in our societies, entire sectors of economic activity (and of services of the States) are based on the Internet, the stability of the networks becomes one of the fundamental issues of Internet governance. The Internet thus adopts the shapes and contours of the States when their essential functions require the use of the network.[33] In this sense, the fundamental instruments of sovereignty will soon become indistinguishable from the tools of technological power. The risks of computer attacks on the "critical infrastructures" of the Internet (especially the DNS), which only appeared to be "theoretical," are now daily issues for the network architects. The stability of the network thus becomes a critical element for all Internet users (be they citizens, organizations or States). Trust will be in fact the keystone of the development of the Internet. Thus, in the face of the growing power of "system pathologies," which are viruses, computer attacks and even *spam*, a triple coordination must be arranged bearing on technological and legal measures and also the sensitization of Internet users. Because they are generated by the network users themselves and not from "exogenous" factors, these pathologies will not be able to be warded off definitively. In the absence of an appropriate response, these phenomena could even bring into question the economic and social dynamic of the networks. In fact, if the network

[32] Klaus Grewlich (German Ambassador to the United Nations), "Internet Governance, Definition; Governance tools; Global Multi-stakeholder entity," UN ICT Task Force, April 2005 (www.unicttaskforce.org/perl/documents.pl?do=download;id=784).

[33] Closing intervention by M. Nitin Desaï, Special Representative of the Secretary General of the United Nations for the WSIS, Working Group on Internet Governance, Geneva, April 18, 2005 (www.wgig.org/April-scriptafternoon.html).

hasn't had a "growth crisis" until now, phenomena like *spam* or even viruses could, in return, be at the root of a "crisis of trust", such that it would bring into question the general development of networks in our societies.

HYPERCONTROL OR MASS IRRESPONSIBILITY?

Other changes in the architecture of the Internet could be linked to conflicts around intellectual property on the networks. Thus, one of the risks associated with the criminalization of peer-to-peer exchange would be to push users to adopt more "radical" exchange systems. In fact, technologies of peer-to-peer systems, when they are coupled with encryption technologies, produce "third generation" [34] peer-to-peer networks that are even more difficult to control and potentially more unsettling. Made by programmers who are anxious to avoid censorship, especially in non-democratic regimes, [35] these networks could present new difficulties to public authorities. Such is the case of FreeNet, [36] which makes it possible to share files that are encrypted, copied and fragmented on the hard disks of all its users. Users of FreeNet are constrained by the "nature" of the system not to know the nature of the content placed on their hard disks by other users. The development of this type of technology could present important problems in the case where illegal files would be present on computers unbeknownst to their owners. At a time when citizens are developing many new forms of expression on the Internet, to support a "mass irresponsibility" would be a democratic regression. In fact the interconnection of networks already increases the risks of illegal content dissemination as well as the risk of affecting key infrastructures of the Internet. For some States, these developments could be the starting point for a reconsideration of the architecture of exchange on the Internet.[37]

---

[34] http://en.wikipedia.org/wiki/Peer-to-peer#Third_generation

[35] "More on file-swapping networks than just songs," *News.com*, April 25, 2005 (http://news.com.com/2102-1027_3-5682539.html).

[36] Theodore W. Hong and Ian Clarke, "The Persistence of Memory in Freenet" (www.doc.ic.ac.uk/~twh1/academic/papers/iptps.pdf).

[37] *Cyber Security: A Crisis of Prioritization*, report from the PITAC, February 2005 (www.itrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf).

VIRTUAL OBJECTS AND REAL FREEDOM…

The networks (and even more so their architecture) become "political objects" as they are incorporated into the everyday lives of citizens. Thus, technological developments (like the passage from the fixed telephone lines to mobile phones) have already made it possible to pass from a network through the home to a network through the individual. Connected objects will gradually weave a framework around individuals (even inside individuals[38]) that will accompany all their actions[39]. The next generation of services will establish this major transformation of the Internet; the network could therefore evolve from an "Internet of streams" (where an essential part of the connected devices are computers) to an "Internet of things" that will connect all the objects of everyday life.

