SOCIAL AND ETHICAL ASPECTS OF IPV6

Chris Zielinski

Independent Consultant, Geneva, Switzerland, czielinski@supanet.com

Abstract: The Internet Protocol version 6 (or IPv6) is designed to replace the current version (IPv4), which is now over 25 years old. Three main categories of social and ethical issues arise in connection with IPv6: issues relating to the right to an IP address, issues related to the application of the technology, and issues related to governance. There are many societal benefits of IPv6, as it will enable once more to have end-to-end security of transmission. Nevertheless, the governance of this deployment now and in the coming years needs to be neutral and controlled, and the governance of the IPv6 Internet that emerges after deployment must be transparent and accountable. Any mistakes we make now will be very costly in terms of loss of existing personal freedoms. This paper will explore these issues.

1. INTRODUCTION

Most of the ethical and social issues that arise in the use and development of the Internet have to do with access to and integrity of information (whether personal or public). It can be argued that most of these issues arise in the analogue world as well, and that they are not the products of technological advance.

Nevertheless, there are issues which have been completely transformed by the introduction of digital technology, either in their nature and scope, or as a result of a massive change in scale, such as those which, it will be argued, will be experienced in the shift from the Internet based on IPv4 and that enabled by IPv6. These issues are the subject of this paper.

In a short Request for Comments on “Ethics and the Internet” written in January 1989 by the Network Working Group, Internet Activities Board (RFC 1087), it was possible to say, “Access to and use of the Internet is a privilege and should be treated as such by all users of this system”. The notion that access to the Internet was a privilege was perfectly acceptable for something which was seen as a resource used exclusively for academic research. In the scant years since the publication of this RFC, many people consider access to and use of the Internet as a *right*, largely on account of its extraordinary diffusion since then.

The RFC further endorsed a US National Science Foundation statement which “characterized as unethical and unacceptable any activity which purposely:

1. seeks to gain unauthorized access to the resources of the Internet,
2. disrupts the intended use of the Internet,
3. wastes resources (people, capacity, computer) through such actions,
4. destroys the integrity of computer-based information, and/or
5. compromises the privacy of users.”

The first three of these activities would be expressed differently today. “Unauthorized access” would have to be qualified (for example, as a property right associated with a website which is compromised by a hacker), to remove the impression that someone had the authority to allow “access to the resources of the Internet”. “Intended use” suggests that someone was able to state for which use the Internet was intended (now we would talk more specifically about “denial of service attacks” and the like). Even the waste of resources might now be held to be a personal or cultural choice (is the Jennycam¹ a waste of resources or contemporary art?). The issues related to integrity of information and privacy of users have persisted to this day, albeit in a greatly expanded form.

2. IPV6: OPENING THE DOORS TO THE INTERNET WORLD

Vinton Cerf and Robert Kahn published the Transmission Control Protocol/Internet Protocol (TCP/IP) in 1973. In 1978: TCP/IP was split into its separate components, TCP and IP, and in 1983, the Domain Name

¹ The Jennycam started in 1996 and beamed non-stop webcam pictures of Jenny’s mundane doings while consuming impressive bandwidth

System (DNS) was invented, establishing the rules for associating such Domain Names as www.iwsp.org with IP addresses such as 212.234.238.114.

The IP system provides a routing address on the Internet, while domain names are ways of giving these addresses some kind of easily recognisable identity. The strings of characters used in domain names often (but not necessarily) spell out an acronym, word or words which generally convey some meaning in natural language. Websites are generally both named and numbered, but networked devices (web and mail servers, home PCs) using IP addresses do not need domain names.

The fundamental principle of the Internet Protocol is that communicating devices anywhere on the Internet have unique IP addresses, so that data packets can be carried (routed) between the devices across one or more ISP networks.

When IPv4 was designed in the 1970s, 32 bits were used to represent IPv4 addresses. Mathematically, this allows for 2^{32} , or 4.3×10^9 (4.3 billion, or 4,294,967,296 to be exact) addresses. However, the number of addresses available is actually less since the full range of IP addresses cannot be utilized. Large allocations were made per ISP or per site in the early days of the Internet. A European Commission report asserts that “74% of the IPv4 address space is already allocated to organizations in North America (15% to the US government alone); the Universities of Stanford and MIT each have more allotted addresses than the Peoples Republic of China.”² While this may overstate the actual situation, it is still the case that the IPv4 address space is finite in size and continues to be consumed rapidly as the Internet spreads further throughout the world.

