United Nations
Educational, Scientific and
Cultural Organization

Organisation
des Nations Unies
pour l'éducation,
la science et la culture

COMEST

World Commission on the Ethics
of Scientific Knowledge and Technology

8th Ordinary Session
Bratislava, Slovakia, 27-29 May 2013

Réf: SHS/EST/COMEST2013/EN/pub-5

ETHICAL AND SOCIETAL CHALLENGES OF THE INFORMATION SOCIETY

Background document distributed for the session on Ethics of the Information Society

Tuesday 28 May 2013, 9.10-11.00

ETHICAL AND SOCIETAL CHALLENGES OF THE INFORMATION SOCIETY

S. Romi Mukherjee

Background Report Prepared for the
WSIS+10 Review Meeting – Action Line C10

FINAL DRAFT
May 2013

ACKNOWLEDGEMENTS

This report has benefited greatly from the input and efforts of the following colleagues: Paul Hector, Iulia Sevciuc, Vincenzo Romano, John Crowley, Cedric Wachholz, Mika Yamanaka, Boyan Radoykov, Dulat Kasymov, Julia Tami Ishikawa, Eva Goettert, Marie-Christine Botte, Coetzee Besser, Grace Githaiga, Rafael Capurro, Guy Berger, Denisa Kera, and Mark Coekckelbergh. I thank the UNESCO Social and Human Scineces Sector and the UNESCO Communication and Information Sector for their comments on each draft of the report.

The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The ideas and opinions expressed in this publication are those of the author; they are not necessarily those of UNESCO and do not commit the Organization.

Table of contents

I. INTRODUCTION

At the World Summit on the Information Society in 2003, the Geneva Plan of Action was tabled to engender and embolden sustained critical reflection on the changing stakes of the information society with a view to formulating normative codes of conduct and principle-based frameworks for governmental and civil society policy in relation to the infosphere. Eighteen key areas of activity were identified and UNESCO was charged with pursuing six action lines.[1]

This particular study is a contribution to Action Line C10 – The Ethical Dimensions of Information Society. It is thus informed by article 25 of the Geneva Plan which stipulates that the Information Society should be subject to universally held values and promote the common good and to prevent abusive uses of ICTs (Information Computer Technologies). In addition,

a. [*The International Community should*] Take steps to promote respect for peace and to uphold the fundamental values of freedom, equality, solidarity, tolerance, shared responsibility, and respect for nature.[2]
b. All stakeholders should increase their awareness of the ethical dimension of their use of ICTs,
c. All actors in the Information Society should promote the common good, protect privacy and personal data and take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including pedophilia and child pornography, and trafficking in, and exploitation of, human beings,
d. Invite relevant stakeholders, especially the academia, to continue research on ethical dimensions of ICTs.[3]

Article 25 constituted the first phase of the WSIS process. It aimed to broadly "develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake."[4] Phase one was essential in 1) identifying the common contours and characteristics of what is referred to as the information society, 2) mobilizing the international community to take seriously the simultaneous capacity for the information society to advance democratic societies and encroach on their potential realization, and 3) outlining the groundwork for a principle-based approach to the ethics of the information society. Phase two of the WSIS process, known as the "Tunis Phase," produced the 2005 Tunis Commitment and Tunis Agenda for the Information Society. The former reaffirmed the international commitments made by the Geneva plan. It also took note of the need to broaden the scope of the original plan to take into account the accelerating pace of the ICT revolution and its larger implications on sustainable development, sustainable diversity, human rights, and social and economic growth.[5] The latter, a document of more than 120 articles, closely examined the financial and economic implications of this revolution and assessed its repercussions (or lack thereof) in Small-Island Developing States and vulnerable

[1] See http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/unesco-and-wsis/implementation-and-follow-up/unesco-and-wsis-action-lines/
[2] Unlike the other themes listed here, "respect for nature" remains a domain in which the international system has been slow to make progress. This is due, in part, to the theoretical and ethical quandaries that emerge in defining "nature," its intrinsic value, and its rapport with the human, and also to the complexities laden within on going debates on climate change and the anthropocene. Moreover, ICT-issues are ever difficult to articulate in relation to the abstract category of "nature."
[3] See http://www.itu.int/wsis/docs/geneva/official/poa.html#c10
[4] See http://www.itu.int/wsis/geneva/index.html
[5] See http://www.itu.int/wsis/docs2/tunis/off/7.html

regions. Moving beyond the rhetoric of the "digital divide,"[6] it also outlined key modalities of implementation for the evolving WSIS agenda.

