United Nations
Educational, Scientific and
Cultural Organization

# of Emerging Technologies: A Survey

Prepared by Mary Rundle and Chris Conley
Geneva Net Dialogue

IFAP — Information for All Programme

Communication and Information Sector

Ethical Implications of Emerging Technologies: A Survey

Prepared by Mary Rundle and Chris Conley

Geneva Net Dialogue

UNESCO: Paris, 2007

The ideas, facts and opinions expressed in this publication are those of the authors. They do not necessarily reflect the views of UNESCO and do not commit the Organization.

Recommended catalogue entry:
UNESCO. Information for All Programme (IFAP).
« Ethical Implications of Emerging Technologies: A Survey ».

Edited by the Information Society Division, Communication and Information Sector (Editor: Boyan Radoykov) – Paris: UNESCO, 2007 - 92 p ; 21 cm.
I - Title
II – UNESCO
III – Information for All Programme

Published in 2007 by the United Nations Educational, Scientific and Cultural Organization,
7, place de Fontenoy F-75352 Paris 07 SP, Paris, France

Coordinator of the publication: Boyan Radoykov

CI-2007/WS/2 - CLD 31112

Ethical Implications of Emerging Technologies: A Survey

Prepared by Mary Rundle and Chris Conley [*]

Acknowledgements

In the course of compiling this report, a number of prominent members of the worldwide technology and infoethics communities have shared their expertise and perspectives with us, including: Hal Abelson, Ben Adida, Ang Peng Hwa, Kader Asmal, Ted Barnett, Stefan Bechtold, Peter Berghammer, Scott Bradner, Stefan Brands, Kim Cameron, Shunling Chen, David Clark, John Clippinger, Urs Gasser, Lauren Gelman, Georg Greve, Dick Hardt, Dewayne Hendricks, Chris Hoofnagle, Hai Huang, Ben Laurie, Ronaldo Lemos, Lawrence Lessig, Jamie Lewis, Abdel-Hamid Mamdouh, Désirée Milošević, Nicholas Negroponte, Cory Ondrejka, David Reed, Eric Rescorla, Jonathan Robin, Judit Rius Sanjuan, Wendy Seltzer, Lara Srivastava, William Terrill, Paul Trevithick, Jake Wachman, David Weinberger, Ian Wilkes, and Jonathan Zittrain.

[*] Mary Rundle is a fellow at the Berkman Center for Internet and Society at Harvard Law School and a non-resident fellow at the Center for Internet and Society at Stanford Law School. Chris Conley holds a master's degree in computer science from M.I.T. and is currently a J.D. candidate at Harvard Law School, where he focuses on the intersection of law and technology. This paper has been produced under Geneva Net Dialogue, a Geneva-based, open, international association whose mission is "to lend its support to the operation of human rights in the information society by improving ties between the technology community, the policymaking community, and civil society at the international level."

Ethical Implications of Emerging Technologies:
A Survey

Mary Rundle and Chris Conley

Table of Contents

Foreword

Embracing coherent ethical guidelines is essential for building inclusive knowledge societies and raising awareness about the ethical aspects and principles is central for upholding the fundamental values of freedom, equality, solidarity, tolerance and shared responsibility. Thus, UNESCO encourages the definition and adoption of best practices and voluntary, professional guidelines addressing ethical issues for media professionals, information producers, and service providers and users with due respect to freedom of expression.

The quickening speed of technological evolution leaves little time to decision-makers, legislators and other major stakeholders to anticipate and absorb changes before being challenged to adapt to the next wave of transformation. Lacking the time for lengthy reflection, the international community is often faced with immediate policy choices that carry serious moral and ethical consequences: Increase public infrastructure or permit preferential use by investors? Allow the market to oblige people to participate in digital systems or subsidize more traditional lifestyles? Let technology develop as it will or attempt to programme machines to safeguard human rights?

The Infoethics Survey of Emerging Technologies prepared by the NGO Geneva Net Dialogue at the request of UNESCO aims at providing an outlook to the ethical implications of future communication and information technologies. The report further aims at alerting UNESCO's Member States and partners to the increasing power and presence of emerging technologies and draws attention to their potential to affect the exercise of basic human rights. Perhaps as its most salient deduction, the study signals that these days all decision makers, developers, the corporate scholar and users are entrusted with a profound responsibility with respect to technological developments and their impact on the future orientation of knowledge societies.

It is our hope that this study will impress upon the policy makers, community, producers and users the need to carefully observe evolutions in ICTs – and, by so doing, to comprehend the ethical and moral consequences of technological choices on human rights in the Knowledge Societies.

Abdul Waheed Khan
Assistant Director-General for
Communication and Information,
UNESCO

Introduction

The Internet boom has provided many benefits for society, allowing the creation of new tools and new ways for people to interact. As with many technological advances, however, the Internet has not been without negative aspects. For example, it has created new concerns about privacy, and it has been hampered by spam and viruses. Moreover, even as it serves as a medium for communication across the globe, it threatens to cut off people who lack access to it.

New solutions in information and communication technologies (ICTs) are constantly emerging, and, for good or for ill, the changes they bring may open up our societies and our world to a greater extent than did the first phase of the Internet revolution. It is imperative to consider the implications of these new technologies, and to encourage positive choices regarding their uses.

UNESCO is well situated to call the attention of the international community to these advances, particularly as to their ethical and societal consequences, which this report refers to as "infoethical" challenges or "infoethics." To that end, this survey analyzes certain UNESCO goals in light of emerging technologies that will usher in the future Information Society[1] – in particular:

1. **The Semantic Web and Other Metadata** – Metadata, or data about data, enables greater automated analysis of information; the Semantic Web promises to use metadata to create an environment in which computers can serve as intelligent agents rather than mere tools.

2. **Digital Identity Management and Biometrics** – Digital identity management allows the amassing and automatic processing of personal data; biometrics provides means by which human beings can be uniquely identified.

[1] UNESCO is increasingly using the term "Knowledge Societies", which reflects a development-oriented, people-centred and pluralistic vision of the future societies. However, for the purposes of this study, the term "Information Society" is used throughout the document.

3. **Radio Frequency Identification (RFID) and Sensors** – These technologies monitor the physical world, using communications technology to distribute information about a specific location.

4. **The Geospatial Web and Location-Based Services** – Both of these technologies serve to associate digital data with physical locations.

5. **Mesh Networking** – Mesh networking facilitates the formation of networks across areas without existing communications infrastructures. As such, it can help connect underserved areas.

6. **Grid Computing** – This technology may allow the world's computing power and data storage resources to be pooled for people to access as needed.

7. **New Computing Technologies** – Combined with the technologies listed above, a powerful mix of optics, quantum computing, and other new technologies has potential to bring about a "global brain."

Because choices in their design and use carry moral consequences, these technologies pose significant infoethics challenges.

This survey considers these choices in the light of key UNESCO infoethics goals - in particular:

(a) Fostering the application of human rights and fundamental freedoms in cyberspace;

(b) Extending the public domain of information;

(c) Enabling diversity of content in information networks; and

(d) Promoting access to information and means of communication.

Taking these objectives as a given, the survey employs them as measures in assessing likely consequences of different technological choices.

In presenting results of this examination, the report first tells an introductory story of how the technologies covered relate to one another. Next, infoethics goals are presented. Then, for each technological trend surveyed, the report contains a short chapter drafted in lay terms to provide an overview of the relevant technology and to highlight ramifications and concerns. The report then summarizes this infoethics analysis and revisits the story of the emerging technologies. Finally, the report offers recommendations on ways to advance infoethics goals in anticipation of these oncoming technologies.

The Technologies as a Short Story

In the short history of the Information Society, technology has moved from making sense of cyberspace to making sense of the physical world, with new modes of connectivity now holding promise for a seamlessly integrated Internet to reach all regions of the globe.

For the Internet's first phase, humans initiated the exchange of text, images, and other information. Given the enormous amount of content and code that has been generated, computers now need interoperable metadata, or data about data, to navigate. The **semantic web** promises to offer such metadata. This new metadata language offers predictability in a cyberspace of ever growing exchanges, with the vocabulary of metadata lending greater precision to human use of the Internet or even allowing computers to access and analyze content directly.

Since people have been the actors in the first phase of the Internet, and should remain of central concern in all future developments, it makes sense that computers would need a detailed set of terms to facilitate exchanges on behalf of individuals. Put another way, as programmes navigate the web (with web agents querying many web sites to answer any given human question), a person needs to be able to delegate his identity to a programme so it can think and act on his behalf – for example negotiate for his preferred rental car model, designate which friends may have access to his calendar, or pay taxes on online transactions. Hence, records are being developed to refer to elements of a person's various digital personae (e.g., name, date of birth, citizenship, etc. for one persona; pseudonym, favorite songs, etc. for another). In this way, metadata serves as a language for describing **digital identities**.

To date, digital identities have typically been dissociated from physical identities. However, the emerging technology of **biometrics** promises to correlate the two, linking an individual's various digital identities to his embodied person. An embodied person can be represented in digital form through the translation of unique attributes – for example his fingerprints, iris pattern, or walking gait. These attributes are taken as measurements, with the biometrics translated into numerical expressions that computers can refer to in their machine-readable language. A physical person can thereby be uniquely identified and then abstracted as data.

Similarly, both **radio frequency identification (RFID)** and **sensors** are making other aspects of the physical world manageable and searchable in the digital world. RFID tags enable the tracking of physical objects or people using cheap, digital technology: A person bearing an RFID chip can easily be identified for different purposes – for example, ensuring that new-born babies do not get mixed up in a hospital, or granting the proper people access to restricted areas of a building. Likewise, a specific product (say, a bottle of shampoo) can be tracked from its production line to the store where it is sold and even associated with an individual consumer. This information can be used for a range of purposes, from promoting efficiency in the supply chain to allowing the recall of faulty products.

One might take issue with metadata's linguistically equating an individual with a bottle of shampoo. To such an objection, a computer scientist might respond that these problems can be resolved as the metadata languages are refined to add dimension and ascribe value.[2]

There are certain signs that this refinement is underway, driven in part by the importation of the physical world into cyberspace. Sensors are enabling the further digitization of the physical world – measuring observable qualities such as oxygen level or acceleration, and then translating them into digital form. With more material added to cyberspace, flesh is put on the bones of previously catalogued ideas. Different contexts provide dimension and establish added meanings for the semantic web to recognize.

Meanwhile, just as cyberspace is importing the real world, it is itself being exported to that physical space through the **geospatial web** and **location-based services (LBS)** technology. These Internet-rendered services superimpose themselves on the real world and offer web-based views of real-world locations overlaid

[2] Such issues point to the problem of technological neutrality – that is, the question of whether technology is neutral or whether it is laden with values. Values may be ascribed during the development of a language, and someone or something needs to choose how to order things – for example deciding if a human falls into the same category as an object, or how categories should overlap.

with relevant information (e.g., home prices, crime rates, or hiking trails). The line separating the "real world" and "cyberspace" has already begun to blur; in time, these two worlds may be integrated.

However, the Information Society is not there yet. Huge swaths of the globe remain without Internet connectivity, particularly in the developing world. While this territory historically has seemed vast, it may not be long before global connectivity is realized. The advent of **mesh networking**, which allows network-enabled devices (e.g., mobile phones) to establish a peer-to-peer network spontaneously, offers one means of extending the range of connectivity without requiring an expensive infrastructure. The evolving ability of mobile phones and other electronic devices to connect to the Internet and to each other will expand the reach of mesh networks, perhaps eventually extending a global network to every location on earth in ubiquitous networking.

Of course, a network comprised largely of devices without significant computing power has limitations in terms of computing resources, data storage and accessibility. This problem could be addressed by **grid computing**, whereby storage and computing power are pooled in a network, with people tapping into resources as needed and providing them as available, in accordance with some cost allocation scheme.

Should a combination of ubiquitous networking and grid computing come about, the Information Society would find itself in a world of **ubiquitous computing** – at which point the physical and digital worlds will become less distinguishable. Every object – even doors, clocks, refrigerators, or watches – will be able communicate its status and respond to its environment. Meanwhile, computing power itself may continue growing exponentially, supported by new technologies such as **optical** or **quantum computing**, which will be important for processing this immense quantity of data. In combination with a massive computing grid, this force could constitute a large virtual "brain" that continuously pushes computational limits in an expanding universe.

This story tells of a bright future in which emerging technologies are applied to the benefit of all humanity. History suggests, however, that technology can also be used to limit rather than to promote human rights and dignity. Thus, it is important to consider how these technologies may promote or thwart the realization of infoethics goals.

Infoethics Goals for Neutral Technologies

Information and communication technologies (ICTs) are an increasingly powerful force in the modern world. Their influence can be seen in all spheres of public life, from business interactions and education to politics and international affairs. These technologies, particularly the Internet, have also become a dominant mechanism for conducting private affairs and participating in society. Advancing technology frequently serves to allow prior activities to be performed more easily and can open up entirely new possibilities.

Moreover, the rate at which technology advances is itself increasing. Moore's Law,[3] which states that the computing power of a single microprocessor grows exponentially, applies to other technologies as well. The Internet and related technologies allow for new ideas and inventions to be distributed far more rapidly than before, and encourage the ever-increasing pace of technological growth.

But technology in itself is neutral; it does not directly contribute to the advancement of human rights. Many technologies have multiple possible applications, some of which may serve to further this goal, others of which may hinder it.

It is therefore imperative that emerging technologies be examined in light of their impact on the exercise of human rights. As described above, the infoethics goals provide a framework for this examination. The first infoethics goal, derived from the *Universal Declaration of Human Rights*,[4] establishes the fundamental priority of putting technology in the service of human rights. Stemming from that goal are three others that aim to promote the public domain, diversity of content, and access to information and the means of communication – with these three based on the premise that all people should be able to share in the benefits of ICTs.

[3] *See* http://en.wikipedia.org/wiki/Moore%27s_law (viewed November 8, 2006).

[4] UN General Assembly resolution 217 A (III) of 10 December 1948.

Human Rights and Fundamental Freedoms

Technology can serve to promote or restrict human rights. The Information Society should foster the use of emerging technologies in such a way as to maximize the benefits that they provide while minimizing the harms. In many cases, this promotion may be less a matter of technological control than of oversight: establishing the proper legal or regulatory system to ensure that technology capable of abuse is not in fact abused, and that the benefits of technology are shared among all.

In discussing human rights, we take as a starting point the *Universal Declaration of Human Rights*. Many of the rights stated in this document are particularly important when considering the ethical ramifications of new technologies and their potential uses. For the purposes of this study, key provisions include:

ARTICLE 2:

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

ICTs enable the collection and parsing of information and, as such, allow myriad categorizations. Personal data may be broken down to such elements as ethnicity, gender, religion, nationality, and socio-economic status, among others. From an infoethics perspective, it is important to ensure that the categorization of data elements according to such lines does not result in interference with a person's rights and freedoms.

ARTICLE 3:

Everyone has the right to life, liberty and security of person.

The right to life, liberty and security of person is one of the most fundamental rights included in the *Universal Declaration of Human Rights*, and yet among the most difficult to define. This right encompasses a right of access to all of the necessities of life, including food and shelter.

ICTs contribute to health-improving and even life-saving benefits, ranging from clean-air technologies and coordinated medical research to early emergency alerts and quick access to medical information. Does a right to life encompass universal access to these benefits of technology, regardless of ability to pay?

So, too, the economic efficiencies brought on by ICTs may raise the standard of living in many areas of the world. Hence, the economic gains normally translate into better enjoyment of the right to life, liberty and security of person.

While this Article may be construed as entailing a right of access to the information, ideas, cultural elements, and communication media that allow people to take part in society, it may also be read to allow an individual to *opt out* of participating in ICT systems. For example, under this right a person might be permitted to refuse to have an ICT device implanted into his body. If such an implant were to become de facto requirement for participation in the Information Society, should the law step in to allow that person to have access to all of the necessities of life, including food and shelter, despite his refusal to receive the implant?

ARTICLE 7:

All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

The concept of equal protection can be aided or hindered by the deployment of ICTs. Technologies that serve to provide all people with equal opportunity and access, without discrimination, serve this provision. However, technology can also be implemented to identify members of specific groups, and thus to enable discrimination against those groups.

ARTICLE 11:

(1) Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.

(2) No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

Data that is gathered or analyzed by technology is increasingly used in judicial proceedings. When evidence stemming from the application of technology contradicts a person's testimony, a dilemma arises as to which account deserves more credence. Despite the tendency of society to trust evidence produced by machines on the basis of general statistical accuracy, computer code may carry mistakes or be corrupted. In this sense, then, there are infoethics nuances in the use of technology to establish "proof".

ARTICLE 12:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ICTs can serve to protect or limit the right of privacy. For example, encryption technologies can make communication between private parties confidential, or they can be modified to allow outside interests (such as governments) to intercept this communication. Likewise, surveillance technologies can serve to guard privacy, but they may also be used as tools to infringe on the privacy of others.

ICTs can afford anonymity, allowing people to feel comfortable sharing ideas they might not air if their names were associated with these ideas. In this sense, privacy and anonymity in communication bear a close relationship to the right to seek, receive and impart information (Article 19) as well as the right to associate or assemble (Article 20).

Efforts to protect privacy, however, may impose other costs on society, and efforts to protect other rights may have privacy implications. For example, any protection that technology provides for anonymous, secure communication may limit the effectiveness of protection against attacks on a person's "honor and reputation."

Privacy concerns are also raised by the increasing collection of personal data by private and governmental entities. A question receiving growing attention is the duty that private companies have to safeguard consumers' personal data, especially in the international context of the Internet. There are also questions regarding governmental treatment of personal data, particularly concerning what rules apply when different governments share such information.[5]

[5] The United States and the European Union are currently embroiled in a dispute concerning the disclosure and use of information about airline passengers. *See* "Air Security Talks Fail," Daily Mail, October 2, 2006, p. 32.