A mechanism that provides local site addressing, known as Network Address Translation (NAT), is used to “stretch” the number of IP addresses available globally under IPv4. NATs switch addresses dynamically, so that effectively you do not need to have a fixed address at either end of a communication. One effect of NATs is that they set a limit on the amount of addresses that a network can handle to 16 million addresses (and in practice,

² Next Generation Internet: Priorities for action in migrating to the new Internet protocol IPv6, Communication from the Commission to the Council and the European Parliament, COM(2002) 96 final, Brussels, 21.2.2002. This report clearly shares authorship (including entire sentences and paragraphs) with the Main Task Force Report of the IPv6 Task Force (11.02.2002, version 1.76, document number 70 available at <http://www.ipv6-taskforce.org/>

private networks operating under IPv4 will struggle to handle more than 5 million).³

Worse, the use of NATs is also one of a number of IPv4-based “fixes” that offend against the principle of “end-to-end transparency”, applied since 1973. Transparency requires unique logical addresses and datagrams which do not change in transit. When end-to-end transparency is absent, the security or transmissions cannot be guaranteed from one end of the transmission to the other. There are “security blind spots” lurking within NATs and intranets behind firewalls.

Coming to the rescue, IPv6, which has been in development since the early to mid 1990s, uses 128-bit addresses: it can therefore provide globally unique IP addresses to 2^{128} , or over 3.4×10^{38} (340 billion x billion x billion x billion) IP addresses. Where IPv4 allows just under 1 address per person, IPv6 allows just under 10^{29} addresses per person: enough for every cell in every human body to be a website with its own name and address.

In raising the question of internet protocol (IP) addresses in public debates, whether in developing or industrialized countries, whether among quite technologically aware netizens or among novices, some audiences start to laugh at what sounds like the boastful gigantism of future projections of Internet use. The suits with wearable chips demanding to be taken to the cleaners, the intelligent toasters adjusting themselves for each family member, the self-replenishing fridges, the implanted medicine dispensers or Big Brother-ish tracking devices. For some, all this continues to have the air of a Buck Rodgers fantasy: fanciful or foolish, unlikely or simply undesirable.

We may be amused by some of the more fanciful visions of the future, but the future will be upon us none the less. As a matter of fact, in many cases it is here already. For example, LG Electronics has been selling a “webified” kitchen in South Korea with a 15’ LCD screen in the door “so you can not only download recipes but watch TV while you’re cooking...” If dinner isn’t coming out quite right, you can use the fridge’s built-in video camera to open a video conference to your mom’s kitchen’ ...[With another manufacturer’s Whirlpool web fridge] you can use the Web tablet in the den to preheat the oven and start the dishwasher...Xybernaut has 700 patents for wearable computing devices...Raymond Kurzweil is apparently serious

³ Main Task Force Report of the IPv6 Task Force (11.02.2002, version 1.76, document number 70 available at <http://www.ipv6-taskforce.org/>

about retinal implants, not to correct vision problems but so you can 'enter virtual worlds'.”⁴

In the European Commission (EC) paper already cited⁵, the following applications of IPv6 are mentioned:

- Mobile Internet (3G mobile communications, peer-to-peer communications, wireless machine-to-machine communications and LANs)
- Novel forms of interactive multimedia services over broadband access infrastructure
- Voiceover IP (VoIP) or Internet telephony
- Homes, offices, cars and other environments may all contained many IP-enabled devices in the near future
- Remote home-management applications (multiple web cameras, or wireless temperature sensors)
- Always-on environments (such as residential Internet through broadband, cable modem or satellite)
- Rather than connecting temporarily via dialup with a temporary IP address taken at random from a pool, users and applications of the future, need permanent connectivity with dedicated IP addresses.

The paper also notes that “IPv6 projects totalling Euros 55 Million of Community funding is currently operational, including two large-scale IPv6 trials, namely 6NET and Euro6IX...The first IPv6 deployments began in 1996, from which emerged the 6bone IPv6 test bed network, now spanning over 50 countries and 1,000 sites”.

Thus, whether anyone likes it or not, IPv6 is on its way, and a growing band of technologists and visionaries are mapping out the applications of the future, some of which are rolling out today.

The present discussion is not intended to speculate about or promote any one vision of the future deployment of IPv6. Irrespective of one's attitudes towards the desirability or value of the technology, it is important to explore the possible social and ethical consequences of deployment and non-deployment.

⁴ The Webified Kitchen, Trends and Quick Takes, page 9, *Cites & Insights: Crawford at Large*, July 2002, quoting the March 2002 *Computer Shopper*.

⁵ European Commission, *op cit*.

3. ETHICAL, SOCIAL AND POLICY ISSUES

Four main categories of social and ethical issues arise in connection with IPv6:

- The right to Internet address space
- Security
- Applications of the technology
- Issues related to governance

3.1 The Right to an IP Address

As mentioned above, IP addresses are numbers while domain names can be recognisable words. There have been extensive discussions and debates regarding domain names – particularly when two or more individuals or companies lay claim to the same or similar names. Some of these debates turn on issues related to free speech and personal identity. What relationship do such issues have to IP addresses?

First it should be appreciated that naming depends on and is constrained by language, rather than technology or IP addresses. As more people, companies and other entities seek to establish a web presence, the arguments about names will increase. If each of the 9 billion people expected to be on the planet in 2005 want to have a website (and perhaps several, for their home companies and other uses) a) they will need IPv6, as they cannot be accommodated using IPv4, and b) they will need to find satisfactory solutions to the naming problems.