The WSIS process thus moved from a phase of reflection to one of commitment and of follow-up; resolution 2006/46 "Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development", further confirmed this transition in building alliances with ECOSOC which was asked to oversee the system-wide follow-up of the Summit outcomes, as requested in the Tunis outputs. These meetings systematically built on one other, serving to better distill the key ethical concerns of the international community in relation to the information society and clarify the path forward.[7]

For Action Line C10, UNESCO follow-up was initiated by a consultation meeting held in 2006 and by five facilitation meetings, the latter four of which were held in collaboration with the now annual WSIS forum. The CI0 Ethics Meeting at the WSIS Forum in May 2011 focused on "Cyber and Information Ethics: Freedom & Security, Privacy, Malice and Harm, Property", The meeting explored how evolutions in the field of technology called into question normative notions of the human, not only in terms of corporeal life, but in how humans perceive their life-worlds. It further examined how and if the ethical norms that guide interaction in the "real" world necessarily translate to our virtual interactions in the world of cyber-space. It raised the question of the implications of the crowd sourcing of bio-data on personhood and bodily integrity while also probing whether the technology and patterns of use of ICTs creates the conditions for virtual forms of malice and harm. The C10 Ethics Meeting at the 2012 WSIS Forum developed these themes and engaged with the emerging challenges of "Cyber and Information Ethics: Fostering and Enabling Freedom on the Internet." The meeting examined the rapport between the infosphere and political, social, and cultural transformation. It mapped the geographies of the digital divide onto the geopolitical constitution of the world, while reflecting on how ICTs come to bear on policy production and democratic participation. These concerns were contextualized within the larger question of how social institutions can adapt to and engage with technological transformation. This report builds on the progress made at the UNESCO meetings with a view to providing robust conclusions and inputs to the WSIS process, particularly in terms of the development of a potentially more holistic UNESCO and international set of responses and actions.

UNESCO's involvement in the ethics of the information society is further bolstered by the work of the Information for All Program (IFAP). Created in 2000 and composed of an Intergovernmental Body and 50 governmental committees, amongst the core objectives of IFAP are the promotion of international reflection and debate on the ethical, legal and societal challenges of the information society. In the context of the C10 Action Line, the 2007 report "Ethical Implications of Emerging Technologies: A Survey" remains an IFAP milestone in the contemporary study of the ethics of information societies. Prepared by Mary Rundle and Chris Conley, the report drew on case studies, new theoretical frameworks, and policy debates. It

[6] The term broadly refers to relations of economic and social inequity that are systemically created by differential relations of access to ICTs, foregrounding how new paradigms of domination are forged through the maldistribution of scientific advances and information. On UNESCO's work on the digital divide see: http://portal.unesco.org/en/ev.php-URL_ID=15738&URL_DO=DO_TOPIC&URL_SECTION=201.html and http://portal.unesco.org/en/ev.php-URL_ID=6060&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html

[7] For further details concerning these meetings, see http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/unesco-and-wsis/about/unesco-in-geneva-phase/ and also http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/unesco-and-wsis/about/unesco-in-tunis-phase/

narrated the recent development of the "technologies story" while detailing the ethical ramifications of inter alia Digital Identity Management, Mesh Networking, Biometrics, and Sensors. Moreover, it outlined a series of important recommendations designed to guide policy-makers, stakeholders, and UNESCO in its development of standard-setting instruments and civil norms. More importantly, it couched the debate on emerging technologies within an ethical discourse that integrated human rights based approaches into its general perspective, thus insisting on the fact that, while technologies may be neutral or "value-free", their usages are not. Hence, the question remains how to put them in the service of human rights, greater equity, and justice.

From a methodological perspective, the ethics of the information society cannot be delimited to a purely formal approach to the new frontiers of the information society. In other words, an ethical approach to the information society is more than an affair of principles, normative frames, and recommendations. Rather "ethics," can be understood as the simultaneous affirmation of human rights, equity, and solidarity, as well as a field of inquiry and style of interrogation in and of itself. The efficiency of such inquiry, moreover, depends entirely on embedding the ethical challenges of the information society in "society." Stated otherwise, the information society is not simply a technical phenomenon to be regulated or measured, but a thoroughly social and human construct that must be engaged with the insights of the social and human sciences. Ethics, then, is not something imposed from the "outside", but rather emerges from within the phenomena that it addresses.