Of course, there are questions as to what constitutes "arbitrary" and "interference". If a policy applies across the board and is supported by what seem to be reasonable arguments, is it "arbitrary"? If surveillance poses no inconvenience, is it "interference"?[6]

ARTICLE 18:

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

ICTs and thought, conscience and religion can interact in various ways. First, and most simply, ICTs can be used to further religious interests and to allow persons to communicate on issues of faith. If, however, the use of technology is contrary to beliefs, then the observance of these beliefs may be threatened by making the use of technology mandatory or practically necessary to function in the modern world.

ARTICLE 19:

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

As with the right of privacy, the right to freedom of opinion and expression in the Information Society is tightly intertwined with ICTs. Technologies can open channels by which information may be shared and opinions expressed; it can also be used to restrict the information available[7] and to identify and interfere with people expressing alternative opinions.[8] In this sense, there is a link between privacy (Article 12) and the freedom to seek, receive and impart information.

Moreover, the right to freedom of opinion and expression loses value without the ability actually to communicate one's views to others. ICTs can be used to create a public forum where this communication can take place, or it can restrict expression by placing limits on a

[6] See Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999, Ch. 11: "Privacy".

[7] For example, many countries currently use filtering software to limit the information that citizens can access on the Internet. *See* http://www.opennetinitiative.org/.

[8] *See, e.g.,* http://www.rsf.org/article.php3?id_article=16402 (describing the prosecution of dissidents based on information provided by Yahoo!).

person's ability to communicate with others. The right to seek, receive, and impart information, therefore, is closely tied to freedom of assembly and association (Article 20) since accessing and disseminating ideas often entail connecting with others in the Information Society.

Anonymous Expression

By Wendy Seltzer[9]

Anonymous expression has a long and distinguished tradition. Voltaire and George Eliot wrote under pseudonyms. Support for the ratification of the U.S. Constitution was procured through anonymous articles in the Federalist Papers. Modern-day bloggers and mailing-list contributors may not use the same flowery language and elegant pseudonyms, but their freedom of expression is no less important. The technology they use can facilitate either identification or anonymity – and that will affect the range and content of online expression.

Anonymity can make possible or enhance many expressive activities. The freedom to impart information thus includes the right to speak anonymously; freedom of assembly includes the right to associate without giving a name or without revealing group membership to outsiders; and the freedom to seek and receive information includes the right to listen, watch, and read privately.

Protections for anonymity are vital to democratic discourse. Allowing dissenters to hide their identities frees them to express minority views critical to an informed democratic discourse. Otherwise, fear that their identity may be uncovered and that they may be persecuted on account of their speech, may prevent those in political, ethnic, religious, or other minority groups from speaking at all. That silence in turn deprives the whole public of access to those ideas.

[9] Wendy Seltzer is Visiting Assistant Professor of Law, Brooklyn Law School, and a fellow at the Berkman Center for Internet and Society at Harvard Law School.

ARTICLE 20:

(1) Everyone has the right to freedom of peaceful assembly and association.

(2) No one may be compelled to belong to an association.

The right of association is affected by ICTs in various ways. Technology may serve to enable this right by providing the means of facilitating contacts, coordinating exchanges, and interacting with other persons in an association. However, technology can also hinder this right, if used to identify and target members of an association, or to disrupt or otherwise prevent peaceful assembly.

Technology also presents a threat to the right to refrain from joining an association. This "right to be alone" depends in no small part on the individual's choice not to interact with others. Technology can infringe upon that right, requiring that a person associate with others in order to obtain the full benefits available to members of society. It can also enable the identification and stigmatization of those who choose not to join a given association.

As noted above, the rights to enjoy privacy (Article 12) and to seek, receive, and impart information (Article 19) are linked to this package of rights – with technology reinforcing this relationship.

ARTICLE 21:

(1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.

(2) Everyone has the right of equal access to public service in his country.

(3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

Democratic elections, like many other facets of modern life, are becoming increasingly reliant on technology. Political candidates rely on media and communication networks to express their views and coordinate supporters. Candidates are not alone in doing so; politically active groups are also increasingly using the Internet to obtain grass-roots support for their proposals and to build a constituency and thus a voice.

Political use of ICTs can be harmful, however, where technology is abused to further a political candidacy or agenda.[10] Furthermore, the increasing use of technology in politics can present a barrier to entry, where certain classes of persons are effectively barred from political activity if ICTs are not broadly available for their use. Finally, as electronic voting is adopted as a means for carrying out elections, security against corruption is increasingly dependent on specialists.

ARTICLE 26:

(1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.

(2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace.

(3) Parents have a prior right to choose the kind of education that shall be given to their children.

Education is becoming reliant on technology in two ways. First, education about technology itself is growing in perceived importance and value as technology emerges as a dominant facet of business and thus a viable career route for many learners. Second, technology is used to enable education on a vast range of subjects, allowing learners to improve their access to outside sources of information, use multimedia educational materials, and interact with teachers and fellow learners in new ways.

For these reasons, the single greatest threat that ICTs pose to the right to education is the possibility that they will serve to increase stratification based on income level and access to technology. As ICTs become a key component in an educational system, learners who are unable to obtain access to the technology have fewer

[10] For example, staff members of several members of the U.S. Congress have altered online encyclopedia entries about their employer, sometimes removing facts that cast the Senator or Representative in a negative light. *See* http://news.bbc.co.uk/2/hi/technology/4695376.stm.

resources available to them; moreover, the quality of non-technological educational resources may decline as a result of a greater focus on online education. Encouraging programmes that seek to prevent this result should be a primary concern of governments and infoethicists.[11]

Finally, technology can impact the ability of parents to choose the education presented to their children. ICTs can provide a broad range of options, allowing schools and parents to create individually crafted curricula that take advantage of the wide range of options. Conversely, however, parents may find it difficult to limit the information that their children access as part of their education precisely because of the ease of access provided by technology.

ARTICLE 27:

(1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.

(2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

Perhaps the greatest promise of ICTs is the concept of a true information commons, a medium that allows for the increasingly rapid discovery and distribution of new ideas. At the same time, technology can serve as a barrier to the spread of new ideas. For example, ideas that are only available on a specific medium may infringe on the rights of those who have no access to the required technology. Furthermore, even those with access to the Internet and other forms of ICTs can be blocked from full participation in cultural life by technological means, for example technology implementing data use restrictions.

Technology also poses a threat to existing intellectual property regimes and thus to the protection of rights-holders interests. File-sharing networks and other activities made possible by new technology have made the infringement of copyright much easier to effectuate and harder to prevent or prosecute.

In order to encourage a vibrant cultural life for all, infoethics must

[11] Two such programmes are the "One Laptop per Child" programme at the Massachusetts Institute of Technology (*see* text box, *infra*, and http://laptop.media.mit.edu/) and the Global Education and Learning Community (*see* http://www.sun.com/products-n-solutions/edu/gelc/).

consider the role that technological advancement may play in strengthening or weakening the enforcement of intellectual property rights.

Access to Information and Communication

In order for human rights to be fully operational in the Information Society, people need access to information, which in turn requires access to the means by which it is delivered. Therefore, infoethics goals must also focus on three major categories of access to information and communication that are essential to the exercise of human rights: (i) the public domain of knowledge and creative works; (ii) diversity of content on information and communication networks; and (iii) unfettered access to such information (including the means of delivery and the ability to use content).

■ Public Domain

One primary goal of infoethics is to extend the public domain of information; that is, to define an illustrative set of knowledge, information, cultural and creative works that should be made available to every person. This category contains, but is not necessarily limited to:

- **Government documents**, allowing an informed democracy to observe and evaluate the actions of their elected leaders, and thus allowing all persons to participate in the process of government;
- **Information about personal data retained by entities**, allowing individuals to understand the extent to which actions may or may not be private;
- **Scientific and historical data**, allowing all persons full access to the knowledge that they need to interpret events and to further the progress of knowledge;
- **Information relating to health hazards**, allowing persons to understand the risks to which they may be exposed and to act accordingly;
- **Information on the state of technology**, allowing the public to consider how the Information Society might guard against information warfare and other threats to human rights.
- **Creative works that are part of a shared cultural base**, allowing persons to participate actively in their community and cultural history.

UNESCO's *Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace*, adopted at its 32nd session in October 2003, provides the following definition of public domain information: "Public domain information is publicly accessible information, the use of which does not infringe any legal right, or any obligation of confidentiality. It thus refers on the one hand to the realm of all works or objects of related rights, which can be exploited by everybody without any authorization, for instance because protection is not granted under national or international law, or because of the expiration of the term of protection. It refers on the other hand to public data and official information produced and voluntarily made available by governments or international organizations."

The extent of the public domain is frequently contested. Public access to government documents and deliberations is naturally restricted by the need for confidentiality in certain affairs; similarly, access to personal information is constrained by privacy concerns. Some nations choose to remove certain content from the public domain, deeming exposure to this material harmful to the population at large.[12] Scientific research and knowledge may be limited by government regulation, often due to ethical concerns.[13] Intellectual property laws frequently reduce the public domain by granting exclusive license over creative works to the holder of the intellectual property rights, with varying degrees of fair use permitted.[14]

However, infoethics perhaps need not determine whether any given line between "public domain" and restricted information or intellectual property is "right." Instead, infoethics should focus on ensuring that information that is clearly part of the public domain is available to all persons. Information on health risks of new technologies should be readily available and distributed to all potential users. Creative works that are part of the public domain should be clearly indicated as such. Governments should allow access to documents that are not properly secret,[15] including

[12] In Germany, for example, content promoting neo-Nazi organizations or denying the Holocaust is prohibited. *See* Deutsche Welle, "Trial Highlights Limits of Free Speech in Germany," *available at* http://www.dw-world.de/dw/article/0,2144,1896750,00.html (describing the criminal trial of Ernst Zündel on charges of "inciting racial hatred" based on his denial of the Holocaust).

[13] For example, the UN has recently passed a resolution urging Member States to prohibit human cloning in any form, but it was unable to reach an agreement to pass a binding form of the same resolution. *See* United Nations Declaration on Human Cloning, U.N. Doc. No. A/59/516/Add.1 (2005).

[14] *See* Ruth Okediji, "Towards an International Fair Use Doctrine," 39 Columbia J. Transnat L. 75 (2000).

[15] South Africa provides individuals a right of action to obtain information held by private entities. *See* Promotion of Access to Information Act, Act No. 2 of 2000 (The Republic of South Africa).

making those documents available over commonly used communication and information media.

Diversity of Content on Information Networks

ICTs also can have a great impact on the diversity of content on information networks. In an ideal society, the content available on information networks should reflect the diversity of legitimate preferences of the population. In addition, the information networks should be open to content from all sources, allowing any interested person to be a creator of content rather than a mere consumer.

Broadcast media, such as television and radio, allow content to be rapidly delivered to consumers in distant places. However, broadcast media tends to cater to the population segments with the most economic power; the substantial startup costs of operating a television channel or radio station deter the distribution of content targeted at niche audiences,[16] and existing channels may have no incentive to accept content from other sources or to provide diverse content.[17]

In Brazil, observers have expressed concern about the diversity of content available on cellular phone networks.[18] Cellular phone networks are currently the dominant means of distributing interactive content; while 45% of the population has access to cellular phones, only 12% has access to the Internet. Not surprisingly, then, cellular phone networks are increasingly becoming carriers of various forms of content beyond voice telephony; music, video, interactive games, and other material can be accessed on cellular phone networks. Thus, as with traditional media enterprises, cellular phone companies may have exclusive control over the content available to a large fraction of the population, and therefore have the potential to promote or limit the delivery of available content.

ICTs offer the potential to overcome these obstacles to content diversity.

[16] Some nations have attempted to address this problem through regulation. In Germany, for example, each state must either provide a public network supplying diverse content or must regulate private networks to ensure that they provide a diversity of content matched to the interests of subsets of the population. *See* Uli Widmaier, "German Broadcast Regulation: A Model for a New First Amendment?", 21 B.C. Int'l & Comp. L. Rev. 75, 93-99 (1998).

[17] The United States attempted to regulate the relationship between television networks and the creators of television programming, but has abandoned that effort. See Christopher S. Yoo, "Beyond Network Neutrality," 19 Harvard J. L. & Tech. 1, Fall 2005, p. 49 n.188.

[18] Email conversation with Ronaldo Lemos, Creative Commons Brazil, February 2006.

In principle, ICTs substantially reduce the cost of producing and distributing content, allowing diversity of both creative works and creators. In allowing the generation of more interactive content, they transform consumers into active participants.

■ Unfettered Access to Information

Establishing a base of public domain information and diversity of content on information networks are laudable goals. However, the fulfillment of the spirit of these goals depends on the actual ability of persons to access and use the content and information that the public domain and diversity make available. Thus, one of the dominant goals of infoethics is to achieve universal access to all legal content. There are two, largely distinct, components to this goal: ensuring that all persons are able to *obtain* the content, and ensuring that all persons are able to *use* the content that they obtain.

The ability to obtain content requires access to the information networks or other channels of distribution, which can be accomplished either by increasing access to a particular channel or by providing additional channels of distribution. For instance, a country whose citizens have limited access to computers and the Internet cannot achieve the goal of universal access to information simply by ensuring that content is available online. Instead, it must determine the best course of actually making that content available to its population. This might be achieved by deploying new technologies like web-enabled mobile phones to increase connectivity; it might also be accomplished by ensuring that the content is also available in other forms to those who cannot access it online.

Diversity of content is heavily reliant on maintaining "network neutrality" so that no single entity can serve to limit access to (legal) content.[19] Under network neutrality, each node on the network is content-blind, passing along all traffic without concern as to its type or content. Thus, if fully implemented, network neutrality would require that all nodes on a network (including Internet service providers, or ISPs) pass along traffic without concern for (or even identification of) its origin, destination, and content.

Complete neutrality, however, carries its own hazards: a network that is entirely content-neutral encourages the diversity of legal content, but it also permits various forms of illegal

[19] *See, e.g.,* Mark N. Cooper ed., *Open Architecture as Communications Policy*, Center for Internet and Society at Stanford Law School, 2004.

content, ranging from pornography to spam and viruses. Infoethics should thus seek to shape the future of ICTs to retain the positive features of network neutrality while encouraging developments that limit its harms.[20] A key question here is whether edge devices might better address harms than could changes to the network itself since edge devices may be better technically and are more likely to rest under the user's control.

Search engines present another access point where the practical accessibility of content may be limited. Given the sheer volume of data available on the Internet, many users rely on search engines to locate desired content; thus, any content that cannot be accessed via search engines may be effectively inaccessible. Like ISPs, search engines thus have the potential to act as a chokepoint and to affect the diversity of content available on an information network, promoting some content by placing it atop a list of search results while selectively filtering other content. Google, for example, has filtered searches conducted on its French and German language sites, removing matches that link to Nazi or anti-Semitic content.[21] Again, however, this capability is not ethically questionable per se; it may simply require oversight to ensure that it is being utilized to remove only illegitimate content.[22]

If information is distributed via ICTs, access to it fundamentally requires access to the technology itself. Increasingly, projects are being launched to remedy lack of ICTs access, providing a solution that may be more cost-effective and more beneficial than projects to provide information in various offline formats. The One Laptop per Child Foundation, for instance, seeks to leverage advancing technology to produce cheap, low-powered computers with wireless network capacity that can be widely distributed in poorer segments of the world.[23] (See Text Box, below.) Moreover, as will be discussed in the sections that follow, the problem of exclusion could diminish as the cost of networked computing drops.

Still, even if the cost of ICTs declines to a point where today's technology

[20] *See* Jonathan Zittrain, "Without a Net," in Legal Affairs (January - February 2006), *available at* http://www.legalaffairs.org/issues/January-February-2006/feature_zittrain_janfeb06.msp.

[21] *See* http://cyber.law.harvard.edu/filtering/google/results1.html; *cf.* Isabell Rorive, "Freedom of Expression in the Information Society," Working Paper for the Preparatory Group on Human Rights, the Rule of Law and the Information Society 8, Sept. 15, 2004 (discussing censorship by search engines in France, Germany, and China).

[22] In addition, users could configure personal filters to prevent exposure to undesired content.

[23] *See* http://laptop.org/.

becomes affordable for all, there will always be new advancements that begin with limited accessibility. In this regard, the *process* of ICTs diffusion warrants attention.

In the development of information networks, it is important to ensure that standards organizations and the like are not overly influenced by particular agendas. Allowing any one group to capture a regulatory or standard-setting organization prevents these organizations from achieving a balance between interests. Designers of network technologies could be mandated or given incentives to offer the greatest overall benefit to society, rather than to support the demands of a specific group (e.g., owners of copyrighted content).

Ensuring that all persons are able to use the content that they obtain poses other challenges. Even where content is "available," it is of little value unless it can in fact be understood and used. Thus, universal access to information requires that content be distributed multilingually, or that technology be deployed to translate content into a usable form. Similarly, technology can be used to make information accessible to the physically disabled. In addition, content should be easily machine-readable; public domain content in particular should be released in a format that is broadly used and does not require specific applications or devices to access.

One Laptop per Child: The $100 Laptop

By Samuel Klein

The "One Laptop per Child" (OLPC) initiative, conceived at the MIT Media Lab and first announced in January 2005, is an effort to mass-produce cheap, durable laptops and to distribute them throughout the world to improve education for children. The stated goal of the project is "to provide children around the world with new opportunities to explore, experiment, and express themselves." If all goes as planned, these opportunities will be provided entirely through the laptops, which, equipped with free software, will be tools for creating and receiving content.

The project to date has focused on developing cheap, durable hardware designs, particularly a low-cost display – with a target production cost of $100 per laptop in its early stages (less later) – and building a network of partners to help produce the necessary hardware and software. The project relies on economies of scale: The production schedule calls for at least 5 million laptops. The laptop will have built-in wireless capability, will work as part of a local mesh network when there is no access to the global Internet, and will support innovative power sources, including winding by hand.

The laptops are meant to be widely distributed within a given area, one to every child in a school or region. Distribution is to be carried out through schools via national governments. The OLPC Chairman, Nicholas Negroponte, says the team has had initial discussions with officials in China, India, Brazil, Argentina, Egypt, Nigeria, and Thailand;[24] the team recognizes, however, that unless a country can provide one laptop for every child in its population, hard decisions about where and how to distribute the laptops must be made.