Thus, providing more IP addresses only has a tangential effect on the naming problem, insofar as it enables it to get worse by removing restrictions: everybody can get on board, thanks to IPv6. But the problem does not really depend on the technology, nor is it likely that the solution will be found in technology.⁶

After satisfying the needs for billions of websites, the main uses for trillions of IP addresses will no doubt be to allow networked devices to speak with other networked devices, thus enabling the “Semantic Web”. These uses and the social and ethical issues arising from them will be discussed in later sections.

⁶ One apparently permissible solution would be to use distinct images instead of names for domains (Dominic Pinto, personal communication)

Here we will focus on the remaining subset of issues that arise in relation to the question, Do people have a right to an Internet address? This question relates to the notion that owning an Internet address is akin to having the right to free speech. In a sense, you need an Internet address to express your personality online. We will examine this assertion below.

3.1.1 The right to access the Internet and the right to have an Internet presence

Irrespective of the more fanciful possibilities of future Internet use, the need for IP addresses is related to providing equitable access to the Internet. First, let us consider if access to the Internet is a human right.

The line of argument is as follows: If education is a human right, then there must be a right to access information essential for education and human development, and thus to media providing such information, including the Internet.

The right to education is explicitly enshrined in the Universal Declaration of Human Rights (UDHR). Other related rights defined in the UDHR include those of “expressing opinions”, and having access to art, culture and science.

In general, however, there is no such thing as an access right to information. Some national jurisdictions provide Freedom of Information clauses to grant citizens the right to access specific categories of government-held and/or produced information. All international and most national copyright laws and treaties allow exceptions and limitations to copyright laws allow forms of access to information for the purposes of education, citation and the like. And the public domain is growing largely thanks to proactive initiatives on the part of academics. But an explicit right of access to information essential to human development is so far absent from the international treaties and conventions.

Many declarations and manifestos have pushed the case for a right to access the Internet. This also is the explicit or implicit assumption in all the efforts to “bridge the digital divide” and eliminating the gap between the “information rich” and “information poor”. This right is contained in UNESCO’s Recommendation on Multilingualism and Universal access in

Cyberspace⁷, which was ratified by the UNESCO Conference and tabled as a key contribution to the World Summit on the Information Society (WSIS).

Apart from the right of access to the Internet, there is the question of what you have a right to do when you get there. We have already discussed the “passive” right of access to information and education – in the sense that you can *receive* information. How about the right to *transmit* information? The right to “express opinions”, in the Universal Declaration of Human Rights has been mentioned. Discussions of information provision assisted by information and communication technologies often stress the need to provide for two-way communications – an uplink as well as a downlink, the right to respond to messages received, so that the result of the medium is not just to emit advertising. This is the case in relation to the digital divide and information provision in developing countries, as well as in connection with e-government (online voting and citizen-government interchange).

If there is a right of access to the Internet, and a right to communicate on the Internet, then it can surely be argued that there is a right to have a personal presence on the Internet, up to the point of having a right to an IP address.

As the importance of the Internet in storing personal information and enabling various aspects of personal and social life expands with the roll-out of IPv6, the time will surely come when having a presence on the Internet in the form of your own web space associated with your own IP address will be considered as much a human right as the right to have a presence and occupy “meatspace” in the analogue world.

3.1.2 The concentration of addresses in industrialized countries

The core technology powering the Domain Name System (DNS) is focused at the Root Servers, which are the basic backbone of the Internet. While the concentration of DNS Root Servers is striking – there are 10 in the USA, 2 in Europe (London and Stockholm), and 1 in Japan – this is more an authority and governance question than one of restricting volume.

The shortage of IP addresses clearly arises as an ethical and societal issue in considering the scope for increasing the participation by people in developing countries.

⁷ UNESCO’s draft Recommendation on Multilingualism and Universal Access in Cyberspace

Less than 10% of the world currently has access to the Internet⁸. Given a world population estimated at 6 billion (9 billion in 2050), it is clear that each person on the planet could not have an IP address even now. Most of these digitally disenfranchised people are currently living in developing countries. While they may have more pressing issues to face than surfing the net, even if they wanted to participate in the digital revolution, they currently could not participate to the extent of their peers in industrialized countries owing to a lack of IP addresses under IPv4.

It should be noted that, from the perspective of developing countries, the value of access to the Internet focuses is not about being on the web. As Alan Levy wrote on the GKD list⁹,

“Being ‘online’ is only one of the tools... the Internet Protocol itself, running over the electronic (Internet) pipeline, and that offers low-cost communications applications such as VoIP, voice/text mail, electronic ID’s, electronic payments, online filings, etc., is more highly valuable to our Southern neighbors than the web itself. In fact, e-government and distance education are the only other vital requirements... which requires little bandwidth... Future growth in ICT adoption lies within the confines of the local community. This will come about not through websites, or a dozen computers in a telecenter that accesses websites, but through the beneficial (universal) access to a minimum set of basic IP-based communications applications. This is where economic development arises... this will initiate local adoption, and an equitable local e-commerce.”