Within the context of UNESCO, such a social and humanistic approach to the ethics of science and technology has been most saliently represented by the work of the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST). COMEST is an independent advisory body charged with assisting the Director General of UNESCO in the implementation of ethical policy in relation to environmental change, accelerating technologies, and development. It is currently involved in a reassessment of the 1974 UNESCO Recommendation on the Status of Scientific Researchers. In addition, while not explicitly engaging with the issues raised by the information society, the 1999 Declaration on the Use of Scientific Knowledge**,** offers a series of foundations for a set of socially-based ethical paradigms on which the ethics of the information society can be built. For instance, it foregrounds how

Today, more than ever, science and its applications are indispensable for development. All levels of government and the private sector should provide enhanced support for building up an adequate and evenly distributed scientific and technological capacity through appropriate education and research programmes as an indispensable foundation for economic, social, cultural and environmentally sound development. This is particularly urgent for developing countries. Technological development requires a solid scientific basis and needs to be resolutely directed towards safe and clean production processes, greater efficiency in resource use and more environmentally friendly products. Science and technology should also be resolutely directed towards prospects for better employment, improving competitiveness and social justice. Investment in science and technology aimed both at these objectives and at a better understanding and safeguarding of the planet's natural resource base, biodiversity and life-support systems must be increased. The objective should be a move towards sustainable development strategies through the integration of economic, social, cultural and environmental dimensions.[8]

It goes without saying that this article of the 1999 declaration lends itself readily to the study of the ethics of the information society.

[8] See http://www.unesco.org/science/wcs/eng/declaration_e.htm

Much has changed in recent years. The ethical and theoretical debates surrounding emerging technologies have also undergone a series of shifts and new technological borders and new paradigms of technological personhood present new moral and social challenges. While some technologies (such as smart phones and GPS) have become fully "naturalized" without great ado, others have been perceived to have massive implications on social and political life (drones, genetic information, the political usages of YouTube etc.). This report aspires to critique the latest chapter of the technologies story while also asking what the next chapter might look like.

Access to information and the capacity to be able to enjoy the "right to communication" are essential to the achievement of greater equity in a global society. Information and communication are both "resources" whose ethical usage and distribution can create the conditions for democracy and greater well-being. Following from this, information and communication are certainly "natural" (i.e. what we do), but neither should be considered neutral by virtue of their respective status as facts. Communication and the free circulation of information are essential to the realization of "democratic selfhood" and the formation of the global public sphere. However, when refracted through the information society, such a public sphere appears radically reconfigured. While such a sphere is certainly defined by communicative action, it is not necessarily founded upon any consensual framework of liberal reason. Indeed, it is precisely where those who are shut out of this sphere find their own voices and channels of communication.

Information and communication are also the means through which discursive hegemony is constructed and the loci from where social hierarchies are naturalized through the forging of monopolies on truth, coercion and persuasion. Moreover, following Mcluhan, the medium may be the message, but it is a message not without ideological consequences. Communication is a symbolic site girded by certain laws, rules, and social grammars. It is a code which codes subjectivities in ways that can either embolden democratic practice or pervert it. While communication and information may appear to be simple social "givens", the technologies that bring them to circulate cannot simply be reduced to mere "tools." Communication, information, and their respective technologies (technologies which dialectically create the conditions for the possibility of certain types of expression), pose a series of complex ethical questions. These questions traverse the spectrum from the politics of performativity and speech-act (who says what, to whom, with what consequences etc.?) to the larger communicative sphere of the global socio-techno interface and the ethics of technology (how is what we say and the life world in which we say it dependent upon ICTs?). Beyond this particular theoretical framing are a host of others which formulate the ICT-driven world as a new space of cosmopolitan solidarity, a site of popular resistance and critique, and a network-driven infinity where one can be whatever one wants. Stated other-wise, ICTs necessarily open up a chiasmus of opposing spaces of agency that collide on the level of transmission and reception and subversion and recuperation.

A term that began readily circulating in the mid-1970s, by "infosphere" and information society we understand a world where the boundaries between the human, technology, and the media are dissolved, a world where "information" functions as a type of substance that animates, orders, and delimits human activity as both a field of possibility and constraint. Following Luciano Floridi, moreover, the infosphere, like the biosphere denotes an environment and an ambience which establishes the frontiers and horizons of human agency and knowledge.[9]

[9] See Floridi, L., 2002, On the Intrinsic Value of Information Objects and the Infosphere. *Ethics and Information Technology* 4 (4), , 287-304. Of course, Floridi's transposition of ecological discourse onto the information society should be understood as a hermeneutic mechanism for its reconceptualization. However, while such a theoretical transposition may lead to the creation of new ways thinking about the

Hence, any serious study of the ethics of the information society will therefore necessarily sidestep the temptations of both technophilia and technophobia.[10] It will avoid both hyper-modern mystifications of technology's innate emancipatory power and anti-modern condemnations of technology's inherent destructive capacity and perversion of various imagined "natures." This is to say that emerging ICTs, ranging from the internet to cyber-military paradigms, cannot be divorced from larger global political transformations and the creation of new subjectivities, new political processes, and new modes of being in the world.