There are philosophical goals to the project, in addition to the technical ones. Laptops were chosen in part because they can be taken home and can engage the whole family. A stated intent is that children will *own* their laptops, though these may be among the most expensive and novel personal items in their neighborhood.

[24] From the One Laptop Per Child FAQ: http://laptop.org/faq.en_US.html (viewed November 8, 2006).

The development of a deployment and education plan – from the design of software and content to be included on the machine, to research and suggestions on how to implement an effective "One Laptop per Child" teaching environment – is one of the more recent project goals to take form. OLPC is currently soliciting input on how to proceed with and study this goal.[25] While OLPC is an educational project, this effort is not simply a question of pedagogy. Distributing millions of laptops to areas where computers are scarce, and providing every member of a community's youngest generation with "a world view" and with exotic tools and knowledge completely foreign to their elders, disrupts the status quo in a significant way.

The question of how to select content, distribute the laptops, and recommend their uses, so as to produce desired change without unwanted social and cultural upheaval, is a crucial question and one on which many groups may wish to engage. For an initiative of its size, OLPC is unusually open to suggestions; the project has a publicly editable list of tasks that includes a request for panels of thinkers to study some of these issues and propose improvements and recommendations.[26]

[25] From http://wiki.laptop.org/wiki/OLPC_software_task_list#Eductional_community_engagement (viewed November 8, 2006): "We propose including other intellectuals, artists, civic leaders in order to provide a diversity of experience and expertise."

[26] *Id.*, http://wiki.laptop.org/wiki/OLPC_software_task_list#Strategic_research (viewed November 8, 2006).

The Ethical Challenges of Emerging Technologies - Case Studies

With the increasing importance of ICTs in the world comes a growing need to recognize the ethical ramifications of new technologies. Moreover, the rapid rate of technological change demands that we understand emerging technologies and their potential effects as they are being developed, and not wait until the consequences are manifest before we prepare for them. By understanding tomorrow's technologies in light of infoethics goals, society can better anticipate their effects and deploy them in a manner that leverages their benefits while mitigating potential harms.

The following case studies highlight some of these technologies and flag many of the infoethics concerns that accompany them.

The Semantic Web and Other Metadata

What the Semantic Web Is

The Internet was conceived as a mechanism to allow humans to initiate the exchange of text, images, and other information. With the exponential growth of content available on the Internet, however, this is increasingly becoming impractical. Search engines seek to mitigate this problem by providing a tool to navigate the web, but they provide only a partial solution. To make the web fully navigable, interoperable metadata, or data about data, is required. This metadata can also serve to make the web more machine-readable, allowing computers to evolve from dumb tools to intelligent agents. The semantic web[27] promises to offer such metadata.

[27] The Semantic Web is an official project of the World Wide Web Consortium, which was founded by Tim Berners-Lee, the web's inventor.

How the Semantic Web Works

The Internet existed for nearly three decades before it took off as a popular medium for information and communication.[28] Although the Internet was based on common computer "languages", or code, from the start (TCP/IP, SMTP, etc.), what triggered its uptake was the royalty-free nature of the languages of the "World Wide Web" (web) – that is, HTML and HTTP – and the fact that HTML was particularly user-friendly. These two languages allowed the "loose coupling" of machines involved in exchanging information – meaning any web client seeking information could talk to any web server, which could then provide that information remotely, in a form that people could enjoy. Internet usage increased dramatically, and this phenomenon spurred the creation of more content, which in turn gave rise to more exchange.

Given the high volume of web content, the semantic web is being designed "to create a universal medium for the exchange of data"[29] – using the same loose coupling properties for programmatic data as there was for human-rendered data with HTML. This new language should provide predictability in a cyberspace of ever growing exchanges, with the vocabulary of metadata lending greater precision as computers access and analyze content directly.

The semantic web combines a set of computer languages[30] to provide machine-readable descriptions of web content. This metadata may be created by humans or computers, and is designed to provide context about the content without requiring a person or machine to actually parse the content. Once a piece of information is tagged, the semantic web can reason about it and develop contextual meanings based on observations about connections that the piece of information has with others. This enables machines to search web sites and carry out tasks in a standardized way.

Although the name refers to "web", this initiative is geared toward enabling machines to handle data among a range of Internet applications.

[28] *See* History of the Internet (Wikipedia entry), http://en.wikipedia.org/wiki/Internet_history (viewed November 8, 2006).

[29] *See* http://www.w3.org/Consortium/activities#SemanticWebActivity.

[30] For example, Resource Description Framework (RDF), Web Ontology Language (OWL), and Extensible Markup Language (XML).

Ramifications and Concerns

The wealth of content available on information networks, particularly the Internet, is useful only if people can actually find and access the information that they need. The semantic web allows people to use computers as agents to search for appropriate content based on a wide range of criteria – which could include the public domain or intellectual property status of the content, alternate sources of the content in different formats or languages, or even the existence of evidence serving to refute the view offered in the content.

The wealth of content is closely related to the Internet explosion, which is often credited to the "network neutrality" principle that holds that all traffic should be treated equally. Oddly, the semantic web could cut against this neutrality by equipping parties with tools to filter Internet content based on its associated metadata: ISPs, routers, or search engines could use the metadata to distinguish between types of content and grant preferential treatment to certain traffic, raising barriers to entry for new service or content providers. In this regard, the semantic web's machine-readable labels could mark content for discrimination and reduce the ability of users to generate and share material.

Moreover, some would contend that, in giving users the ability to access only the content that they desire, the semantic web could damage public discourse. The theory here is that full participation in society requires a forum in which a person can make his voice heard, but that the semantic web and other technologies allow other users fully to customize their experiences and to receive only the content that they explicitly request. In other words, the semantic web enables end-user insularity and so indirectly destroys the forum. Here again, the worry is that the semantic web could in fact harm the very connectivity that it was designed to promote.[31]

More theoretically, machines must be programmed to categorize and assign values to information – so that, for example, personal data can be distinguished from weather patterns and flagged as warranting privacy. In

[31] *See* Cass R. Sunstein, "The Daily We," Boston Review (Summer 2000), *available at* http://www.bostonreview.net/BR26.3/sunstein.html. Others would argue, however, that even a seemingly low rate of exposure to differing views via the Net (e.g., 15 per cent) may suggest greater public dialogue than had previously been the case. *See* work by Eszter Hargittai, *Cross-Ideological Conversations among Bloggers*, http://crookedtimber.org/2005/05/25/cross-ideological-conversations-among-bloggers/ visited November 8, 2006 (describing work by Eszter Hargittai, Jason Gallo and Sean Zehnder analyzing cross-linkages among liberal and conservative political blogs).

this sense, there are risks inherent in designing tools simply to exchange information without simultaneously coding them to assign a higher value to data relating to humans. Safeguarding human rights may require programming computers to put personal data on a higher plane.

Still, one should not overstate the dangers of the semantic web. After all, these harms are possible even without metadata and are far from certain to occur even with metadata.

On balance, it seems the semantic web will support the goal of promoting access to information by making existing content far easier to identify, locate, and use.

Digital Identity Management

The previous case study discussed how metadata is allowing increasingly sophisticated machine-to-machine exchanges. This increase in communication between machines creates the potential for good or harmful consequences, such as the lowering of transaction costs in commerce or the launching of malicious virus attacks.

This section first looks at how the automated exchange of data is driving the need for digital identity management tools that afford better control over the flow of personal information. It sets the stage for the next case study, which explores how, through biometrics, metadata can go beyond a person's diverse digital personae to pinpoint an embodied person.

What Digital Identity Management Is

Simply stated, digital identity management concerns the control of digitized information pertaining to a person. This information is sometimes referred to as "personal data," or "personally identifiable information." This latter term more precisely suggests that the data can be linked to the specific individual involved.

As originally designed, the architecture of the Internet did not provide a mechanism to verify, or authenticate, the identities of users. Its designers were working in a different time and culture from today's online environment, with that early community of Internet users comprising essentially a highly cooperative, high-trust society of computer scientists. The Internet they brought to bear reflected this culture.

With the explosion in Internet usage drawing strangers to interact at unprecedented rates, it is not surprising that the once trustful atmosphere of the Internet has changed, and that people are starting to view the space with growing reserve. Put another way, the Internet has undergone a sort of urbanization, where more and more people are gravitating toward it for its benefits, but where the "traditional" sense of community has broken down and people find they must be on guard. Computer scientists are starting to say: "In retrospect, we should have designed an authentication layer into the Internet. Now, with the Internet scaled up large, and with so much commerce passing over it, the potential for fraud is enormous."[32]

E-commerce statistics bear witness to this shift. Statistics published last year showed a sharp drop in the number of consumers who feel comfortable participating in e-commerce.[33] People have learned to question whether the person or entity at the other end of a transaction is indeed who he, she, or it claims to be, and people wonder if they can actually hold that other party accountable should something in the exchange go awry. By responding to an email or filling out an online form, will a person be a victim of phishing or pharming?[34]

At the same time, it is natural for Internet users to lament the fact that they currently have to remember passwords and fill out all sorts of forms when reserving a rental car, purchasing a book, or engaging in some other common transaction online. Although this is a repetitive and often frustrating task, people have been "trained" to provide information in this way, and do so without thinking.[35]

[32] Interview with Paul Trevithick, Project Lead of the Eclipse Foundation's Higgins Trust Framework project, August 2005.

[33] Riva Richmond, "Internet Scams, Breaches Drive Buyers Off the Web, Survey Finds," Wall Street Journal, June 23, 2005, p. B3, reporting on a Gartner study of 5000 online consumers. The article states that more than 42% of online shoppers and 28% of those who bank online are cutting back on these activities due to security and privacy issues.

[34] David Bank and Riva Richmond explain in "Information Security: Where the Dangers Are," Wall Street Journal, July 18, 2005: "In 'phishing' scams, fraudsters send emails that appear to come from a trusted source, like Citibank or eBay. Click on a link in the email, and you're directed to a fake Web site, where you're asked to reveal account numbers, passwords and other private information… Then there's 'pharming,' where hackers attack the server computers where legitimate Web sites are housed. Type in the address of the legitimate site, and you are redirected to a look-alike."

[35] This point is often made by Kim Cameron, Microsoft's Identity and Access Architect. He reminds industry colleagues that people are not stupid, but rather they have been given poor tools for interacting online.

Industry specialists say that digital identity management tools will allow online exchanges to be much more secure and convenient, as this technology will enable enhanced control over digitized information relating to a person.[36]

Consumers have to date not embraced this technology because it has not yet been presented in a form they are willing to accept. Microsoft is still smarting from its past experience trying to provide such tools,[37] and other technology companies have taken note: People do not want a single, powerful company to be at the center of their trust relationships or to occupy a monopoly position in handling their personal data.

Technology developers[38] are therefore now focusing on user-centric approaches to digital identity management. In this new paradigm, a person will choose among different "identity providers" to take care of his personal data, with his permission then required for that identity provider to pass his information to another person or entity in a transaction; meanwhile, the new system will also verify the identity of that other party to the transaction.

How Digital Identity Management Works

This user-centric identity model has two primary parts: one that handles the exchange of identity information as it passes *between* endpoint computers or devices, and the other that helps a user manage his identity information *on* his computer. For the part between devices, this new system may be thought of as a set of rules for exchanging information[39] (called computer protocols) in the form of packaged, sealed "tokens". The user can hire whatever identity provider he wants to guarantee his information and package it into tokens, even employing different providers for different purposes (e.g., one to handle credit card details; another to manage core personal information like name and date of birth; another to process medical records; etc.). Identity providers may reside on a

[36] See, e.g., Kim Cameron's "Identity Weblog" at http://www.identityblog.com/, Dick Hardt's "Identity 2.0" weblog at http://www.identity20.com/, and others available at http://www.identitygang.org/individuals.

[37] In the past several years the market has largely rejected Microsoft's "Passport" identity management systems. The market also resoundingly rejected Passport's predecessor, "Hailstorm".

[38] OpenID, Sxip, the Liberty Alliance, Shibboleth, Passel, and other industry players have joined Microsoft in the quest to provide identity management tools that the market will accept.

[39] A consortium involving Microsoft, IBM, and other technology firms developed the standards for this exchange as part of a larger set of standards for web services.

person's computer or device, or they may be located elsewhere, accessible through the Internet.

So, for example, when a person wants to conduct an online transaction, the computer or device on the other party's end (in industry parlance, the "relying party") will indicate to his "agent" what package of information is needed. The agent will then request a token containing these claims from one or more identity providers that the person has entrusted with this information; the identity provider(s) will then pass the token to the relying party. A person can supervise this exchange every time it occurs, or he can do so once and then opt to let the exchange take place automatically henceforth.

The second part of the system is what takes place on a person's computer or device. Instead of remembering passwords or typing in an array of information in an online order form, a person conducting e-commerce will simply choose a visual representation or icon of the particular package needed (e.g., an icon symbolizing banking, medical, or tax information). When he chooses that icon, his agent initiates a call for the release of digital tokens by identity providers to the relying party, as described above. The agent will be able to operate on all sorts of devices, be they desktop computers or cellular phones or other mobile devices. This agent will be the sole component of the digital identity system with which the user will need to authenticate himself directly (e.g., through a fingerprint scan).

As the trusted intermediary, a person's identity agent will sit at the center of the user's communication and have access to all identity information exchanged. It will unwrap a token and translate the claims from one system's language into a format recognizable to another. To protect privacy insofar as possible, this trusted intermediary will ideally keep to a minimum the amount of information disclosed for a given transaction. In many cases, this may require that the information in a given token be transformed into an alternate token corresponding with a specific request. For example, the intermediary will be able to take information from a token vouching that a person was born on a specific date (e.g., July 20, 1969) and translate it so that the new claim reveals nothing more than that the person is indeed over 21 years old.

Putting theory into practice, Microsoft is planning to roll out a user-friendly token exchange system with visual icons called "Cardspace" that will resemble cards that people currently carry in their wallets, such as a driver's license, a credit card, etc. While the plan is to introduce this system in the new version of Windows, called "Windows Vista",[40] the digital identity system will also be available in upgrades for Windows XP. Microsoft has been on the private campaign trail to convince big e-commerce players like Amazon and eBay to accept these new services in exchange for more direct access to Microsoft customers. Because so many people already use Windows XP, the spread of these services will not hinge on widespread adoption of the newer Windows Vista. Given the fact that Windows XP runs on hundreds of millions of machines today, these digital identity management tools have a strong probability of taking root.

Meanwhile, IBM and Novell in February 2006 announced their intention to offer programming code to allow for similar digital identity management tools to be built using open-source software. The project, named "Higgins", will enable different identity management tools to interoperate.[41] Rather than managing digital identities itself, Higgins overlays different systems in order that information might be exchanged among them at a user's request.[42] One attractive prospect is portability in reputation systems, which would allow, for example, a person to take the reputation he has built up in the eBay[43] community and carry it over into the world of Second Life.[44] The technical requirements for such portability are just starting to be explored.

Ramifications and Concerns

The new digital identity management tools promise to cut today's phishing and pharming and may also address spam problems. Since an identity agent can help to minimize data disclosed to a merchant or other entity with which a person interacts, the technology may boost privacy as it minimizes the number of entities that have access to an individual's profile. Perhaps most significantly, the system's distributed architecture should reduce vulnerability to attack since theoretically data is not concentrated in one place.

If the system can protect personal data in this way, digital identity management has many possible ben-

[40] Worldwide availability of Windows Vista is scheduled for early 2007.

[41] The Eclipse Foundation, an open-source community, manages Higgins.

[42] Interviews with John Clippinger, a senior fellow at the Berkman Center for Internet and Society at Harvard Law School, Fall 2005.

[43] *See* http://pages.ebay.com/services/forum/feedback.html describing the eBay reputation system (viewed November 8, 2006).

[44] *See* http://secondlife.com/whatis/ describing the 3-D virtual world of Second Life (viewed November 8, 2006).

efits to society, including preventing malicious conduct and making the Internet a better forum for commerce. From this vantage point, the technology promotes privacy, security, and improved living standards.

So, too, tools enabling the exchange of personal data based on an individual's preferences may facilitate social interactions. Paul Trevithick, Project Lead for Higgins, emphasizes the benefits of a user-centered networking layer that "gives people more control over their digital identities across a wide variety of computer-mediated contexts (e.g., email, instant messaging, e-commerce, shared spaces, and enterprise directories), especially those involving social networks."[45] In this way, digital identity management tools may serve as a boon to freedom of assembly.

Looked at from another perspective, however, the existence of digital identity management systems could pose significant risks for privacy and security. As noted, in the proposed architecture a person's identity agent will serve as the most trusted intermediary in the new digital identity system; however, current technology provides no guarantee that a person's identity agent will not collude with the other parties to a transaction (i.e. identity providers and relying parties).

In addition, it is quite conceivable that the market will not support the host of identity providers that advocates of systems speak of, but that instead there will be a natural concentration in identity provisioning. Quite simply, users might find it inconvenient or expensive to separate their data and designate elements to different identity providers. Or, relying parties might be restrictive in recognizing identity providers, with the result that a limited set of identity providers would dominate the market. Either way, a small number of identity providers would have control over a great deal of personal data. Moreover, given current designs of the system, it is technically possible for identity providers and relying parties to collude. In other words, it is unclear how the players in the identity management infrastructure will be accountable to users and the Information Society generally.[46] Of course, the market may spur improved technologies whose architecture guarantees trustworthy behavior, and the law may well reinforce these incentives.[47]

To some, the primary infoethics concern is what happens if a big player

[45] Interview with Paul Trevithick, September 20, 2005.

[46] Mary Rundle and Ben Laurie, "Identity Management as a Cybersecurity Case Study," Berkman Center Publication Series, September 2005, p. 8.

[47] Microsoft took a strong stance advocating privacy legislation in 2006.

– e.g., a government or a mega-corporation – usurps a distributed, user-centric identity system and applies its own globally unique identifier, violating all the user-centric principles that industry developers have advertised. In other words, there are currently no innate technological protections regarding possible future uses of these tools. If the tools were used throughout the Information Society in an abusive manner to discriminate, intimidate, and block communication, human rights and related infoethics goals would be in serious jeopardy.