A crucial infrastructural issue is the cost of wiring the world, of course, but this is where mobile telephony is currently enabling the developing world to make a leap “due to their dual benefit of being faster to deploy in any area (wide-scale cabling is not required), and of ‘giving wings’ to the Internet with their mobility... The PC era will be overtaken by the non-PC world (PDAs, Smart Cell Phones, personal network devices, etc.)... Now, adding IPv6 to it would give the developing world immediate access to not only the Internet but to many next generation applications currently under development. Failure to provide access to digital technology to countries in the developing world would be to essentially deny them an opportunity to participate in the new economy of the 21st century.”¹⁰

⁸ According to NUA, 8.46% (<http://www.netvalley.com/intvalstat.html>)

⁹ Alan Levy, 17 June 2002, Global Knowledge for Development (GKD) list (gkd@phoenix.edc.org), Re: [GKD] Proposed Open Knowledge Network

¹⁰ Main Task Force Report of the IPv6 Task Force *op cit*.

In fact, from 1999 through 2004, the number of mobile subscribers in Africa jumped to 76.8 million, from 7.5 million, an average annual increase of 58 percent. This has happened so quickly that pundits are still found spouting the now-false comparisons equating the number of phones in all of sub-Saharan Africa to those in Manhattan or London. Asia, the next fastest-expanding market, grew by an annual average of just 34 percent in that period.¹¹

Having said that, wireless access is likely to provide less bandwidth than is available through wire. Countries dependent on wireless may thus end up with less capability than those with wired with regard to absolute bandwidth and thus limitations on the applications that can be supported in the wireless context. Mobile communications would enable the developing world to get online faster, and thus bridge the digital divide, but it would still leave the two sides of the bridge at different levels.

Thus, IPv6 should be considered a benefit to the developing world, insofar as it enables those who are currently effectively disenfranchised to have equitable access to IP addresses.

3.1.3 Multilingualism and IPv6

The same can be said for the prospects for a multilingual web. Currently the fastest-growing area of web development is in Internet sites and users from developing countries and in languages other than English. More websites with more languages inevitably means more addresses.

“I believe that IPv6 will be crucial in promoting culture (which includes local languages). Today, I find recipes of Peruvian dishes on the Internet and even some of the main national dishes have “fan clubs” to discuss on how to improve traditional dishes. Not only expatriates use these addresses but local people. The different cultures should be able to fit with all others and share values in cyberspace. Somebody said, the Internet will be even more useful when people can buy a ticket to the local cinema, pay with local banking transactions (local money) and have everything explained in the local dialect.”¹²

¹¹ Sharon LaFraniere, New York Times, August 25, 2005

¹² Rosa Delgado, Director of Internet Industry Relations – Société Internationale de Télécommunications Aéronautique (SITA), Geneva, Switzerland (personal communication).

Widespread use of the Internet will be dependent upon IP addresses being widely available everywhere. Encouraging local use of the Internet by providing the address bounty offered through IPv6 is thus likely to strongly favour the presence of local content, in local languages, on the Internet.

However, as the Internet Engineering Task Force has discovered, implementing modifications to the Domain Name System to accommodate domain names drawn from the rich UNICODE space is very complex and has not yet been sufficiently deployed to provide convincing evidence of its efficacy.

3.2 Security

When discussing the Internet Protocol, the term “security” usually has a purely technical sense, as exemplified in the following definition in the *webopedia*¹³:

(n.) In the computer industry, refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords.

The broader sense of the term, in which such concepts as privacy and anonymity are included, will be discussed briefly in the next section.

The technical security issues arising relate to the inherent or eventual capabilities of IPv6 to provide a secure environment for end-to-end transmission, on one hand, and the expansion of possible risks owing to the new uses to which IPv6-enabled devices will be put, on the other.

3.2.1 A culture of security

Increasingly, it is recognized that the greatest risks of destroying the promise of the information age stem from systems unable to guarantee an adequate level of security. The weaknesses of IPv4 in this regard have already provided a rich field of loopholes for malicious or criminally minded to exploit. Poor technological security invites the legislators and governments into the party. IPv6 is mandated to avoid this, and to guarantee security and quality. We will explore this further below.

¹³ <http://www.webopedia.com/TERM/S/security.html> accessed 30 September 2005

The (OECD) recently drew up guidelines on the security of information systems and networks¹⁴, identifying a clear social and ethical significance in “efforts to enhance the security of information systems and networks”, and stressing that these should be “consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy”. The OECD Guidelines offer the following nine principles to govern security:

- 1) Awareness:** Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
- 2) Responsibility:** All participants are responsible for the security of information systems and networks.
- 3) Response:** Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
- 4) Ethics:** Participants should respect the legitimate interests of others.
- 5) Democracy:** The security of information systems and networks should be compatible with essential values of a democratic society.
- 6) Risk assessment:** Participants should conduct risk assessments.
- 7) Security design and implementation:** Participants should incorporate security as an essential element of information systems and networks.
- 8) Security management:** Participants should adopt a comprehensive approach to security management.
- 9) Reassessment:** Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

It is generally accepted that IPv6 offers much greater and more robust security than IPv4 because it assures a one-to-one link between communicators. This restores the end-to-end principle violated by NATs, firewalls, and other characteristics of the IPv4 world. Nevertheless, the inexhaustible pace of development is bringing entirely new stresses to security: notably the wireless internet and internet communications mediated by mobile telephones. Proponents of IPv6 maintain that the protocol will assure security even in conditions where messages are whizzing wirelessly through ambient space in pavement cafes, but this remains to be seen. We will return to this below.