Beyond the DNS, whose primary function was to identify computers, new kinds of tracking and connection of everyday objects will guide the development of the new directories of the Internet.

In the future, bar-codes will also be gradually replaced by "contactless" chips on all manufactured products and will give access *via* the Internet to dynamic data updated on each object (data on the origin, shipment of the merchandise, traceability, etc.). These links between objects and their specific data rests on the development of a new technology derived from the DNS: the *Object Naming Service* (or ONS). The social consequences of these technological developments are still difficult to predict.[40] So, when the American authorities decided to integrate a RFID[41] chip in passports, organizations for the defence of civil liberties, as well as industries tied to tourism, reacted to the risk of "involuntary identity collection," and saw in this technical

[38] Computerising the body: Microsoft wins patent to exploit network potential of skin (The Guardian Tuesday July 6, 2004) http://technology.guardian.co.uk/online/news/0,12597,1254911,00.html

[39] Howard Rheingold, *Smart Mobs: The Next Social Revolution*, Perseus Publishing, 2002.

[40] Mark Monmonier, *Spying with Maps: Surveillance Technologies and the Future of Privacy*, University of Chicago Press, 2002.

[41] Radio Frequency Identification: "Identification by radio frequency is a method of remotely stocking and recuperating data by using markers called RFID tags."

innovation the possibility of making "each American citizen abroad a living target…" [42]

Beyond data streams, control of the DNS (and ONS) will thus extend to the movements of individuals, as well as that of goods and merchandise. Be it sovereignty, civil liberties or economic control, the political stakes of this "Internet of things" [43] will be considerable. More still than with the "Internet of machines," it will thus be necessary that this "Internet of things" be under the control of citizens. They must be able to control the way in which their personal data are used, and even the way in which these chips can be deactivated. So in the future, citizens will have to intervene in the architecture of these systems in order to enjoy a new kind of freedom: the "silence of the chips."

TOWARDS A CONSTITUTION FOR THE INFORMATION SOCIETY? [44]

The architecture of the Internet, like the architecture of our cities, carries a political message, and all Internet stakeholders must therefore be linked to the definition and evolution of this architecture. This is necessary in order to etch (or embed) the principles to which we are attached within technologies, and beyond in the "common base" of Internet governance.

Technological determinism does not exist in these areas, and the evolution of the Internet in our societies will be directly linked to the technological choices we implement. We will have to create a culture of governance of technologies in order to implant ideas in the education of the general public that they will need for citizenship in the information society. An increased transparency in terms of Internet governance must also go hand in hand with a greater transparency of technologies, content and services accessible on the network. This transparency will in particular enable

[42] Sara Kehaulani Goo, "Privacy Advocates Criticize Plan to Embed ID Chips in Passports," *Washington Post*, April 3, 2005 (www.washingtonpost.com/wp-dyn/articles/A21858-2005Apr2.html).

[43] *ITU Internet Reports 2005: The Internet of Things* (report by the International Union Telecommunications on the "Internet of things:" www.itu.int/osg/spu/publications/internetofthings).

[44] See Lawrence Lessig, *Cyberspace's Architectural Constitution*, Amsterdam, WWW9, 1999 (http://cyber.law.harvard.edu/works/lessig/www9.pdf).

networks to avoid being perceived by citizens as a threat to their privacy and freedoms.

Finally, we must establish an Internet governance, and therefore an architecture of the Internet, that is true to the principles and values shared by all citizens. This is why the information society (like bioethics or nanotechnologies) must be the subject of a large democratic debate. This debate, far from being just "technical," will be essential for determining how exchanges and the broadcasting of ideas, or even new forms of social or political organizations, will take shape.[45]

[45] It is the mission that was just entrusted to the Secretary General of the United Nations at the Forum on Internet Governance, which will meet for the first time in November 2006 in Athens.