The magnitude of these effects should not be underestimated given the revolution that digital identity management may bring in machine-to-machine interactions, or "web services". Dale Olds, a key Novell engineer in this area, has indicated that Higgins may seek to develop an additional technology that would *automatically* transfer information from an individual's given digital identity (or persona) when he visits a web site.[48] It may be here that digital identity management tools will have their strongest impact: By enabling machines to exchange personal data automatically on people's behalf, the tools will throw off one of the biggest impediments to web services. Hence, the empowering of machines in this way could ignite an explosion in machine-to-machine interaction.

Machine empowerment points to perhaps the biggest unknown and the one with the greatest potential impact – concerning *not what humans* may do with these tools, but rather *how machines will treat humans* with personal data so well organized. Kim Cameron, Microsoft's chief Identity and Access Architect, underscores these apprehensions:

> The broader aspects of the way network intelligence responds to who we are is of much more concern to me when I think forward twenty years… Beyond the abuse of power there are other equally chilling possible futures – involving the potential relationship between human kind and machine intelligence. I realize people are not likely to want to discuss this because it is too forward thinking, but the two actually can mutually reinforce each other in truly frightening scenarios.[49]

[48] Robert Weisman, "Harvard, tech firms push data privacy: Goal is to let Net users control the personal," Boston Globe, February 27, 2006.

[49] E-mail exchanges with Kim Cameron, Fall 2005 (cited with permission).

Biometrics

While digital identity management is expanding the metadata vocabulary to allow automated exchanges of personal data, its real-world counterpart, biometrics, is fostering the application of metadata to physical space. Since both deal with a person, there is a blending of the virtual and real worlds through linguistic fiat as the same basic metadata is used to describe aspects of both.

What Biometrics Is

Biometrics is an emerging technology that measures and analyzes unique characteristics of individuals, including both physical and behavioral. Among others, the following characteristics are often listed as biometrics:

- DNA
- Facial patterns
- Fingerprints
- Gait
- Iris patterns
- Retina patterns
- Scent
- Signature
- Typing cadence
- Voice

Although biometrics is known to have existed in China as early as the 14th century,[50] it is considered an emerging technology because the capture, measurement, and analysis of biometrics are increasingly automated and in digital form. As such, biometrics can be combined with other technological advancements – for example metadata (since biometrics can be categorized for processing and exchange by machines); digital identity management (since they concern control over personal data); and sensors (since measurements are often captured by sensing devices).

The primary driver of development in recent years has been the desire for security, both on the part of the private sector (e.g., to restrict access to trade secrets) and on the part of government (e.g., to limit travel by criminals or suspected dangerous persons). Many governments stepped up research and development in this area following the terrorist attacks in the United States on September 11, 2001.

How Biometrics Work

A person's biometric is registered in a system when one or more of his physical and behavioral characteristics are captured by a device. The measurement is then processed by a numerical algorithm that in essence abstracts it into a digital form. The result is then logged into a database. At this point the person may be considered "enrolled", whether or not

[50] Wikipedia entry for "Biometrics" (http://en.wikipedia.org/wiki/Biometrics), viewed February 7, 2006.

he is aware of it. Each subsequent attempt to have that person's biometrics authenticated by the system requires the biometric to be captured and digitized anew. That digital representation is then compared against those in the database to find a match.

Ramifications and Concerns

In 1997 the International Civil Aviation Organization (ICAO) began developing "a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents…"[51] This blueprint was adopted by ICAO members in 2003. With implementation requiring major effort, a full programme is underway in ICAO to accomplish this harmonization.

ICAO's 188 member countries are arguably obliged to conform to this global requirement for electronic travel documents: After all, Article 22 of the Chicago Convention charter calls for signatories to "adopt all practicable measures... to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially in the administration of laws relating to immigration, quarantine, customs and clearance." ICAO has stated that the blueprint will help members "to implement a worldwide, standardized system of identity confirmation."[52]

As mentioned above, the pivotal step in the user-centric identity management system involves the initial authentication of the user to his electronic agent – with subsequent claims transfers then based on this verification. It is conceivable that ICAO's universal biometric standards for Machine Readable Travel Documents would evolve into a global mechanism for government-sanctioned proof of identity – and at the same time serve in the initial authentication. Such an internationally recognized digital identity would then seem to constitute the ultimate guarantee that a person was who he said he was and that claims transfers based on that identity were valid.

It is easy to see why the international system might adopt such an approach. After all, a globally unique identifier would seem the ultimate backer for digital identity management and so would allow online transactions to thrive; it could also help ensure order in the face of cyber attacks. So, too, it would provide a global method for enforcing other international commitments to monitor individuals' activities for the sake of stability in taxation, financial services,

[51] See ICAO's web site at http://www.icao.int. For an additional overview of this organization and a summary of this initiative, see http://www.netdialogue.org/initiatives/icaomrtd/.

[52] ICAO Press Release dated May 28, 2003.

environmental protection, and more.[53] In short, a globally unique identifier could seem the answer for according a person official digital existence in the Information Society.

For a system to ensure that each person had one and only one government-issued identity, it would need to have a central administration.[54] It is foreseeable that an international agency might be tasked with administering this system. In light of the fact that international bodies have not been immune from corruption, trusting a single, global body with this critically sensitive information could leave the Information Society in terrible shape. Simply stated, international institutions are not equipped with mechanisms to prevent the abuse of power.

Moreover, a centrally administered identity system would be a prime target for attacks. No institution is able technically to guarantee system security. A far less risky approach would be to prevent centralization of this data.

If the international system did embrace extensive use of biometrics or another globally unique identifier, the move could signal the effective end of anonymity. It would become feasible to compile a complete profile of a person's activities – including where the person has gone, what he has spent money on, with whom he has been in contact, what he has read, etc.[55]

This death to anonymity would meanwhile be coupled with asymmetry in information: The individual's every move could be monitored, yet he may not have any knowledge of this surveillance. Beyond privacy, such a state of affairs does not bode well for the exercise of other fundamental freedoms such as the right to associate or to seek, receive, and impart information – especially as the intimidation of surveillance can serve as a very restrictive force.

Finally, biometric techniques like facial recognition are becoming more accurate over time. However, false positives in biometrics could implicate a person in a crime, raising the infoethics question of what constitutes proof if a person is to be presumed innocent until proved guilty.

[53] For a discussion of these initiatives, see Mary Rundle and Ben Laurie, "Identity Management as a Cybersecurity Case Study," Berkman Center Publication Series, September 2005.

[54] Stephen T. Kent and Lynette I. Millett, *Editors*, "IDs – Not that Easy: Questions About Nationwide Identity Systems," Computer Science and Telecommunications Board: Committee on Authentication Technologies and Their Privacy Implications, Washington, DC: National Academy Press, 2002, Chapter 2.

[55] Of course, such profiling may be possible without biometrics or other globally unique identifiers. Data profiling is a growing business and will be furthered even more by the technologies that follow.

Radio Frequency Identification

What RFID Is

Radio frequency identification (RFID) is a technology that enables data exchange from a small, inexpensive, wireless device, called an RFID tag, that is equipped with a computer chip and antenna. An RFID device can simply transmit its unique identification number; it can also transmit additional data about a specific object (e.g., date of a product's packaging, price, factory of origin, etc.) or person (e.g., name, health status, etc.). Although the technology has been used since the 1980s, it has become more widespread today due to advances in networking, miniaturization, and computing.

One major use of RFID technology is in the area of product tracking. Wal-Mart and the U.S. Department of Defense are known to be big drivers from the demand side as they have required their largest contractors to use RFID tags.[56] A main motivator is supply chain and inventory management. When a pallet is loaded with products that each contain an RFID tag, the entire load can be accounted for as it passes a reader – for example, as it is transferred onto or off a delivery truck. In retail RFID tags are expected to replace barcode labels altogether since the newer technology allows item-specific labeling.[57]

So, too, RFID technology is being applied to transportation, in the name of promoting smooth travel and public safety. Airline companies hope to use RFID to cut costs and increase reliability in baggage handling, with an estimated savings of US $700 million per year.[58] Demonstrating the marketability of RFID chips for the recall of faulty products, Michelin in 2003 began testing chips in tires to allow automobile manufacturers to comply

[56] As reported by Todd Spangler, "Wal-Mart, the world's largest retailer, says it will double the number of stores using RFID to more than 1,000 by January 2007… bringing to more than 600 the number of supplier companies using RFID technology in concert with Wal-Mart. ("Wal-Mart Plans to Add RFID to 500 More Stores," Extreme RFID, September 12, 2006.) In 2003 the U.S. Department of Defense announced a policy requiring its suppliers to use RFID chips by 2005 (U.S. Department of Defense Press Release No. 775-03 of October 23, 2003, available at http://www.defenselink.mil/releases/2003/nr20031023-0568.html).

[57] Although predicted to be some years out yet, RFID tags could eliminate the check-out line as customers might walk past a reader with their collection of purchases and have an account automatically charged when leaving a store (http://en.wikipedia.org/wiki/rfid viewed October 6, 2006).

[58] Andrew Price, RFID Project Manager for the International Air Transport Association (IATA), speaking at RFID Journal's Aerospace Summit (September 26-28, 2006).

more readily with U.S. requirements for tire tracking, and the industry has since moved to standardize this practice.[59] Meanwhile, the automotive industry has decided as a group internationally to embed RFID chips in vehicles for reading by roadside equipment. This initiative follows government initiatives to reduce traffic congestion and accidents and to support environmental standards.[60] Many highway systems offer RFID enabled toll passes that allow vehicles to speed through electronic collection booths. These applications are used in parts of Australia, Canada, Chile, France, the Philippines, Portugal, Singapore, and the United States. Similarly, public transportation systems in Hong Kong, London, Moscow, New York, Paris, Perth, Taipei, and other cities have incorporated RFID chips into passenger passes.

RFID tags are also being used in items that people carry or wear in order to track individuals or verify their identity. Several corporations have begun embedding RFID tags into employee uniforms or identification badges, allowing an employer to track the whereabouts of an employee at all times or to restrict access to areas of buildings.[61] In 2005 Cisco began selling RFID servers that work with RFID chips embedded in uniforms to track employee whereabouts.[62] Similarly, for immigration control, many countries are incorporating RFID chips into passports to implement ICAO's requirement for contactless, machine-readable travel documents.

[59] These tire-tracking requirements stem from the Transportation, Recall, Enhancement, Accountability and Documentation Act (TREAD Act) passed by the U.S. Congress in 2000 in the wake of the Firestone tire problems encountered with Ford Explorers. For more information on RFID chips in tires, *see* http://www.rfidjournal.com/article/articleview/269/1/1/ and http://www.rfidjournal.com/article/articleview/2043/2/1/ (viewed October 11, 2006).

[60] Through its Dedicated Short Range Communications initiative, the international automotive industry has agreed to a short- to medium-range wireless protocol designed especially for automotive use. *See* http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm for information from the U.S. Department of Transportation, and http://www.ictsb.org/ITSSG/Documents/Mandate_M270.pdf for an overview of a European Commission mandate in the area of Road Transport Telematics (Mandate 270, published April 24, 1998 by Directorate-General III).

[61] This application of the technology dates back to 1989, when Olivetti Research introduced Roy Want's Active Badge. Use of such badges did not appear practicable until the broad uptake of the Internet in industrialized societies.

[62] "Cisco slammed for RFID staff tracker," Iain Thomson, Vnunet.com, May 4, 2005 (http://www.vnunet.com/vnunet/news/2127277/cisco-slammed-rfid-staff-tracker, viewed October 3, 2006).

(See the discussion above in the case study on Biometrics.)[63]

In the public health context, RFID chips were used in badges in two Singaporean hospitals[64] in 2003 to record who had been in contact with whom, as a preventive measure against the spread of Severe Acute Respiratory Syndrome (SARS). Information was stored for 21 days (the incubation period for SARS being 10 days) and then deleted to protect confidentiality.[65]

RFID chips are also being implanted in people. These devices currently are the size of a grain of rice and are said to last 20 years.[66] In the area of health, people may receive chip implants to store their medical data so that it is easily accessible and associable with them, particularly if they are unable to communicate.[67] Another use of human implants is in the employment context, where a few employers have used implants in employees to control access to ultra high-security areas. In 2004, the Mexican Attorney General's office implanted a number of its staff with an RFID chip to control such access and to serve as a tracking device in case they were kidnapped.[68] Perhaps testing early social acceptance of chip implants in humans for everyday uses, a nightclub has offered these devices to their VIP clients in Barcelona and Rotterdam for easy identification and drink payment.[69] Human-implantable chips are also being marketed as tools for immigration control, with the CEO of one leading company touting, "It's really no different than a tamperproof passport you can carry all the time," and adding, "[a]s concerns mount

[63] Malaysia issued the first RFID enabled passports in 1998 (http://www.wikipedia.org viewed October 6, 2006). At the June 2005 Computers, Freedom and Privacy Conference, the RFID technology planned for use by the U.S. Department of State was shown to be hackable. Shortly thereafter the agency put plans for RFID passports on hold; after apparently bolstering encryption, in March 2006 the State Department issued its first batch of these RFID travel documents in a pilot project. *See* Marc Perton, "US Issues First RFID Passports," Engadget, http://www.engadget.com/2006/03/13/us-issues-first-rfid-passports/.

[64] Alexandra Hospital and the National University Hospital participated in the pilot project.

[65] "Singapore Fights SARS with RFID," RFID Journal, June 4, 2003, available at http://www.rfidjournal.com/article/articleview/446/1/1/ (viewed October 23, 2006).

[66] "I've got you under my skin," The Guardian, Technology section, June 10, 2004, available at http://technology.guardian.co.uk/online/story/0,3605,1234827,00.html (viewed October 11, 2006).

[67] The VeriChip Corporation markets its VeriMed chip implants as allowing the identification of patients and health records. *See* http://www.verimedinfo.com/content/intro/patients (viewed October 3, 2006).

[68] *See*, e.g., http://www.verichipcorp.com/images/GSN_Mar06.pdf.

[69] *See* the "VIP" section of the web site of the Baha Beach Club in Barcelona, http://www.bajabeach.es/ (viewed October 11, 2006).

about falsified documents, VeriChip technology ensures security and privacy for the individual as well as increased security at our borders..."[70]

RFID implants are incorporating other technologies as well. For example, RFIDs equipped with bio-thermal sensors can register temperatures among animal populations. This technology has been put forward as a way to help monitor and combat the spread of the H5N1 avian flu virus.[71] Similarly, in a joint pilot programme, the Digital Angel Corporation[72] and the Brazilian Agriculture Research Corporation (Embrapa) have been implanting bio-thermal RFID chips in cattle so as to curb the spread of Hoof and Mouth Disease. According to the company's press release, "When scanned with an RFID scanner and used in conjunction with a database program, the bio-thermal chip can, in addition to sensing temperature, provide immediate access to specific information such as the identity of the animal, its age, medical history, where it has been, and its contacts with other cattle."[73]

In addition, motion-sensing RFID chips are being developed to monitor activity levels and routines of the elderly and people with chronic diseases. Data logs of people's movements will be used to profile people's habits, with alarms going off if behavior changes (e.g., if a person stops eating, taking medicine, or getting out of bed).[74]

For the visually impaired, a company called En-Vision America has developed smart-label RFIDs that work with readers to offer speech synthesis technology. The chip is programmed with the information written on a product's label, and this information is then spoken out in audible form

[70] "VeriChip Highlights Role Implanted Chip May Play in a Government Immigration and Guest Worker Program," U.S. Newswire, June 9, 2006, http://releases.usnewswire.com/GetRelease.asp?id=67264 (viewed June 16, 2006).

[71] *See*, e.g., Ephraim Schwartz, "RFID tags for chickens? Digital Angel says tracking temperature of poultry could be early warning system for avian flu," InfoWorld, December 5, 2005 (viewed at http://ww6.infoworld.com/products/print_friendly.jsp?link=/article/05/12/05/HNchickenflu_1.html October 11, 2006).

[72] Digital Angel Corporation is majority-owned by Applied Digital Inc., which is also the parent company of VeriChip Corporation. Another of its subsidiaries, Signature Industries, is a leading developer and manufacturer of search-and-rescue GPS beacon equipment (trade name SARBE), used by different countries' militaries.

[73] *See* http://www.digitalangelcorp.com/about_pressreleases.asp?RELEASE_ID=217 for the Digital Angel Corporation's Press Release of April 25, 2006 announcing an agreement with the Brazilian government.

[74] Pacific Health Summit's Health and Information Technology and Policy Briefing Book, Health Information Technology and Policy Workgroup, June 2006, page 6.

when the reader and RFID label are coupled. These smart labels are being marketed in the prescription drug context, with pharmacies attaching them to drug packages so that a patient can use a reader to hear what is printed there: for example, the patient's name; the type of drug; the recommended dosage; warnings; general instructions; the prescription number; and the doctor's contact information.[75]

These applications may give the impression that RFID technology is a niche market; however, the technology has already become quite prevalent. As of early 2006, several hundred million RFID tags had already been used in food packaging, and more than 70 million tags had reportedly been applied to livestock.[76] Recent bulk pricings of passive RFID tags have been at US$.07. Meanwhile, some companies are developing new forms that can be printed directly into paper, antennae and all.[77] With extensive RFID uses already underway in objects, animals, and humans, one expert has predicted that by 2010, more than 500 billion RFID tags will be put in circulation annually.[78]

How RFID Works

An RFID system usually has a small "tag" that has been assigned a unique electronic number and sometimes can store additional information. The tag is equipped with a transponder as well as a digital memory chip. The tag works in conjunction with a separate "interrogator" antenna or reader that has a transceiver and decoder; the reader emits a signal, and this signal activates the RFID tag so that it can send that device data that is encoded in the tag's integrated circuit (silicon chip). As opposed to barcodes that

[75] *See* http://www.envisionamerica.com/scriptalk.htm (viewed October 3, 2006).