¹⁴ OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. 2002., Organisation for Economic Co-operation and Development, Paris. Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002. Available at <http://www.oecd.org/>

3.3 The Application of the Technology

Some of the social and ethical aspects of IPv6 relate to the possible applications that could be enabled by, or that would be impossible without, the deployment of IPv6. These include security (aspects of privacy and anonymity), the consequences of implanting chips in animals and humans, the spectre of Big Brother (e.g., individual unique ID systems), risks associated with collection and storage of data (from issues related to the facts of your own biography, to concerns about the transience of document archives), and social impacts on employment and education.

There will be other social/ethical aspects of IPv6 based on the changes it will imply on society – hospitals, doctors, employment, etc. Will it require changes in the law? Some new or more extreme forms of data protection, for example? The concept of privacy is expanding from its “traditional” areas associated with crime, politics, sex and religion, to encompass commercial invasions of your personal space, including reading your suit/toaster/fridge chips. These issues, and legal recourses for them, have always been present, there, but the scope will expand enormously in an IPv6-enabled world.

3.3.1 Privacy and IPv6 technology

Privacy issues arise not just in the application of IPv6 but also in the technology itself. IPv4 has catered to a world in which typically a stationary PC initiates contact with the Internet by dialling in¹⁵. As a target for prying eyes, such PCs are not much use because they are disconnected from the Internet most of the time. Such devices do not need to have unique, stable addresses and, given IPv4’s natural parsimony with addresses, it deals with such connections by temporary addresses picked at random from a pool of addresses.

However, the IPv6 user is envisaged as operating in an always-on mobile world. Such a user needs a permanent IP address for each device connected with the Internet. Extended use of the identifier over time can compromise privacy:

¹⁵ This section is based on the Internet Engineering Task Force (IETF) Request for Comments (RFC): Privacy Extensions for Stateless Address Autoconfiguration in IPv6 <ftp://ftp.isi.edu/in-notes/rfc3041.txt> and the Statement on IPv6 Address Privacy by Steve Deering and Bob Hinden, co-chairs of IETF’s Next Generation Working Group, November 6, 1999 at <http://playground.sun.com/pub/ipng/html/specs/ipv6-address-privacy.html>

“For example, a network sniffer placed strategically on a link across which all traffic to/from a particular host crosses could keep track of which destinations a node communicated with and at what times. Such information can in some cases be used to infer things, such as what hours an employee was active, when someone is at home, etc... The use of a constant identifier within an address is of special concern because addresses are a fundamental requirement of communication and cannot easily be hidden from eavesdroppers and other parties. Even when higher layers encrypt their payloads, addresses in packet headers appear in the clear. Consequently, if a mobile host (e.g., laptop) accessed the network from several different locations, an eavesdropper might be able to track the movement of that mobile host from place to place, even if the upper layer payloads were encrypted”.¹⁶

Thus, the privacy risk is in disclosing the address of the individual, as this is tantamount to locating him topographically, in real space. When unique serial numbers based on IEEE identifiers are used, privacy can be compromised. To tackle this, an IPv6 address that contains a random number was introduced into the IPv6 development process.. Later, a solution was proposed to deal with the numbers based on the IEEE identifiers, as well, (essentially by letting them change over time) thus closing the door on “eavesdroppers and other information collectors”.

This inherent security issue need not be considered as an insoluble vulnerability, but it is likely to remain a point of concern in the development of IPv6. The European Commission is well aware of this concern:

“...the Internet has, from the very beginning, been considered as an open network, there are many characteristics of its communication protocols which, more by accident than design, can lead to an invasion of the privacy of Internet users... The fundamental right to privacy and data protection is enshrined in the EU Charter on fundamental rights and developed in detail in the EU data protection directives 95/46/EC and 97/66/EC which both apply to processing of personal data on the Internet. In its Communication on the Organisation and Management of the Internet Domain Name System of April 2000, the Commission stated already that an IP address can be a personal data in the sense of the legal framework (for example dynamic IP addresses). Also the Article 29 Data Protection Working Party, the independent EU advisory body on data protection and privacy established by Directive 95/46/EC, draw the

¹⁶ IETF RFC on Privacy Extensions for Stateless Address Autoconfiguration in IPv6 *op cit*

attention at several occasions to privacy issues raised by the use of the Internet. The Article 29 Data Protection Working Party as well as the International Working Group on Data Protection in Telecommunications (the “Berlin Group”) consider to work specifically on IPv6. It is therefore of indispensable that the European Commission and the European Union as a whole consider privacy issues in the further development of Internet. While privacy issues are currently being taken into account in the development of IPv6, it is essential that the trust and confidence of Internet users in the whole system, including in the respect of their fundamental rights, is ensured.”¹⁷