[76] "Food and Livestock RFID - Where, Why, What Next?" IDTechEx, February 10, 2006 (viewed October 11, 2006 at http://www.idtechex.com/products/en/articles/00000434.asp).

[77] Companies such as PolyIC and Philips are developing tags made with polymer semiconductors, which, if commercialized, are expected to be printable and much cheaper than tags made with silicon. *See* "Philips Demos Polymer HF Tags," Mary Catherine O'Connor, RFID Journal, February 7, 2006, available at http://www.rfidjournal.com/article/articleprint/2139/-1/1 (viewed October 11, 2006).

[78] Loring Wirbel, "RFID tags ubiquitous by 2010, MIT prof predicts," My-ESM, September 15, 2004. There had been concerns that licensing and intellectual property disputes could slow deployment of RFID technology. A company called Intermec holds various patents on RFID, while the industry association EPCglobal has developed the "UHF Class 1 Generation 2" standard (Gen 2). It has been decided that Gen 2 does not infringe on Intermec patents, but royalties may need to be paid to Intermec depending how the tag is read. *See* Mark Roberti, "EPCglobal Ratifies Gen 2 Standard," RFID Journal, December 16, 2004, available at http://www.rfidjournal.com/article/articleview/1293/1/1/ (viewed October 11, 2006).

are commonly used on products today, RFID tags do not require that the reader be in direct "line of sight." As suggested above, the tag can be applied as a label, or it can be embedded.[79]

RFID tags fall into three categories: passive, semi-passive, or active. Passive tags contain no internal power supply; the minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the integrated circuit in the tag to power up and transmit a response. In other words, the antenna both gathers power from the incoming signal and transmits its own signal back. Passive RFID tags can be so small as to be almost invisible. For example, as of the spring of 2006, the smallest devices along this line measured 0.15 mm × 0.15 mm (without antennae) and were thinner than a sheet of paper; despite their lack of internal power, they can nevertheless still be read by a reader a few meters away.

A semi-passive tag, on the other hand, does contain a small battery, obviating the need for the antenna to collect power from the incoming signal.[80] A semi-passive tag activates only when it detects a signal from an interrogator.

Active RFID tags serve as beacons. With their own power supply, they have a longer range (up to tens of meters) and larger memories than passive tags, plus they can store additional information sent by the transceiver. At present, the smallest active tags have a battery life of up to 10 years, cost a few dollars, and are approximately the size of a small coin.[81] (Of course, in 10 years the size of today's tag and antenna will likely seem monstrous.)

Ramifications and Concerns

While RFIDs themselves may be neutral, their wide-scale rollout is sure to have broad infoethics consequences. Similar to digital identity management and biometrics, RFID technology presents particularly pressing issues for privacy.

These issues emerge even if the technology is deployed only in connection with consumer goods. For example, if the bulk of a person's purchases have RFIDs attached to them, and if the person's identity is ascertainable (e.g., through his use of a credit card to buy the items), the information can be linked. Vast amounts of data accumulate over

[79] *See* generally http://www.glandi.com/epackaging.htm.

[80] *Id.*

[81] *Id.*

time, allowing a detailed profile of that person's spending patterns. Add this compilation to the data on where a person travels in his RFID-tagged car, and the profile becomes highly sophisticated.

Katherine Albrecht, director of the consumer privacy group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), warns that RFID tags on consumer products could emit data even after purchase, allowing each tag to act as a potential beacon for trackers.[82]

As noted above, there are already direct associations of RFID tags with specific human beings. A current concern with RFIDs in the employment context is whether companies appropriately inform their staff of how data from RFIDs in chip-embedded badges is collected, used, and retained. While companies usually say they require these tags for the purpose of controlling access to buildings, a recent study by the RAND Corporation suggests that U.S. companies are in fact using RFID data for additional purposes. For example, RFID data is used to account for employee whereabouts during evacuations, to investigate thefts, and to enforce employee-conduct rules (such as break times).[83]

Of the companies studied, not a single one had informed its employees about these additional applications, leaving them to assume the RFID chips were used solely for controlling locks. Generally speaking, explicit written policies did not exist, and none of the companies had a limited data retention policy; rather, they all held the records indefinitely. Noting that fair information practices would give employees the right to inspect and correct records about their activities, the study insightfully cautions that, even if acknowledged, this right may lose its effectiveness because it would be difficult for an employee to reconstruct a given day's activities after time had elapsed. The study draws an important conclusion: As technologies collect and analyze data on individuals' behavior with increasing sophistication, elements of fair information practices may need to be rethought.[84]

Reflecting the European Union's greater attention to the protection of personal data, governments in EU

[82] Lecture by Katherine Albrecht at Harvard University, April 7, 2006. *See* http://www.nocards.org/.

[83] Edward Balkovich, Tora K. Bikson, and Gordon Bitko, "9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace," TR-197-RC, 2005, 36 pp. The study compares and contrasts practices of six private-sector companies with over 1,500 employees.

[84] *Id.*

member states have given companies more guidance on RFID usage. In the United Kingdom, for example, the Information Commissioner's Office has published best practices in its Employment Practices Code, calling on companies to avoid "oppressive or demeaning" forms of employee monitoring. Similarly, France's Commission nationale de l'informatique et des libertés (CNIL) has advised companies to brief employees fully on any use made of data from RFID-enabled identification badges. This body also recommends that individual workers be allowed to access their data records.[85]

Employers argue that security and public safety justify the use of RFID tags. However, in addition to sacrificing employees' privacy and personal autonomy, the tags could enable employers to intimidate employees and keep them from exercising their legal rights – for example the right to collective action in trade unions. Surfacing these tensions, the British general union GMB argued in 2006 that the practice of some retail distribution centers of requiring employees to wear RFID tags was dehumanizing. Reacting against the surveillance of employees as they take breaks, Union Network International, an international federation of service sector unions based in Geneva, Switzerland, has organized a campaign to contest this use of RFIDs.[86]

As for RFID use to prevent the spread of disease, it is imaginable that the type of system used in Singapore during the 2003 SARS crisis could be deployed on a wide scale in the event of a human pandemic (such as an outbreak triggered by a mutation in avian flu). To monitor possible contamination, authorities could use RFID chips in identification cards, in combination with RFID readers located at the entrances to buildings.[87] Even if such measures were embraced for public health advantages, protections for people's privacy and freedom of association would beg for serious attention given the enormous surveillance potential brought on by this technology.

RFID identifiers for people could be required by law; they could also, however, become a practical necessity for a person to participate in society even if they were not officially required – similar to the way that it has become difficult for adults in industrialized societies to make many types of purchases without a credit card. If the market required

[85] Andrew Bibby, "Invasion of the Privacy Snatchers," Financial Times, January 8, 2006.

[86] *Id.*

[87] For a brief account of new building-code plans in the United States, *see* the case study on the Geospatial Web and Location-Based Services, below.

a person to have an RFID identifier to participate in commerce but this condition were not mandated by government, it would be difficult for a person to claim that the state was infringing on his rights by requiring him to participate in such a system – unless the person argued that the government, in allowing the market to establish such a requirement, had abdicated its responsibility to protect his autonomy.

It is imaginable such a de facto or de jure requirement could extend to human implants, and it is unclear whether people would have the right to refuse such measures.[88] For example, in the same way that bio-thermal RFID chips are used to identify cattle exposed to infectious diseases, these chips could be used in humans to quarantine people so as to limit the spread of pathogens. While some people might object to subjecting their bodies to such treatment (e.g., on account of religious beliefs), individuals' convictions may be required to give way to the health interests of the greater public.

Some commentators point to the national security interests in supporting infrastructure for RFID. As Désirée Milošević puts it, governments are starting to view this technology as a geo-political necessity, igniting a sort of "surveillance race".

For now, however, there are very immediate concerns regarding vulnerabilities in RFID chips. A recent study on deployment in credit cards has shown that cardholder information can be gleaned by small, homemade readers assembled from computer and radio components that are easy to obtain. Because such devices can read chips even through a wallet or clothing, the concern is that someone could skim people's information simply by passing through a crowded area with a reader. Although the major credit-card issuers contest that most RFID-enabled cards have strong encryption, all the cards examined in the study had been issued recently, yet none was found to be secure.[89]

[88] The U.S. state of Wisconsin in the spring of 2006 was among the first states in the United States to pass legislation making it illegal to require an individual to have a microchip implant. "Wisconsin Bans Forced Human Chipping," Free Market News Network, June 1, 2006. Many other states have since followed suit.

[89] Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu1, Ari Juels, and Tom O'Hare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards," University of Massachusetts in collaboration with RSA Labs, October 2006. The paper is the first published under a new consortium involving industry and academic researchers to study RFID. Research is financed by the National Science Foundation in the United States. The paper is available at http://prisms.cs.umass.edu/%7Ekevinfu/papers/RFID-CC-manuscript.pdf (viewed October 23, 2006).

Similarly, RFIDs used in human implants have also been criticized as insecure. In July 2006 hackers demonstrated that they could "clone" a VeriChip implant and attribute that same identifying information to a different device.[90]

These concerns aside, broad-scale RFID deployment could support numerous infoethics goals. By revolutionizing the supply chain and bringing great economic efficiencies that raise the standard of living, RFID technology arguably contributes to the exercise of life, liberty and security. RFID-based identification systems, if secure, reduce the need for other methods of security, increasing access to transportation and public resources. Implanted RFID tags enable better medical treatment by ensuring immediate access to accurate health records. The list of benefits is long.

While there are clear infoethics tradeoffs with this technology, there is nonetheless marked demand for it on the part of wholesalers and retailers who can gauge inventories quickly, and there will also be demand eventually by everyday buyers who will be able to avoid check-out lines by passing through a scanner. Governments are adding their own mandates and incentives for use of the technology in public services. With serious pressures driving companies and local governments to adopt the technology, and little incentive for them not to do so, it appears that RFID has an almost guaranteed place in the Information Society in the near term.

Thus, in some ways, RFID represents a microcosm of the possibilities and threats of ICTs. If carefully deployed and regulated, RFIDs present an opportunity dramatically to improve many facets of life; if used without adequate safeguards for security, privacy and other liberties, they threaten to bring nightmarish consequences.

Sensors

What Sensors Are

A sensor is a device that detects the presence of a biological or chemical entity or a physical stimulus and pro-

[90] The hackers, Annalee Newitz and Jonathan Westhues, demonstrated these vulnerabilities at the HOPE Number Six conference in New York City; the VeriChip Corporation said it needed to review the evidence but noted that hacking into an RFID chip is difficult. *See* Donald Melanson, "VeriChip's human-implatable RFID chips clonable, sez hackers," posted to Engadget on July 24, 2006 (available at http://www.engadget.com/2006/07/24/verichips-human-implatable-rfid-chips-clonable-sez-hackers/, viewed October 24, 2006).

duces a signal to give a measurement of that quality.

Sensors are most commonly categorized based on the type of phenomenon that they measure – for example, acceleration, acoustics, displacement, flow, gas, humidity, inclination, magnetism, light, oxygen, position, pH, pressure, proximity, rotation, and temperature.[91]

How Sensors Work

Sensors have two basic parts – a sensing element and a transducer. Simply stated, the sensing part interacts with the surroundings and generates a response. The transducer then converts that response into a quantifiable term that can be interpreted.[92]

Sensors can be deployed remotely, allowing information about the environment at a specific location to be determined by a sensor located at a distance from that location (e.g., from an aircraft, spacecraft, satellite, or ship).[93] Remote sensing generally relies on radiation to measure the environment. Such sensors may measure a fairly broad range of phenomena, including heat, light (visual imaging) and sound.

Sensors may also be placed "*in situ*," or on site, in areas where measurements are desired. Although many such sensors provide measurements only to persons present at the site, a sensor can also relay information through an information network. In such an arrangement an individual sensor is sometimes referred to as a "pod," with each pod having certain components, including:

1. A *sensor suite* that contains the sensing element and transducer;
2. A *microcontroller* that contains the system's protocols/communication standards, that communicates with the attached sensor suite, and that performs data analysis as needed;
3. A *radio* linking the pod to its local neighborhood or network;
4. A *power system* that today often comes in the form of a battery pack with solar panels, with a current life span of several years; and
5. *Packaging* that usually must be lightweight, durable, cheap, easily mountable, and sealed

[91] Web Sensor Portal, http://www.sensorsportal.com/HTML/Sensor.htm, viewed November 7, 2006.

[92] Sensor Technology Exchange, http://www.sentix.org/info.htm, viewed November 7, 2006.

[93] *See* http://en.wikipedia.org/wiki/Remote_sensor (viewed November 7, 2006).

against weather, elements, and animals.[94]

Increasingly, these sensors are being produced as microelectromechanical systems, or MEMS. MEMS sensors are able to amplify the output signal generated by the sensor, to adjust the sensor reading for conditions such as temperature, and to perform some calculations based on the sensor readings. (So, for example, such a sensor might monitor a perishable product through a supply chain to ensure appropriate temperature.)

A recent article addresses ways to reduce the size of wireless MEMS to the micrometer level – approximately the size of a grain of sand.[95] (These devices are sometimes referred to as "motes" or "smartdust".) The U.S. Department of Defense is reportedly funding research and development along this line.

At the opposite extreme, large satellites in space are using sensors to provide web content through the form of images, which can then be combined with other web services like driving directions to allow new, useful creations in the form of "mash ups".[96]

Ramifications and Concerns

While sensors themselves may be neutral, the service supplied and the data gathered may give rise to concern. For example, the same type of sensors used to monitor a forest fire could be employed surreptitiously on the opposite side of a wall to surmise a person's activities based on body heat.[97]

Even data obtained for ostensibly benevolent purposes may prove harmful if used in a way that violates human rights. This would be the case, say, if sensors were used to detect the presence of infectious diseases, but the data were then used to establish a quarantine area that discriminated against a segment of the population.

So, too, the data collection and its general purpose may be acceptable

[94] Kevin A. Delin, Shannon P. Jackson, David W. Johnson, Scott C. Burleigh, Richard R. Woodrow, J. Michael McAuley, James M. Dohm, Felipe Ip, Ty P.A. Ferré, Dale F. Rucker, and Victor R. Baker, "Environmental Studies with the Sensor Web: Principles and Practice," Sensors 2005, Volume 5, 103-117, p. 106.

[95] Michael J. Sailor and Jamie R. Link, "Smart dust: nanostructured devices in a grain of sand," *Chemical Communications*, vol. 11, p. 1375, 2005.

[96] *See infra* case study on Location-Based Services.

[97] The Supreme Court of the United States has barred law enforcement officials from using this form of technology, *see Kyllo v. United States*, 533 U.S. 27 (2001), but there is no general bar to its use by other parties.

to the public, but downstream uses to which the data is put may cause alarm. For instance, satellite images made available online by companies like Google have caused consternation among governments – not because of what Google itself is doing or what the images represent, but rather because of the danger posed by the accessibility of sensitive information to potential enemies.[98]

To get a handle on these tensions so that they may be considered more generally, it is useful to consider sensors in the light of infoethics goals. Sensors may be viewed as contributing to the human right to life, liberty and security. For example, many sensors serve as life-saving devices, such as those used to detect the presence of harmful chemicals in water or to track the progress of a major storm. In anticipation of the spread of the avian flu virus, STMicroelectronics, Europe's second-largest chipmaker, and Veredus Laboratories of Singapore have been developing a laboratory chip that can analyze a minute blood sample to diagnose the virus in one hour. Instead of sending samples to labs for a several-day examination, the chip will allow quick displays on laptops deployed in the field. Each disposable chip will cost in the "tens of dollars", according to a Financial Times article.[99]

Sensors also help to optimize the production and distribution of food, energy, and other essential components of life in industrialized societies. As such, they may be viewed as contributing to a higher standard of living and thus to life, liberty and security.

In terms of human rights, one of the most glaring issues is that of privacy. Simply put, information that a person has traditionally assumed to be in his private domain may now be observable by sensors, with him possibly having no idea of the sensors' existence or presence. Data gathered about him may be personally identifiable, but it is unlikely that he has effective notice or choice about this collection, or that he himself has access to it or a can be assured as to its security.

Of course, sensors can also help enforce privacy, for example by detecting intrusions.

If sensor data is used in a court proceeding, a person may be at a significant disadvantage in trying to disprove its reliability as evidence.

[98] See, e.g., Katie Hafner and Saritha Rai, "Governments Tremble at Google's Bird's-Eye View," New York Times, December 20, 2005.

[99] Maija Palmer, "STMicro, Veredus plan quick-test bird-flu chip," *Financial Times*, January 19, 2006.

Does this weaken the right of a person to be presumed innocent until proved guilty?

Sensors also pose infoethics questions relating to the public domain and access to information. There are ambiguities regarding how the benefits of sensor data will be shared – specifically, whether exclusive rights to sensor data about public spaces exist, or whether all such data is part of the public domain and available to everyone.

A standard interface for sensor data would promote the accessibility of data. Information might be accessed either from a central repository storing the data or directly from the sensor itself if the sensor were connected to an information network. As noted by David Clark,[100] a leading architect of the Internet since the mid-1970s, "The interesting policy question is: 'Will there be an open infrastructure for sensors?'."[101]

While law is often viewed as the way to address such questions, scientists tend to be wary of regulation because it quickly can become outdated and constrain technological advances. By way of example, environmental monitoring is generally considered necessary to protect the public from toxic contaminants and pathogens that might be released into the air, soil, or water of an area. Sensor technology enables cheap monitoring, avoiding the high costs of sending a team out to collect samples, and preventing additional expenses that might accrue if samples are compromised during transport, storage, and off-site analysis. Nonetheless, many regulations still require manual collection of samples for off-site analysis.[102] Hence, the regulation of sensors, or any other form of technology, requires legislation and administrative procedures that are flexible enough to evolve along with the technology that they propose to regulate.

Despite the difficulties, policymakers and technologists must confront the problems that sensor technology is likely to present and take steps now to create a climate that is conducive to ethical uses.

[100] Clark served as the Internet's Chief Protocol Architect from 1981-1989; he currently chairs the Computer Sciences and Telecommunications Board of the (U.S.) National Research Council and is a Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory.

[101] Interview with David Clark at MIT, November 11, 2005.