3.3.2 Privacy and information and communication technologies

Before considering it as an IPv6 matter, the debate on the privacy of communications should be addressed from the broader perspective of information and communication technologies (ICTs). Whatever applies to ICTs applies *a fortiori* to IPv6. A useful summary of the issues¹⁸ was posted to a list operated by the now-defunct Internet Societal Task Force (ISTF):

- First, ICTs (and biotechnology) have produced the ability to assign an absolutely *unique identifier* for every person (e.g., a DNA-based marker). The issue here becomes who has a right to demand that unique marker and under what circumstances.
- Second, ICTs have produced the ability to engage in *non-intrusive tracking*. Walking from my residence to my office today I was recorded on 5 different surveillance cameras. ICTs mean they be fed to identity software. Who has a right to those images and under what conditions?
- Third, ICTs have produced the ability to engage in *intrusive tracking*. Consumer Relations Management (CRS) software can be used to data mine, and track, extensive personal information. Cross linking commercial data can present an individual profile which heretofore was knowable only to me. Under what conditions can that data be mined, by whom, and shared in what ways?
- Fourth, governments have both extensive information on individuals, and the legal power to engage in various forms of surveillance. This gives them the power to engage in *intrusive tracking* and construct rich individual profiles. The same questions arise. Who has the right, under what conditions, and what can be done with the information?

¹⁷ European Commission, *op cit*.

¹⁸ Edited from a message sent by Sam Lanfranco on 14 October 2001 to the Internet Societal Task Force (ISTF) Participants list (bounce-istf-participants-l3688@lists.istf.org – now defunct

Clearly IPv6 can play a role in each of these: DNA-based markers, web cams with their own IP addresses, establishing stable personal profiles – all of these are among the benefits IPv6 will bring. We must ensure the conditions for these benefits are right, however, so as not to undermine the legitimate aspirations to personal privacy of the individual citizen.

3.3.3 Tagging and personal ID

Among the uses suggested for all the new IPv6 addresses is the tagging of animals with chips enabling the monitoring of their location, numbers, health status and other measurable data. Not only would this help in the husbandry and management of ecologically threatened species, it would also help to minimize the impact of zoonoses and other animal diseases – both those transmitted animal-to-animal, and those transmitted across species, including from animals to humans. The social and economic impact of outbreaks of zoonoses such as foot-and-mouth disease could be sharply reduced, as could the risks of cross-species transmission of such conditions as scabies, and perhaps Creuzfeld-Jakob (“mad cow”) disease.

Clearly, the project of tagging significant proportions of the animals of the world and essentially turning them into information servers on the Internet would be impossible without the addresses created by IPv6.

Animal tagging may find resistance in animal-rights quarters, and there are ethical issues to face in this respect.

The application of such technology to the human race raises a number of further ethical questions. Apart from the human scale of tagging represented by implanting a chip, it is also possible to tag at the genetic level. “Affymetrix is...applying the principles of semiconductor technology to the life sciences.. The Company’s customers include pharmaceutical, biotechnology, agrochemical, diagnostics and consumer products companies, as well as academic, government and other non-profit research institutes. Affymetrix offers ... its integrated GeneChip® platform, to address growing markets focused on understanding the relationship between genes and human health.”¹⁹ The GeneChip Probe array is using the output of the Human

¹⁹ See <http://www.affymetrix.co.uk>

Genome Project and is designed to analyse or screen for specific genetic expressions.²⁰

Thus, IPv6 will enable the vast effort and address space required to tackle the human organism at genetic-code level. It is hard to overstate the importance of this, both from the perspectives of enormous opportunities in the health field, and equally significant possibilities for abuse, if the social and ethical issues are not addressed.

3.3.4 Anonymity and IPv6

Essentially, anonymity is a special case of privacy. Privacy may be an unconditional right, but anonymity is conditional – you can insist on some privacy, but you are usually allowed anonymity under certain conditions (for example, if you are participating in a medical trial under the terms of a consent agreement).

Privacy guards knowledge about a person’s thoughts, activities or whereabouts, while anonymity may do all that and also cloak the person’s name and identity. On the other hand, you may know everything about an anonymous communicator, except for their name. Proponents of a right to anonymity in online communications identify the following beneficial and harmful aspects of anonymous communication:²¹

Benefits	Harms
Investigative journalism	Spamming
Whistleblowing	Deception
Law enforcement	Hate mail
Self-help	Impersonation and misrepresentation
Personal privacy protection	Online financial fraud
Avoiding persecution	Other illegal activities

In the IPv6 world, anonymity depends on there being no way of identifying the individual owning or using an IP address. The problems regarding assuring privacy mentioned above would often compromise the anonymity of the address holder.

²⁰ According to Dominic Pinto (private communication), Senior Associate, Telesphere Limited (<http://www.telesphere.com>), to whom I am indebted for the reference to Affymetrix.

²¹ Table based on Kling, Rob, Ya-Ching Lee, Al Teich and Mark S. Frankel, 1999. Assessing Anonymous Communication on the Internet: Policy Deliberations. *The Information Society* 15(2), <http://www.slis.indiana.edu/TIS/abstracts/ab15-2/kling.html>

It has been argued that anonymity is morally neutral and that it is a human right: "Anonymous communication should be regarded as a strong human right; in the United States it is also a constitutional right."²²

More broadly, the Universal Declaration of Human Rights (UDHR), contains provisions that protect the ability of individuals to communicate anonymously. Article 12 governs freedom from interference with privacy, home, and correspondence, and Article 19 provides for freedom of opinion and expression and the right "to seek, receive, and impart information and ideas through any media and regardless of frontiers."

With regard to Internet communication...recipients have the right to choose to accept or refuse anonymous messages and that individuals do not have the right to impose messages upon an unwilling recipient. At the same time, law enforcement agencies and commercial interests do not have the right to interfere with individual privacy in electronic communication, regardless of whether it is anonymous or not... Closely related to these provisions of the UDHR is the First Amendment of the U.S. Constitution, which guarantees the right of free speech to all Americans. The First Amendment applies equally to communications in which the initiator is identified and to those that are sent anonymously."²³

If these views, expressed in the summary report of a conference of the American Association for the Advancement of Science, are to be maintained, such conditions will need to be implemented into IPv6.

Beyond that, anonymity enters the world of governance, and the rules that are agreed governing the registration of names associated with addresses. Other conditions expressed in the AAAS report are that "online communities should be allowed to set their own policies regarding the use of anonymous communications", and that "individuals should be informed of the extent to which their identity is disclosed online".

²² Teich, Al, Mark S. Frankel, Rob Kling and Ya-Ching Lee, 1999. Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference. *The Information Society* 15(2), <http://www.slis.indiana.edu/TIS/abstracts/ab15-2/teich.html>

²³ Teich, Al *et al*, *op cit*.

There are strong ethical arguments on both sides, and these will need to be mustered when the time comes to debate registration procedures. It is enough to place a marker here that this will need to be done.

3.3.5 Other application issues

Don Cameron²⁴, an IT Manager at a moderately sized rural firm with 400 staff ran a simple series of tests over a number of months in a fairly diverse cultural setting designed to determine true bandwidth requirements under a variety of Internet usage circumstances. He found that 72% of all their web-based traffic resulted from third-party web URL redirections – banner advertisements, animated GIFs, Java pop-up screens, hit counters, cookie downloads, browser & IP referrals (the information we all unknowingly send to some sites). This traffic represented nearly 40% of the total bandwidth utilisation (including e-mail) of the company. Furthermore, he determined through server logs that 20% of all inward mail traffic was unsolicited Spam.

The story continues as a technical optimization story, culminating in a win-win solution resulting in more bandwidth, faster and easier access and lower costs by switching of all the extraneous connections to the firm's traffic and tackling Spam in a systematic way.

However, from the perspective of IPv6, the fact that fully $\frac{3}{4}$ of all web traffic might be third-party web URL redirections is worth pondering. Will virtually unlimited namespace, will the flow of cookies, Spam and advertising of all kinds similarly hit exponential growth. With the remarkable growth of the good things on the Internet heralded by the application of IPv6, will the bad things grow with the same amazing vigour?

The guess is that we are reaching a critical phase in each of the applications of technology which have an abusive edge. For example, most people would acknowledge that advertising can have a positive role in the information economy (such as free-to-air television programming), turns abusive in Spam. The Internet, which has thrived on self-regulation so far, has so far failed to regulate Spam effectively. Any major expansion of what are generally seen as abusive edges of applied information and communication technology will certainly lead to a strengthening of the international regulatory framework. This by-product of IPv6 dissemination will have to be monitored carefully in relation to possible social and ethical consequences.

²⁴ Based on a message sent by Don Cameron [mailto:done@mudgeeab.com.au] on 21 July 2002 to communityinformatics@vancouvercommunity.net

Giving in to the Internet and enabling it to do everything means that if anything goes wrong, everything goes wrong. By facilitating turning every atom of human existence into an Internet address, equal care needs to be devoted to fail-safe and security systems: “work on end-to-end security models should be pushed to achieve security for everyone as for access for everyone... Security needs not only a protocol but also a PKI infrastructure, which is an expensive investment and that is going to hinder immediate deployment of security at a larger scale to enable e-commerce and the like. The digital divide is complemented by the security divide!”²⁵

Clear examples of new risks include the collection and storage of data. When you have every fact of your life stored on a tiny device, what happens when you lose it? If it is backed up, who will have the key? How will back ups be preserved? There are security issues involved, but also storage issues. Where security may be a problem (as mentioned above) storage should be facilitated by the provision of unlimited IPv6 addresses.