[102] For the foreseeable future, the environmental field instrument market is expected to grow by an average of 7% annually – a figure that would be much higher if law and culture were faster to embrace technological change. Clifford K. Ho, Alex Robinson, David R. Miller and Mary J. Davis, "Overview of Sensors and Needs for Environmental Monitoring," *Sensors,* 2005, Volume 5, 4-37, p. 5 and 7.

The Geospatial Web and Location-Based Services

What the Geospatial Web Is

Whereas sensors measure the real world and turn it into data that can be read by machines, the geospatial web inverts this process, taking digital data and applying it to locations in the real world. By merging data from various sources, geospatial web applications can, for instance, show a map of the various restaurants in a given city, complete with contact information and reviews.

What Location-Based Services Are

A location-based service (LBS) takes this concept one step further. Rather than providing information about a requested geographic location, a LBS automatically determines the user's location and provides information based on those bearings. To extend the application above, a LBS user can be informed of all restaurants within a given distance of his present location, as well as directions to those restaurants from the user's current location.[103]

More significantly, LBS can automatically track the location of a person and provide this information to others. This tracking allows such services as Dodgeball.com, which alerts people when friends or acquaintances are nearby. It can also permit emergency assistance to be summoned to the location of a car accident without any action by the driver whatsoever. Some parents are providing LBS cell phones to their children so that the children's whereabouts can be tracked. Applications are only just beginning to be conceived.

How the Geospatial Web and Location-Based Services Work

The concept behind the geospatial web is quite simple: Just indicate the geographical location that corresponds to a given piece of (virtual) data, and then provide a mechanism for combining real-world maps and that data. To show a map of restaurants in a city, for instance, the

[103] The OnStar system, for instance, provides directions to drivers by determining the location of the vehicle and combining that information with street maps and the driver's destination – the driver need not know his own location to take advantage of the service. *See* http://www.onstar.com/us_english/jsp/index.jsp (visited March 15, 2006).

geospatial web need only collect the addresses of various restaurants and combine those with a mapping programme that places each onto a street map or some other representation of the geographic area.

LBS works by ascertaining the location of a specific person or device. At the simplest level, the person merely reports his location to the service. Alternatively, a person's location can also be calculated automatically. In the case of a mobile phone, for instance, a person's location may be determined by detecting the closest cellular towers to the phone and "triangulating" the phone's location based on its distance from each of these towers. The accuracy, and even availability, of this method of determining a user's location may vary with the density of cellular towers in the area. A satellite-based positioning system such as Global Positioning System (GPS)[104] can provide an alternative method of determining the location of a user without the constraint of nearby cellular towers. (Indeed, many, if not most, new cell phones include GPS receivers.) Another recent phenomenon is the linking of mobile phones to nearby Wi-Fi hubs, giving a reading that can indicate, e.g., where a person is in a building.

Plans are in the midst for building codes to require the use of RFIDs and sensors for LBS. As described on the web site of the U.S. National Institute of Standards and Technology (NIST):

> The RFID-Assisted Localization and Communication for First Responders project will determine the feasibility of using RFID-assisted localization in combination with an ad-hoc wireless communication network to provide reliable tracking of first responders in stressed indoor RF environments, where GPS-based localization and links to external communication systems are known to be unreliable. The research will also consider the means and potential for embedding critical building/occupant information in specific on-site RFID tags to enhance the safety and efficiency of the first responders' mission as well as

[104] According to the Wikipedia entry for GPS viewed March 15, 2006, "United States Department of Defense developed the system … and the satellite constellation is managed by the 50th Space Wing at Schriever Air Force Base… GPS is available for free use in civilian applications as a public good." Meanwhile, "Russia operates an independent system called GLONASS (global navigation system), although with only twelve active satellites as of 2004, the system is of limited usefulness. There are plans to restore GLONASS to full operation by 2008. The European Union is developing Galileo as an alternative to GPS, planned to be in operation by 2010. China and France are also developing other satellite navigation systems." http://en.wikipedia.org/wiki/GPS.

> to minimize dependence upon communication with external building databases.[105]

The project description in the study notes the connection among technologies: "The system… is intended to leverage advances in ubiquitous RFID tag technology, in combination with recent advances in miniaturized inertial sensors, to develop a low-cost tracking system…"[106]

Other LBS uses may be found in RFID chips for human implantation. While the VeriChip CEO stresses that the chips he is advocating for immigration purposes will be passive, the company web site indicates that they also have human-implantable chips that can serve as beacons.[107]

Ramifications and Concerns

In associating information with a specific geographic location, these technologies can enable a person to exercise various rights. For example, they allow a person readily to identify and locate persons in his social network and provide opportunities for increased social interaction.[108] In so doing, they can be viewed as helping a person to exercise his right to associate. This right can serve to support democracy and freedom generally as citizens can assemble to petition for a government to honor their rights.

The geospatial web and LBS can also be viewed as helping to protect the health and safety of individuals since the availability of emergency services in many cases depends on the ability to determine a person's location. In this sense, the technology allows people to enjoy more fully the right to life, liberty and security of person.

Of course, there are potential downsides to the use of the technology. From a privacy perspective, people may be concerned that their locations are being observed. In the case of a repressed minority, the tracking of location could result in discrimination as the knowledge could lead to people's harassment. And just as location-aware services could help a group gather, they could also be used to impede association or assembly, depending on who had access to the data and what kind of forces they

[105] National Institute for Standards and Technology (NIST), Advanced Network Technologies Division, http://www.antd.nist.gov/wctg/RFID/RFIDassist.htm, updated on 03/03/06 and viewed on 14 March 2006.

[106] Leonard Miller, "Indoor Navigation for First Responders: A Feasibility Study," National Institute for Standards and Technology, February 10, 2006, p. 7.

[107] *See* VeriChip web site at http://www.verichipcorp.com/ (viewed June 22, 2006).

[108] *See, e.g.*, www.Dodgeball.com (a social networking LBS where users send a text message on a cell phone to indicate their current location).

could exert to stop a gathering. Even the threat of location surveillance could have a chilling effect and stop people from assembling.

These tensions point to one overriding concern: Who should have knowledge of a person's whereabouts? As currently designed, LBS allows the service provider to ascertain the location of a person and to share that information; it does not follow, however, that the service provider should have the capability or permission to determine a person's location at any given time, or to use or share that data as it sees fit.

Similar to protections in digital identity management, one approach to this potential privacy hazard could be to utilize trusted intermediaries that would provide the minimum necessary information about a person's location, in a way that would not be linkable to other information. So, for example, software might prompt an individual to choose when and to whom his location is revealed. Still, a person might not have the ability to choose when a LBS combines with sensors and biometrics (e.g., facial recognition technology) to identify people's whereabouts. Again, machines may need to be programmed to treat personal data with extra care.

As with other emerging technologies, choices in law and computer code will determine who has ownership and control over this information. Legal and technological safeguards should therefore be put in place to ensure that location information associated with a person is used in a manner that a polity (including its minorities) deems acceptable. Such a combined solution would help the Information Society to reap the benefits of these tools without incurring heavy infoethics costs.

Mesh Networking

In addition to the content that is already on the Internet, there will be a vast amount of data generated by RFID, sensors, and LBS, especially once standards enable interoperability. This great quantity will require a more extensive communication network to tie the technologies together. Mesh networking appears to be an ideal tool to begin to create this network.

What Mesh Networking Is

In mesh networking, network-enabled devices (e.g., computers or mobile phones) establish a peer-to-peer communication network spontaneously. This connectivity is touted as self-configuring, self-healing, scalable, strong, and inexpensive.[109]

How Mesh Networking Works

Mesh networking works by devices' sensing each other's presence and negotiating with each other to set up a network for transmitting communication. Instead of passing through centrally-controlled hubs, data exchanged via mesh networks travel in an ad hoc, "multi-hop" path, with each point or "node" along the way functioning as a router to relay messages to other nearby nodes. A participating node can be fixed or mobile, wired or wireless.

The primary advantage of a mesh network is its ad hoc nature: a mesh network can form between nodes with no underlying infrastructure, relying solely on the ability of individual nodes to connect to each other. So, for example, a mesh network would allow a rescue team on the scene of a toxic spill to form their own network to share information.

Similarly, a mesh network using radio or other wireless communication technology could be deployed in terrain where a wired infrastructure does not exist, due to terrain or other constraints. If the network needed Internet connectivity, this link could be achieved through just one node with a connection – although the greater the number of nodes with a connection, the greater the reliability and speed of transmission. Mesh networking could thus allow poor regions to share a limited number of Internet connections. To extend to remote areas, the network merely needs to add nodes.[110]

Mesh networks boast many possible communication routes for data to travel along, and this redundancy makes the network resilient in case any node fails.[111] Whereas in business the idea of redundancy often connotes inefficiency, in mesh networking the contrary is true for three main reasons: (1) the nodes themselves can be cheap, (2) installation

[109] *See* Mesh Networking (Wikipedia entry), http://en.wikipedia.org/wiki/Mesh_network (visited March 11, 2006).

[110] In a traditional wireless mesh network, all devices operate on the same communication channel; in a large network, this can lead to congestion and reduced bandwidth. This limitation can be alleviated by using multiple channels to prevent interference. *See* Richard Draves et al., *Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks* (2004), *available at* http://research.microsoft.com/mesh/papers/multiradio.pdf.

[111] This method is similar to that of the Internet and other networks using peer-to-peer routing.

is easy (a new node is automatically detected and incorporated by the network), and (3) a dense network of wireless nodes allows for lower-powered communication.[112]

Mesh networking has other applications as well. Sensors can utilize a low-power mesh network to send messages directly to other devices in the network, and could for example trigger a specific response if a chemical spill was detected. Since mesh networks rely on distributed control, and messages need not pass through a center; the implication is that systems can become self-directing.

Ramifications and Concerns

Mesh networking is a relatively young technology, and there is a need for standardization: At present there are over 70 competing schemes for how the networks form and how the devices communicate with each other. The IEEE professional association is pursuing standardization, a sign that this challenge may be addressed in the near future. As with other technologies, mesh network standards should be set in an open manner that best serves the interests of all, without allowing powerful entities to drive standards in a way that leads to abusive market dominance.

Mesh networking has the potential substantially to disrupt the ability to control content. In a more traditional Internet topology, almost all content is relayed through ISPs, which then have the capacity to filter that content – whether in service to government (as by preventing access to illegal content), or for their own interest (as by limiting the bandwidth available to content provided by a competitor). A mesh network, by contrast, allows the creation of a great pool of users who connect to each other in an ad hoc fashion, without necessarily using an ISP or any other central hub. The technology thus can enable users to exchange information freely, thereby furthering freedom of expression.

At the same time, by reducing the need for ISPs in local connectivity, mesh networking has the potential to concentrate power in those ISPs that serve the relatively few nodes that connect to the Internet backbone. These ISPs may be increasingly able to filter content and leverage the situation to promote their own interests. Furthermore, any disruption to the shared Internet connection can have consequences for the entire group of users relying on the mesh

[112] The strength of an electromagnetic signal is inversely proportional to the square of the distance from the source of the signal. It thus requires less power to relay a signal across multiple short distances than to broadcast the signal directly across a greater distance.

network. Given these considerations, mesh networks may need to retain multiple points of connection to the Internet backbone, preferably operated by separate entities to avoid monopolistic behavior.

David Clark notes: "Mesh networking raises issues about policy for spectrum allocation, industry structure, and so forth. There is sort of a classic struggle going on, with incumbents using regulation to slow down change."[113]

Beyond competition, there are security risks implicit in mesh networks. Without checkpoints through which all data must flow, harmful viruses or worms could spread throughout a mesh community. Such hazards may reinforce demand for digital identity management and other security-related technologies, in turn magnifying the infoethics impact of those technologies.

The Tools Make the Rules

An interview with Dewayne Hendricks[114]

Key to the Internet's integration into our lives is its spread throughout our built environments. Where the Internet cannot be found, modern life will not exist; here, the physical layer of Internet governance becomes particularly important. While to date the Internet has reached most users by wires – copper, coaxial, and now fiber – many of its applications will soon derive their value from untethered links to the network. The Internet is becoming a pervasive part of modern life, and wireless access to the Internet will soon become as ubiquitous as air itself.

In one sense, these wireless connections are simpler to deploy than their wired counterparts because they require less physical infrastructure: There are fewer wires to lay and fewer landowners to appease. But while a wire in the ground is virtually the same everywhere, the wireless spectrum is not. In nations such as the United States, spectrum has been carefully divided and mostly regulated. In places like China, the opposite is true. Other countries' policies lie somewhere in between.[115]

[113] Interview with David Clark at MIT, November 11, 2005.

[114] "Serial entrepreneur" Dewayne Hendricks is CEO of the Dandin Group.

[115] See "Focus on Wireless: Special Study on Wireless Spectrum" at http://www.netdialogue.org/casestudy/ -- created in conjunction with the research arm of the Microsoft Corporation. This case study examines the 5 GHz spectrum and its potential for international use. Within these web pages, Net Dialogue presents information on 5 GHz's worldwide availability, its prospects for regulation, and the standards that may someday make use of it.

According to spectrum expert Dewayne Hendricks, “Carving out the radio spectrum into a series of walled preserves is an artifact of the past. By licensing spectrum, policymakers have fostered the notion that the spectrum is a scarce resource where access to it has to be strictly managed or ordered. Changes in technology which started in the early 1950s have shown us that this perspective is inaccurate.”

Dewayne notes that, with the advent of devices such as software and cognitive radios, and concepts like spectrum underlay (a.k.a. overlay), “the Information Society can start to treat the spectrum as a dynamically allocable resource, where access is dictated by the needs and requirements of the devices making use of it at any given time.”

The amateur radio spectrum and its use for almost one hundred years is the best example of this phenomenon, he says. Amateur radio has operated under a spectrum “commons” model for all these years with no major adverse effects, and it has fostered an environment where innovation has flourished; drawing a parallel, Dewayne asserts: “The more recent creation of the unlicensed bands have shown to all what results when society makes a spectrum commons accessible to countless devices.”

When asked about the future, Dewayne replies: “It is hard to predict where a spectrum commons will take us. Just three years ago, if one had predicted that the major industrialized cities of the world would now be covered by Wi-Fi ‘clouds’, people would not have believed it.” Yet this is where these societies are today.

In conclusion, Dewayne reflects: “I believe that there is ample evidence out there now for policymakers all over the world to start to rethink their approaches to spectrum policy and give serious consideration to the concept of open spectrum.”

Grid Computing

Mesh and other networking technologies are paving the way for countless devices throughout the world to be connected to the Internet. Of course, many of these machines have very low storage capacity and computing power. For them to offer true participation in the Information Society, they need a way to access additional resources. Grid computing offers possibilities here.

[116] *See* http://creativecommons.org/licenses/by/2.0/.

What Grid Computing Is

Simply stated, "grid computing" is a technology that allows devices linked through a network to share computing power or data storage capacity, and so to appear to operate as a single, extra powerful computer. By combining resources, machines linked in a grid computing system can perform computations that would be impossible or too time consuming for a single computer to do. This computational cooperation thus allows regular users to perform large tasks, such as modeling the global financial system or predicting climate change. A machine linked in such a system can also access data that is too bulky for it to store on its own.

A grid computing system can be organized to function like a utility, whereby computing resources are available "on tap," similar to the way water and electricity are available in the developed world.[117]

Grid computing has existed as a notion for decades, with the first conceptions in the 1960s cast as "computer time sharing." However, it has only been in the last five years or so that advancements in computer processing, memory, and networking have culminated to allow an appreciation of the technology's benefits. With the spread of the Internet, broadband networks, and cheap, high-performance computers using open standards, grid computing has now enjoyed wider acceptance as a concept.[118]

Grid computing is being marketed to enterprises in the name of efficiency. For example, the Sun Microsystems web site touts grid computing benefits as including "cost reduction," "shorter time to market," "increased quality and innovation," and the "ability to do things previously not possible."[119]

Similarly, IBM says that grid computing brings business benefits by allowing a company to: "Accelerate time to results… Enable collaboration and promote operational flexibility… Efficiently scale to meet variable business demands… Increase productivity… Leverage existing capital investments…," with technology benefits heralded as "Infrastructure

[117] In 1965 developers of the Multics operating system (an ancestor of Linux) presented a vision of "computing as an utility". *See* http://gridcafe.web.cern.ch/gridcafe/Gridhistory/history.html, viewed on March 7, 2006. The term "grid computing" stems from a metaphor used in the early 1990s to connote computing power that is as easy to access as an electric power grid.

[118] Daniel Minoli, *A Networking Approach to Grid Computing*, Hoboken, NJ: John Wiley & Sons, Inc., 2005, p. 3.

[119] *See* http://www.sun.com/software/grid/, viewed March 5, 2006.

optimization… Increase[d] access to data and collaboration… Resilient, highly available infrastructure…"[120]

Meanwhile, Oracle advertises its services in the following way: "Grid computing enables you to create a single IT infrastructure that can be shared by all your business processes. Oracle 10*g* software is specifically designed for grid computing, delivering a higher quality of service to those business processes at a much lower cost."[121]

How Grid Computing Works

As explained on the GridCafé web site of the European Organization for Nuclear Research (CERN), a grid has five basic features:

1. **Global resource sharing;**
2. **Security;**
3. **Load balancing;**
4. **Distance neutrality; and**
5. **Open standards.**[122]

In terms of global resource sharing, computers in a grid computing network share computing and storage resources across geographically distributed organizations that have different administrative domains. Separate computers in a network indicate when they can offer spare computing power or storage space, and devices needing those resources can then draw upon it. When this process is initiated, computational needs of a given user are broken into discreet pieces and distributed to machines on the network. Each individual machine works on its piece and then sends back the result for recombination with the results obtained from other participants. As CERN elaborates, "This is more than simple file exchange: it is direct access to remote software, computers and data. It can even give you access and control of remote sensors, telescopes and other devices that do not belong to you."[123]

Security may be thought of as involving four interrelated aspects – that is, access, authorization, authentication and accounting. For access, participants specify which resources (software, computers, or data) may be used by whom and at what time, and what can be done with them. The authorization mechanism checks to see whether a requested job is in line with the sharing relationships that have been established. In the

[120] *See* http://www-1.ibm.com/grid/about_grid/benefits.shtml, viewed March 5, 2006.