Extrapolating from this scenario to document archives, the proliferation of IP addresses should enable storing as many versions of archive material and any associated software in a uniquely findable way. We envisage IPv6 will be a particular bon in digital storage and archival, and thus in preserving the cultural heritage of humanity.

The massive ramping up of Internet will certainly have a cataclysmic social impact on employment and education. All technological change has such a social impact, but the scale of the impact that could be led by the extensive deployment of IPv6 has never been seen before.

3.4 Governance

The more the Internet expands its scope, the more it matters who (if anyone) is in charge, and how such a role is exerted.

As the vastly expanded name/address space offered thanks IPv6 enables the Internet to infiltrate almost every part of life, the issue of governance becomes far more significant. Whoever controls this name/address space will be very powerful – far more powerful than the managers of the IPv4 name/address space, and perhaps more powerful than elected political representatives in many countries. How will this power be allocated? Will

²⁵ Latif Ladid, Chairman IPv6 Task Force (personal communication).

the process be entirely transparent and democratic? Can everyone have a say? What is the role of developing countries? Will the solutions favour one group rather than another, one language rather than another?

Who in the end is accountable? The fact that the Internet Engineering Task Force (IETF) is not accountable to anyone is often presented as a strength and benefit. Those working on the IETF are in fact accountable to their peers. It has been argued that self-regulation is a stronger form of accountability than explicitly legislated accountability. Nevertheless, conclusions drawn from a study of self-regulating codes of ethical conduct²⁶ suggest significant problems with the application of self-regulation methodology, particularly in determining what the rules are in the first place, and in effective enforcement.

A number of bodies have specific roles in developing and managing cyberspace, including the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union, the World Intellectual Property Organization, and others. Under the terms of Declaration of Principles²⁷, and as a part of the process of the World Summit on the Information Society (WSIS) a Working Group on Internet Governance (WGIG) was established in December 2003 to:

- Develop a working definition of Internet Governance;
- Identify the public policy issues that are relevant to Internet Governance;
- Develop a common understanding of the respective roles and responsibilities of governments, existing international organizations and other forums as well as the private sector and civil society from both developing and developed countries.²⁸

It is not the purpose of this paper to review or assess these bodies, especially since at the time of writing issues of Internet governance are very fluid and it is difficult to draw any conclusions. The specific role of IPv6 in this lies in its enabling a quantum leap forward in how the internet will penetrate all of our lives. The governance structures established, their management and the assignation of responsibilities in them are, and will

²⁶ Jacques Berleur and Tanguy Ewbank de Wespin, 2002, Self-regulation: Content, Legitimacy and Efficiency - Governance and Ethics (In print).

²⁷ Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003, <http://www.itu.int/wsis/docs/geneva/official/dop.html> accessed 30 September 2005.

²⁸ <http://www.wgig.org/>

become increasingly, significant as the Internet becomes increasingly significant. It is as an enabler of such societal penetration that IPv6 matters.

4. CONCLUSIONS

The arrival and deployment of IPv6 can be seen in the classical terms of opportunity and threat. It is certainly an opportunity as it finally enables everyone in the world (and for generations to come) who might want to have use the Internet in any walk of life to do so. No one will be deprived for want of an IP address, at least – although the financial and other infrastructural aspects remain to be resolved.

At the same time, we have to ensure that the vast new possibilities afforded by the technology do not lead to vast new societal and ethical problems. It is important to raise concerns and questions as the technology is being developed, at the earliest stage possible. The development of the Internet can be seen as a giant experiment on human subjects, none of whom have been adequately warned or have formally consented.

It remains to see how the largely technical community labouring over the protocol responds to these societal demands. To develop and assure the consideration of societal concerns, an Internet Societal Task Force (ISTF) was established in 2002 under the guidance of Vint Cerf (who served as its first President) and under the aegis of the Internet Society. This group eventually disestablished as a Task Force and converted into a discussion forum. Among the reasons offered for this was that the ISTF was “unable to agree on positions” and that its process was inefficient.

To an extent the notion of having an Internet Societal Task Force to parallel the Internet Engineering Task Force (IETF) faced a confrontation between CP Snow’s Two Cultures. On one hand you have a body like the IETF, which operates scientifically, issues requests for comments on technical issues and comes to black-and-white conclusions that can be adopted within specified time frames, with measurable resources and consequences. On the other you have an idea like the ISTF, which can only address issues that have no black-and-white-solution, and may indeed end up with two or more diametrically opposed points of view on a given societal issue.

The point of this discussion is to stress that the two cultures must talk to each other. A recognition of the need to address societal aspects of

technological developments associated with IPv6 is overdue. The relentless focus on technology alone is not enough. We need not only to make the IPv6 enabled world work, but to make it worth living in.

Acknowledgements: All errors and opinions expressed herein are the responsibility of the author, but grateful thanks for their comments and suggestions over time (and mainly on much earlier versions) are due to Rosa Delgado, Latif Ladid, Dominic Pinto, Jonathan Robin and Vinton Cerf