[121] *See* http://www.oracle.com/technology/tech/grid/index.html, viewed January 27, 2006.

[122] *See* http://gridcafe.web.cern.ch/gridcafe/challenges/challenges.html, viewed March 5, 2006.

[123] *See* http://gridcafe.web.cern.ch/gridcafe/challenges/share.html, viewed March 5, 2006.

authentication process, the identity of a participant (resource provider or user) is verified. Finally, accounting involves billing for usage; this aspect will increasingly become a focus as grids move from the experimental phase in academic and scientific research centers and become more widely used by society generally.[124] As policymakers and technologists try to address these security concerns, approaches in digital identity management and computer certification may be looked to as solutions.

Load balancing refers to the need for a grid to allocate resources efficiently. Instead of humans trying to optimize resources, myriad "middleware" programmes enable machines to negotiate with each other – with some acting as agents (telling about users, data, and resources) and others as brokers (striking deals on access to and payment for these services) in the market of computing and storage resources. Metadata (data about data) allow this exchange by indicating "how, when and by whom a particular set of data was collected, how the data is formatted, and where in the world it is stored – sometimes at several locations…"[125] As such, there is a relation between the development of grid computing and semantic web and digital identity management technology.

Distance neutrality refers to the ability to share grid resources from diverse, remote locations in an optimally efficient manner and without delays in the processing of jobs.

Similar to the way the Internet is a network of networks, "the Grid" as envisioned will be one large Grid comprised of overlapping grid networks – with a need for common standards to allow applications to run across them. To answer this need, hundreds of players around the world (companies, academic institutions, other research institutions, etc.) have been cooperating in developing standards. Perhaps the biggest boon to this standard making came with their merging of regional grid advocacy organizations into the Global Grid Forum[126] in 2001. This group is now developing a standard called the Open Grid Services Architecture, which is expected to be key for enabling the Grid.[127] To complement this

[124] *See* http://gridcafe.web.cern.ch/gridcafe/challenges/access.html, viewed March 5, 2006.

[125] *See* http://gridcafe.web.cern.ch/gridcafe/gridatwork/middleware.html, viewed March 6, 2006.

[126] Global Grid Forum members as of 2005 are available at http://www.gridforum.org, viewed March 5, 2006.

[127] *See* http://www.gridforum.org/documents/GFD.30.pdf, viewed on March 7, 2006.

overarching architectural standard, the Globus Alliance has released an open source software package, the "Globus Toolkit",[128] to foster development of grids and applications that can run on them.

Notably absent in the basic features is a call for "net neutrality", which holds that there should be no discrimination among types of information flowing over the network. This principle has largely been held as a truth in the first few decades of the Internet, based on the idea that efficiency and innovation are best served by the network's doing nothing other than transmitting information. The idea has been to keep "intelligence at the ends" of the network, meaning where users connect, instead of having assessments made by the network itself in a way that may result in obstacles.[129] In recent years, however, companies have designed technology that can distinguish effectively among different types of traffic (e.g, voice, video, or simple textual data). Hence, those companies are advocating a departure from the net neutrality principle in the name of quality of service.

At the international level this quality of service argument has been advanced effectively in the International Telecommunication Union (ITU), which has launched the Next Generation Networks Global Standards Initiative (NGN-GSI) to implement such capabilities on a worldwide basis. Interestingly, the Global Grid Forum and the ITU's NGN-GSI group are collaborating to see how the technologies may complement each other.[130]

[128] The Globus Alliance has been working on fundamental grid technologies for the Globus Toolkit. The Globus Alliance was started in 1996 as the Globus Project, based at the University of Southern California and the University of Chicago in the USA. Now called the Globus Alliance, this group currently includes the Royal Institute of Technology in Sweden, the University of Edinburgh, the National Center for Supercomputing Applications in Illinois, USA, and Univa Corporation, based in Illinois, USA. Sponsors include a range of U.S. federal agencies (e.g., DARPA, DOE, NASA, and NSF), along with commercial partners such as IBM and Microsoft.

[129] *See* "End to End Arguments in System Design," J.H. Saltzer, D.P. Reed and D.D. Clark, MIT Laboratory for Computer Science, 1984 (available at http://www.reed.com/Papers/endtoend.pdf, viewed on June 22, 2006).

[130] For example, the ITU and the Global Grid Forum hosted a joint meeting in Geneva, Switzerland in October 2006. *See* http://www.itu.int/ITU-T/worksem/grid/index.html (as viewed on June 22, 2006).

Free Software: Access to Information and Knowledge

By Georg Greve[131]

Information and knowledge have always been at the heart of human evolution: They have shaped societies, helped build peace and were reason for war. Information and knowledge in the hand of a few can enslave entire peoples. Used wisely they can liberate them.

Information and communication technologies have fundamentally changed the rules for access to both information and knowledge. Digitalization has for the first time made it conceivable to transfer information in real time, without loss and at virtually no cost, across the planet.

Software is a cultural technique at the heart of this change, the medium that shapes this evolutionary step. Software codifies the rules along which information is exchanged and converted to knowledge. It controls who can do this and under which conditions: Access to and control over software determines, in part, today's knowledge and power structures. That is why software is such a controversial and central issue.

Software can be designed to give all power to change and enforce rules to a single person or group; this is the default approach in proprietary or non-free software.

But software can also be designed to give all users power over their own computers, and the right to determine how to interact with others in this new, virtual environment. For this right to be fully provided, software must give its users four fundamental freedoms: the freedom of unlimited use for any purpose; the freedom to study the software and learn how it works; the freedom to modify the software to adapt it to the needs of others; and the freedom to copy and distribute the software in original or modified form.

The rules of proprietary software make many dependant on the good will of a very few. The rules of Free Software provide an equal and independent playing field, which is why it is a natural choice for all activities that seek to promote Access to Information and Knowledge for everyone.[132]

[131] Georg Greve serves as President of the Free Software Foundation Europe.

[132] More information about Free Software can be found on the web pages of the Free Software Foundation Europe and the GNU Project: http://www.fsfeurope.org; http://www.gnu.org.

Ramifications and Concerns

Grid computing in time could reshape access to computing. Rather than requiring each individual to have a high-powered computer, grid computing encourages the use of low-cost "dumb terminals," each with only enough computing power to perform routine tasks and to coordinate communication with a central computing resource. These terminals are generally much cheaper than a standard computer, and they thereby suggest a way to provide computing access to the poorest regions of the world (particularly in combination with mesh networking).

This optimism presumes that users from poor regions will in fact be able to access the shared computing utility. If, however, grid computing is run as a commercial operation, ability to pay may exclude many areas of the world from sharing this resource; if it is not structured as a commercial enterprise, then some organization will have to agree to subsidize its existence.

While distribution of gains will need to be worked out, grid computing in theory promises outstanding efficiencies. Instead of having billions of devices that either have unused computing power or are constrained in this capacity, this technology allows resources to go where they are needed. Just as other technologies herald vast efficiencies, grid computing's economic gains could boost the standard of living and so buttress the right to life, liberty and security of person.

In practice, of course, there will be significant hurdles in terms of accounting and system security that will need to be overcome. Grid computing within a single organization is far easier than an open grid using the Internet.

A large-scale grid is not without its infoethics hazards. The security risks implicit in sharing computing power and data with others will make demand for digital identity management and other security-related technologies more pronounced, in turn heightening the ethical concerns associated with those technologies. Moreover, if grid authentication were centralized or concentrated, access chokepoints theoretically could discriminate among people wishing to participate in the network.

Similarly, a grid architecture by its nature demands distinctions based on content. The technology facilitating these distinctions as currently designed will allow "deep packet inspection" by governments or companies providing Internet services – meaning that these entities could monitor and possibly block the flow of specific information. The threat to freedom of expression is obviously profound here.

These negative prospects weigh against the benefits of efficiencies and access that will accompany the vast computing power, data accessibility, and data storage of grid computing.

As with other technologies, grid computing itself is neutral, and it can be harnessed for a variety of purposes. Decision-makers today must balance the infoethics tradeoffs and steer the Information Society toward sound grid computing choices.

Reading and Libraries: Two Notes[133]

David Weinberger[134], Joho the Blog, *March 6, 2006*

I can't wait until we're all reading on e-books. Because they'll be networked, reading will become social. Book clubs will be continuous, global, ubiquitous, and as diverse as the Web.

And just think of being an author who gets to see which sections readers are underlining and scribbling next to. Just think of being an author given permission to reply.

I can't wait.

~ ~ ~

As we put our works on line, we'll only need one library…

Why have more than one library when you can link to and aggregate whatever you need? Oh, the library will be distributed and portions will be replicated for safety's sake – we will have learned something from Alexandria – but that's just an implementation "detail."

When all our works are digitized, a local library will be nothing but a playlist.

~ ~ ~

[133] Available at http://www.hyperorg.com/blogger/mtarchive/reading_and_libraries_two_note.html#comments.

[134] David Weinberger is a Research Fellow at the Berkman Center for Internet and Society at Harvard Law School.

New Computing Technologies

Moore's Law holds that the computing power of a single chip doubles approximately every 18 months.[135] Each time we appear to reach a limitation that would end this exponential growth, a new technology arrives that permits computers to continue to increase in capacity as the prior technology approaches its limits.

There are several technologies that offer the potential of expanding computing capacity beyond the capabilities of today's integrated circuits.[136] This section touches on some of these technologies, and then addresses their common consequence: the continuing increase of computing power.

Nanotubes and Three-Dimensional Computing

Current integrated circuits are essentially two-dimensional; as chips become more complex, with multiple subcomponents, the constraint of operating in two dimensions with a fixed number of layers for interchip communication is a limitation on computing power.

By expanding computation into three dimensions, this limitation can be circumvented. Although it may be possible to achieve this augmentation with silicon-based transistors, other transistors may be better suited to a three-dimensional processor. Nanotubes – i.e. cylinders formed of a hexagonal network of carbon atoms – could be a more viable vehicle for three-dimensional computing. However, this technology is not currently available commercially, as manufacturing techniques to place nanotubes into a prearranged pattern do not yet exist.

Molecular and Biological Computing

Other new technologies seek to displace the transistor – the core of modern devices – with completely new computing elements. Molecular computers utilize individual molecules as computing devices, allowing data to be represented by a given configuration of a molecule, and computations to be performed by altering the molecule. Likewise, biological computers use living cells

[135] *See* Wikipedia, Moore's Law, http://en.wikipedia.org/wiki/Moore%27s_law (viewed February 26, 2006).

[136] *See generally* Ray Kurzweil, *The Singularity Is Near*, Ch. 3 (2005).

as computers, with the cell's own DNA determining the computation that it performs. Research is currently ongoing concerning both of these computing technologies.[137]

Optical and Quantum Computing

In a traditional computer, each element performs one computation on one piece of data at any given time. New technologies, however, can allow a single computing element to work on multiple data pieces at once.

Optical computing permits this parallel processing by encoding data in a stream of light. By use of a prism technique, these streams of light can pass through the same device at the same time without interfering with each other. A single optical computing element – which performs a calculation by altering a stream – can thus process several data elements at the same time.

Quantum computing uses the non-deterministic quantum nature of particles to represent every possible state of the particle, eventually generating a particle in a specific state that corresponds to the solution to the problem.

One limitation shared by both optical and quantum computing is the nature of the computations that they solve: Each is only efficient when performing the same calculation on a very large data set. Thus, these technologies are clearly applicable to certain problems – such as image processing calculations that require each portion of the image to be processed – but are more difficult to apply to calculations on a smaller scale. However, the advent of grid computing may offer additional opportunities to utilize massively parallel computing technologies such as these.

Ramifications and Concerns

Although most of the technologies discussed in this section are not likely to exist commercially for a few years, they suggest promising alternatives to the existing method of computation. Each presents its own technical challenges that must be overcome in order to make the technology viable; however, none of the challenges appear insurmountable, and it is all but certain that at least one of these technologies will serve to allow the continuing increase in computing power.

[137] *Id.*

These technologies, taken as a whole, suggest that the Information Society is nowhere near the limits of its capacity. Computers will almost certainly continue to grow smaller, more powerful and more networked in the future, and the Internet's explosion from curiosity 15 years ago to dominant paradigm today signifies only the very beginning of the Information Society.

Such computing power could go far in achieving infoethics goals. For example, high-powered computing could enable translations on a wide scale, helping to bridge people of different language groups and promote diversity. So, too, these resources could boost access to communication by providing computation muscle for computing grids – enabling people with cheap, low-powered devices to access information generated or stored elsewhere.

Cutting in the opposite direction is the potential increase in surveillance capabilities. While today such intelligence may seem far-fetched, this technology could have the muscle to make sense of enormous quantities of data gathered by search engines, ISPs, video cameras, financial intermediaries, and other data collection points. Here again, surveillance could put a severe dampener on the practice of human rights, particularly those instrumental in preventing the abuse of power since surveillance could be used to thwart privacy, assembly, and dissent.

These technologies could also disrupt geo-politics as entities enjoying early access to them would have a significant "first mover" advantage. As such, the technologies could be used to threaten the right to life, liberty, and security of person and other rights; of course, or they could also be used to usher in changes that improve the exercise of these rights.

To prepare for these seemingly overwhelming technologies, the Information Society must consider today's relatively small programmes that will pave the way for such power, and make every effort to ensure that machines are coded with a language of respect for human rights.

Table: Summary of Infoethics Concerns

Technology	Possible Positive Effects	Possible Negative Effects
Semantic web	• Expands access to information; • Could cause polarization and lack of public discourse, though this is debated. • Brings efficiencies (boosting the economy and with it the standard of living, which some people see as directly related to the right to life, liberty and security of person).	• Could make it easier to block people from receiving various content; • Could make it easier to prevent people from imparting content (e.g., thwarting certain content or competition supplied by new entrants); • Could put people on the same level as objects.
Digital identity management	• Could enhance privacy and security; • Could bolster freedom of assembly by helping people identify others with similar interests; • Could bring efficiencies and set web services free (boosting the economy and with it the standard of living, which some people see as directly related to the right to life, liberty and security of person).	• Could allow collusion and profiling by identity providers and relying parties; • Could easily be converted into a government-centric system; • Could enable discrimination; • Could cause humans to be at the mercy of machines tasked to act as agents; • Could intensify security risks of compromised computers.
Biometrics	• Could bring accountability, which some people see as tied to the right to life, liberty and security of person. • Could increase government's capacity to provide the public with governmental services (e.g., speedier passport checks at airports). Some people would view this as promoting the right to life, liberty and security of person.	• Could be coupled with digital identity management tools as a pre-requisite for participation in Information Society activities; • Could lead to international system of central administration, but international bodies are not equipped to prevent the abuse of power; • Could enable extensive surveillance, thereby hurting privacy, freedom of association and freedom of expression, among other freedoms.

Technology	Possible Positive Effects	Possible Negative Effects
RFID	• Could bring efficiencies in the supply chain (boosting the standard of living, which some people see as related life, liberty and security). • Could increase security by augmenting enforcement capabilities.	• Could impinge on freedom of religion if implants were necessary for participation in the Information Society. • Could enable extensive surveillance, impinging on privacy and other freedoms.
Sensors	• Could serve as life-saving devices (directly related to the right to life, liberty and security of person); • Could help optimize production and distribution (contributing to efficiency and thereby life, liberty and security of person).	• Could breed uncertainty regarding the public domain and access to information and the means of communication; • Could cause governments to have sovereignty and security concerns. • Could enable extensive surveillance, impinging on privacy and other freedoms.
Geospatial web and LBS	• Could be viewed as helping people to exercise their right to associate; • In extending the availability of emergency services, could enhance the right to life, liberty and security of person.	• Could hinder privacy through the tracking of location; • Could allow discrimination and the blocking of assembly and expression through the tracking of location.
Mesh networking	• Could disrupt content restrictions (e.g., filtering or bandwidth allocation); • Could help poor regions have access to means of communication.	• Could concentrate power in Internet-backbone connection points; • Could give rise to authentication that carries similar side effects as digital identity management tools (especially privacy).
Grid computing	• Could provide computing and data storage and retrieval for the poor. • By allowing resources to go where needed, would offer efficiencies.	• Could enable extensive surveillance, impinging on privacy and other freedoms; • Could allow discrimination and other restrictions given access chokepoints.
New computing technologies	• High-powered computing could allow translations and bridge people; • As computation behind computing grids, could boost access.	• Could enable extensive surveillance, impinging on privacy and other freedoms; • Could disrupt geo-political balance (e.g., by enabling decryption).

The Short Story Revisited

As noted, the **semantic web** will give computers metadata to help them sift through the enormous amounts of information that have been generated and made available via the Internet. At present humans are helping to develop this metadata, but as the Information Society moves into the future, machines will increasingly create the vocabulary for themselves. Metadata linguistically can equate a person with an object – for example placing a human and a piece of luggage in the genre of things to be tracked through airports – but it can also order the world so as to make its wonders accessible to people in a way they will enjoy – for example labeling photos for easy sharing among friends. Programming computers so that they will put data pertaining to humans on a higher plane than that of objects could prove important down the line.

Digital identity management offers a test case for this fleshing out of what it means to be a person. In the early stage of computers' linguistic development, it would seem essential to describe humans not just in the contextual terms of "frequent renter of cars," or "high insurance risk," but rather in terms that express what is sacrosanct, or not to be violated – such as the right to seek, receive and impart information. In this respect, digital identity management tools could be used to assert rights and seek automatic redress in case they are violated.

If machines are programmed to treat human data with an extra high degree of care, they will automatically process fingerprints, an iris pattern, or a walking gait differently than they would digitize, say, mud, a car engine, or a dog running. In this way, **biometrics** can serve to protect privacy and the right to associate freely rather than to act against these freedoms. The technology can be used for good, for example helping people recognize each other and enjoy access to a multitude of domains.

Similarly, **RFID**, **sensors**, the **geospatial web** and **location-based services** have potential to hem humans in as they make purchases, exhibit emotional reactions, and move about the physical world – with this data becoming as manageable and searchable as other digitized content, subject to possible collection, analysis, and use by unknown entities. It could prove difficult for a person to know what forces he is subject to, or to refute data when society gives it credence over a person's testimony. Looking at the technologies from another angle, there are beneficial uses – for example with RFID tags promising to bring down a company's costs of doing business, with sensors helping to ensure that a water treatment plant is safe, and LBS and the geospatial web bringing a lost child home. These technologies also promise to let new forms of content flower. To ensure the Information Society takes the right direction with respect to these technologies, the key will again be in designating how different types of data should be treated, with the end goal being to promote the exercise of freedoms.

With **mesh networking**, these same possibilities reach the developing world, where new connectivity promises to end the marginalization of economies and the people living in them. While incumbent companies may fear competition and others may deem uncontrolled communication a threat, the sharing of information through these networks can help democratize the Information Society. So, too, this kind of connectivity can open the gateway for diversity of content on information networks, facilitating communities based on shared culture and enabling people of different cultures to understand each other better. In this way, mesh networking technology has potential to maximize the benefits of educational, informational and cultural content by expanding access to information. Indeed, technologies such as mesh networking can extend the reach of the Internet and make universal access to information a reality.

As lightweight devices connected to mesh networks and ever more powerful computers all plug into the **grid**, they may face different constraints depending on whether they are contributing or consuming resources. What will be important here is that people all enjoy the right to equal access and are not discriminated against in the authentication and authorization processes based on criteria that are unrelated to computing and storage resources. Here again, the programmes people design for computers today will be the building blocks for these access controls, and the *Universal Declaration on Human Rights* can serve to guide the process.

Designing the right systems at this stage will prove pivotal for a future that draws upon **new technologies** such as optical or quantum computing. Today's decisions may prove crucial in ensuring that any vast, virtual "brain" that emerges uses its cognitive force to protect people in their humanity. If the Information Society makes the right choices from the ground up, tomorrow's high-powered machines may respect the values that have been ordered. In that sense, this future computing power has potential to guard human rights better than people have to date. The flip side, of course, could be dark.

In sum, the fundamental issue is not information itself, but the freedoms that it enables. The goal of the Information Society, then, is to promote the fulfillment of infoethics goals through the ethical design, deployment, and use of technology.

Recommendations

Emerging technologies open many new opportunities and avenues for action for UNESCO and its partners to fulfill their respective mandates and engage proactively in the development of the Information Society, as shows the following non-exhaustive list of recommendations.

1. ACTING AS A LABORATORY OF IDEAS THROUGH:

1.1. Establishing an Advisory Board

International work on the ethical implications of emerging technologies should benefit from regular insights by an Advisory Board. Policymakers and people generally are interested in what top technology experts have to say, and there are complementarities in the interests of UNESCO and the programmes of certain academic institutions focusing on technology – both of which embrace goals like respect for human rights and access to knowledge. Therefore, having a special Advisory Board on infoethics would allow UNESCO to harness the knowledge of top technologists and to benefit from the respect accorded them.

Such a group could help UNESCO continue to engage in the types of collaboration pursued during the World Summit on the Information Society (WSIS), while avoiding the politics that weigh down large, high-profile forums.

To ensure the group's findings are adaptive and forward-thinking, this Advisory Board should include children and youth from around the world, as well as experts in technology and infoethics.

In addition, UNESCO could collaborate with academic institutions in hosting brainstorming sessions to consider pressing issues of the future.

1.2. Establishing a Community of Technologists to Protect Personal Data

As noted in the survey, the control of personal data flow will prove pivotal for the exercise of human rights and access to information in the Information Society. This factor is one of the most important identified in this survey of "Ethical Implications of Emerging Technologies" as technology will increasingly have potential to be used to wield control over people's existence.

Because digital identity management will serve as the base component for other technologies dealing with the flow of personal data, and because industry is preparing to release new tools in the coming months, this particular technology is suggested here as a subject for special collaboration.

Substantive work on personal data protection would fill a void in the international system. At present, there exists a critical need for the protection of personal data. This need is recognized by the international group of Data Protection and Privacy Commissioners, who in September 2005 adopted the Montreux Declaration calling for multilateral principles in this area. The need is also recognized by computer scientists – especially leading figures in the Identity Gang industry group and in the World Wide Web Consortium (W3C), who see their work as carrying great potential for harm or good, but who are looking for guidance as to what principles they should design code to support.

Of course, the topic of personal data protections is not new: To counteract the possibility of personal data being mishandled in the information age, the Organization for Economic Cooperation and Development (OECD) and the Council of Europe (COE) each developed rules more than two decades ago.[138] Together, these

[138] OECD members adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. The COE adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, CETS 108, in 1981. Subsequent instruments by these organizations have reinforced these ideas.

initiatives comprise a solid list of protections. OECD principles include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. Article 6 in the COE Convention adds an anti-discrimination provision.

However, the OECD rules are non-binding, and those of the COE hold only for signatories.[139] Even if adopted on a binding basis throughout the world, these instruments are legal only and as such are impractical for guaranteeing the proper treatment of personal data by machines located around the world. Working with W3C and academic institutions, UNESCO could help the technology industry to develop tools to enforce personal data protections where law falls short.

2. ACTING AS A STANDARD SETTER

2.1 Examining the Possibilities of Preparing a Code of Ethics

It is recommended that a Code of Ethics be prepared as a worldwide point of reference for ethics in the Information Society. A primary objective of the instrument would be to sensitize stakeholders to the shared responsibility of actors in the Information Society to promote infoethics goals.

2.2 Preparing a Study on Network Neutrality

It is recommended that an examination be conducted of the way different regimes regulate their networks (whether they impose neutrality rules, etc.) and the resulting networks these regulations produce. The Organization could watch to see when international rulemaking or standards setting might upset the principle of network neutrality, and it could intervene with appropriate contributions to discussions. Academic institutions could be asked to assist in this capacity.

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

2.3 Publicizing Infoethics Aspects of International Rulemaking and Standards Setting

While the composition of an Advisory Board and the brainstorming groups should remain relatively small to enable effective discussion, substantive points should be made available to the public via a web site, with summaries also available in written form for distribution to interested areas in the world that are not yet connected to the Internet. Meetings can be conducted via IRC and, if in person, can be webcast.

3. FOSTERING PUBLIC EDUCATION ABOUT THE STATE OF TECHNOLOGY

Other substantive work could focus on (a) whether the public has a right to know what the state of technology is; (b) if so, how this right can be given effect; and (c) how people can learn to understand technology's workings and respond in a way that respects each other's human rights in a crisis.

UNESCO should meanwhile support open standards and protocols that are generated through democratic processes not dominated by large corporations.

The use of OpenDocument Format and other open formats should also be encouraged as they help mitigate lock-in to certain technologies.[140] Other initiatives to consider include pursuing free and open software, as well as the "Roadmap for Open ICT Ecosystems"[141] developed last year.

To further these movements, UNESCO should become involved in standards-setting organizations and consult with technical experts, both to broaden its own understanding of the issues and to lend further strength to its actions.

[140] More information may be found at http://en.wikipedia.org/wiki/OpenDocument, viewed March 15, 2006.

[141] See, e.g., http://cyber.law.harvard.edu/epolicy/roadmap.pdf.

ANNEX: A Democratic Information Society (Summary of an Interview with David P. Reed)

According to David Reed,[142] a computer scientist who has been heavily influential in the development of the Internet, "Ubiquitous computing and ubiquitous connectivity are the synergy of interest – these technologies together would allow large-scale information-sharing systems." This section details an extensive interview with him.

The Legacy of Hierarchies

Ubiquitous computing until recently was affected by where computing originated – i.e. in a small sector of society (including large-scale organizations like the military or big business since they could afford the early versions of the technology). This small sector was using the technology primarily for computing and record keeping. The technology is thus tainted with the bias toward supporting what large-scale organizations share: that is, a "command and control" culture of overall vision with a boss and hierarchical structure, with this limited set of decision-makers defining what information the group was interested in and who had the privilege of sharing information with whom.

In early days of computing, 30 or 40 years ago, decisions concerning many systems were made in this type of hierarchical setting or culture. So, for example, computer security was defined as: "*What's good for the organization as a whole* should be allowed, and *what's not* should be disallowed." Meanwhile, there was no democratic definition of what was good for the organization as a whole. Security in the military context was heavily worked out in computer systems as non-discretionary access control – in other words, it was not within a person's own discretion to decide with whom to share information. The idea was to require individual decisions to be in line with overall goals, with these goals implemented according to top-down rules, manuals, and policy systems that were passed out to people who had no choice but to follow them.

[142] An interview with David P. Reed, Adjunct Professor at the MIT Media Lab. Reed co-developed the Internet design principle of "end-to-end" (with MIT Professors J.H. Saltzer and David D. Clark) and set out "Reed's Law."

The business world was a more heterogeneous environment. The question of information flow focused on boundaries, with each company having its different set of goals. Within a company the goals were shared, and information flowed between and within different divisions. However, cross-organizational information flow was to follow rules defined by a select set of people. (In other words, this system was hierarchical but more flexible than the military.)

That way of thinking about information sharing was not viable: When computerized, the military failed to work. The reason was that in practice, people had always bent the military rules; they were *empowered enough to break the rules* in the real world, and this discretion allowed the organization to function. The same was true in companies, where word-of-mouth information was flowing across organizations irrespective of what was supposed to flow. Trade secrets were not strictly enforced. This flexibility allowed companies to cut deals because people had a sense of valuations.

Ubiquitous computing is here today to the extent that nearly every communication that touches a computer or goes through a network does so in a way that the information is modified, or filtered, or facilitated. The system works despite the fact that designers of computer code have asked the computers to follow a rigid set of protocols or procedures.

System designers have been assuming that *the myth of how people communicate* is the way they actually do, and they have tried to build into computer systems the enforcement of the way society thought it communicated: They try to apply this myth to computers, for example, in the way that a desktop machine relates to a printer. Every time coders try to enforce such hierarchies, there is a universal lesson that the story that society is telling itself is wrong.

Our society tends to think the most valuable information is in the most expensive computer or in the bosses' heads. Not so – actually those in the center have almost no information. There may be some good judgment or wisdom, but most information is at the ends or throughout the culture. As society moves computers out into that space, it frees that information to be more usable … and discovers that the most useful information is not what is stored in the center. The "myth of where the valuable information is" is being corrected.

Ubiquitous computing and ubiquitous networking represent the containers for the most valuable information and the most important decisions – that is, the distributed ones that in aggregate make the world go around.

UNESCO probably has its own myth that it should not challenge strong authority.

By way of example: A government whose leadership prefers the concentration of power and secrecy is harmful to its country. The powerful end up isolated from the very thing that makes the world work – that is, information. There is a risk that the information they have at the center is wrong – after all, anything that is secret is unlikely to be calibrated against reality.

Computing is Extraordinarily Inexpensive

Computing is extraordinarily *in*expensive, and it is difficult for people to comprehend that it is going to be even cheaper. Take, for example, the $100 Laptop Project. It does not matter if it is that project or others – the genius is in recognizing that in a couple of years computers will be that cheap. The magic is it is the first computing device specifically designed not to be another office computing platform – rather, the $100 Laptop is designed to be *a medium for human expression* – thus, these devices constitute "*networked expression machines*". ICTs are no longer primarily concerned with automating a business process, but rather the value is seen in education: This ICT is being distributed to *children*. The focus is not on accessing some distant web site, but rather on enabling a group of people to communicate amongst themselves on a more local and useful basis. The goal is to facilitate individual expression and sharing, to allow collaboration. It may result in a hierarchy, but not one that was imposed, and not one that is permanent.

Fixed hierarchies historically existed because it was difficult to form them in the first place; but now setting up ad hoc groups is easy. This principle is at the heart of Reed's Law, which is a mathematical way of expressing a less mathematical point: If you make group formation or relationship forming lower cost, and it is a valuable thing to do, you'll be doing a lot more and capturing a lot more value.[143]

As Ronald Coase has noted, firms were set up for avoiding transaction costs.[144] Now they are not so necessary. Now organizations can be temporary, efficient, and low cost. As technology changes to enable a more efficient form of these virtual, technological affiliations, pieces of society can organize themselves to a task much more efficiently.

[143] For the mathematical derivation of the number of possible subgroups, see http://en.wikipedia.org/wiki/Reed%27s_law (as viewed on March 14, 2006).

[144] "The Nature of the Firm" in *Readings in Price Theory*, Stigler and Boulding, editors. Chicago, IL: R. D. Irwin, 1952.

Moreover, groups can form efficiently across a larger scope – for instance, the Internet allows *planetary-scale* groups to form efficiently.

Long Distance to Proxi to Mobile

In addition to the dismantling of transaction costs for group organization, ICTs have witnessed another trend relevant here: As networking technology covers local areas more efficiently, "proxi-com" sets in, and telecommunication – "tele" (far) "com" (communication) – is not necessarily an accurate way of describing communication. Rather, nearby communication on the community scale are more aptly called "proxi-com".

In early days of telephony there were many little networks within towns, long-distance networks between towns, and even international calling networks. The phone companies figured they could charge a good deal for long distance because people could not walk to their neighbor's house to have the conversation. Since the phone companies could not make much money off local calls (as people would walk), they set flat rates for local service. These flat rates led to ever more phone lines for local purposes, with the costs funded from long distance service. Next telephony moved to cellular networks that had mobility – meaning industrialized society went from long-distance to proxi to mobile communication.

Internet architects had a grand view of unifying all communication networks so that they would all be interoperable. Much of the value offered by the Internet was cheap long distance as people could log into computers across the country. Indeed, the web was accessing data from around the world. Now growth is happening in the local area Internet. The value a person gets from a broadband connection still includes being able to access sites elsewhere in the world, but newly popular activities like setting up a wiki tends to correspond to local space. People care more about what is local, and those values are being moved onto the Internet.

For telephony, mobile communication became important when people who were accustomed to local communication began moving around while communicating. Now the Information Society is getting mobile Internet. Once local areas have been covered with connectivity, the result is mobility. People can move about and plug into the network.

This last stage of the mobile Internet has not really started yet. It correlates with more mobile computing platforms. The $100 Laptop Project is interesting because it is mobile, an "expression machine" that is also designed to work outdoors rather than in an office. Using straightforward Wi-Fi technology, along with software allowing people with laptops to send files – a group can have a music jam session. This Wi-Fi technology is the first instance of a very flexible, high-speed mobile network – and it represents viral communication, a category of networks that work without preexisting infrastructures. Such a network could cover the whole planet, with the devices themselves forming this network.

The technology has reached the point where to use very efficient radios does not require a lot of money. Historically, the slow evolution of culture has been the brake. "Viral" communication is like viral marketing – it grows by word of mouth… excitement… people teaching other people. Technological changes require synchronization with cultural values to be successful. (Again, the military has not been the key driver of viral communication because they have repeatedly wanted hierarchy, where they add a layer to reduce connectivity. Current Chinese efforts to block communication are based on the same misconception.)

Communication media are not in and of themselves that cultural – rather, cultures will overlay themselves on the Internet as it provides a new vehicle for cultures to express themselves. Wires and digital-ness are not the culture itself, but the means by which culture may be expressed. Culture is not implemented with raw connectivity, but with users. Culture is exogenous not endogenous.

Things that Take Off, Scale, and Reinforce Themselves

Ubiquitous computing and mesh networks allow the creation of big effects. There is one problem, though: The technology can amplify anything, good or bad; it is like a biological epidemic – a process of amplification of viruses. The technology is good the way it allows people to form groups, to reach out, and to spread the word about good things. But the same dynamics happen with computer viruses and spam: When someone wants to use the network for ill purposes, there is a great deal of possibility.

Large-scale network defects could be curbed either by dampening them (that is, slowing their growth) or by creating a counter virus that could chase the whole phenomenon and kill it. This latter approach carries the danger of being a cure that turns out to be as bad as the disease – like using DDT to kill mosquitoes but then having the side effect of killing birds. So the network is not a force for good only.

The best hope is education in a deep sense – to bring every participant in the Information Society up to the level where he understands how the system works and people can act collectively on it. Society dealt with disasters of old through a command-and-control structure. Now people must understand the system they are part of – so they can benefit from local decision-making when undergoing catastrophic failures. The potential from proxi-com is thus in allowing more local and resilient recovery – but, again, humans must understand how it works. The Information Society needs education on this front.

In short, society needs to educate people about the systems themselves. This is a cultural challenge.

Conclusion

The most important part of coming to terms with this "far more connected, global computing and information-sharing" paradigm that the Information Society is entering is that (1) everyone must understand it, and that (2) each piece ultimately shares responsibility (a) for the success of the system as a whole, and (b) for the fact that a person's actions have ramifying and amplifying effects on people far away that he might not even see. It is a challenge to educate all people to be able to live in a world like that. There are huge benefits and shared risk.

To a greater extent than before because of technology, organizational heads do not represent the best knowledge to address problems. There is a systematic bias to ask only the heads to be in the room for decision-making. However, children aged 0-20 are much more aware of cultural and technological issues than older people are. They are more knowledgeable about evolving cultures than older people who assume the children will resemble them. (They will not.) Therefore it is important to incorporate children in decision-making processes more. If society cannot let them vote, it should at least listen to what they are saying and honestly try to understand the people who are adjusting to new technologies at a rapid pace. Places where *de novo* adoption is occurring are the places to learn. Those people are appropriating new technologies without prior constraints – and they may show the rest of the Information Society what is possible or what is useful. The $100 Laptop is a nice example: It will teach about cultural adaptation to technology.

The Information Society must recognize that the scale of things is larger and the reach of things is longer systematically. People need to learn to focus not just on local phenomenon but on global phenomenon.

UNESCO
Communication and Information Sector
Information Society Division
1, rue Miollis
75732 Paris cedex 15
France

Tel.: + 33.1.45.68.45.00
Fax: + 33.1.45.68.55.83

www.unesco.org/webworld

Paris: UNESCO, 2007