Technology is not something "over there." Rather, it is part and parcel of the very tissue of global life, which is typified by ever-accelerating flows and fluxes of communication and information which not only serve to connect "the shrinking world" in the physical sense of the term, but also disconnect communities and actors through engendering the rapid collision of antagonistic world views, sensibilities, and notions of the "good." On one hand, the global techno-communication sphere can foster greater global solidarity and common feeling. On the other hand, it can equally reveal the radically agonistic character of contemporary politics and post-politics as a discursive process or field wherein opposing actors vie for position through ideological and information struggles which "use" technology as their primary means of persuasion, provocation, and perpetuation. And insofar as such politicizing necessarily invokes a vision of what contemporary societies *ought* to look like, this field is intrinsically ethical. The interface of "information" and "technology" thus engenders a new frontier of ethical reflection which refuses a separation between ethical agency and technological hardware all the while recognizing that classical normative ethical paradigms might not be well placed to confront the new domain of responsibilities that accompany the development of the information society.

In a general sense, the ethics of the information society finds its origins in the work of Norbert Wiener and the discipline of cybernetics. For Wiener, recently hailed by Flo Conaway and Jim Siegelman as the "dark hero of the information age," the central problematic of modernity was to be found in the interdependence of communication, technology, and power. Indeed, in his 1954 study, *The Human Use of Human Beings: Cybernetics and Society* he argued that contemporary society can only be understood through its messages and the nature of its "communications facilities" and the development of these messages and facilities, between man and machine, between machines and man, and between machine and machine. Wiener's dystopianism was also set off by an awareness that living effectively meant living with adequate information, that communication was a part of man's inner life, and information, a condition of his belonging to a given society. While cybernetics may have set the general parameters of the sociological issues of the information society, the development of the ethics of information and the ethics of information society as intellectual and policy-based disciplines is fairly new.[11] A transdisciplinary approach to cyber-ethics, media theory, cybernetics, computer ethics, information science, and

---

information society, it should be noted that terms like "biosphere" are forged in particular historical moments in relationship to particular phenomena. In other words, there are risks in fusing the two domains and discourses, not least of which is the disavowal of technological advance's role in biosphere degradation.

[10] It is important note that this polarity still guides both public and academic debate. And while they do certainly reduce the discussion to a set of entrenched social and political binaries, it must be recognized that the tendency to take one side or the other and the debate itself function as aspects of the information society (here, as a discursive construction that imposes itself on material conditions).

[11] According to Thomas Froehlich, Information Ethics emerges in the late 1980s as an offshoot of library and information sciences. The term "information ethics" was first used by Robert Hauptman in his 1988 study, *Ethical challenges in librarianship (*Phoenix, AZ: Oryx Press) and also by Rafael Capurro the same year in his article Informationethos und Informationsethik.(*Nachrichten für Dokumentation*, vol. 39, no. 1-4) See http://www.ub.edu/bid/13froel2.htm

theories of communicative action, the ethics of information society the ethics of the information society concerns itself broadly with the moral questions pertaining to the communicative capacities of new technologies and their/our particular manipulation of data and information. According to one of its recent pioneers, Luciano Floridi

> Information Ethics is the new ecological ethics for the information environment… The ethical use of ICT and the sustainable development of an equitable information society need a safe and public infosphere for all, where communication and collaboration can flourish, coherently with the application of civil rights, legal requirements and the fundamental freedoms in the media. An ecological model for thinking about boundary issues in the infosphere is important to foster the development of ethical rules and legislation about accessing, sharing, and manipulating information.[12]

When perceived as an ecology, the information society can be degraded and afflicted with various forms of entropy or emboldened and rendered more robust with sustainable information paradigms that assure equity, access, and responsibility (which, for for our purposes should be understood as the general conceptual architecture of information ethics paradigms). Floridi's ecology does not necessarily clarify *what* would count as ethical in this context of reflection. However, we can ascertain what its object is; under these general ethical rubrics, the ethics of the information sphere examines debates that move from the daily use of smart-phones to cyber-warfare. Along this range, one finds questions of the digital divide, security, freedom, the right to communication, ownership and property, malice and libel, cyber-war, surveillance, pluralism, and privacy etc.

However, ethical reflection cannot simply engage in purely meta-ethical speculation on the status of ethics nor meditate on abstract principles lest it become recuperated into a form of academic solipsism. The ethics of the information society should rather strive to inform policy makers and stakeholders who find themselves to be the victims of a time lag in relation to rapidly accelerating technologies. *Ethical reflection on the information society is necessarily reflection on the values of that society which understands itself as such and the translation of those values into a set of shared principles and/or normative guidelines.*

Following Floridi, the ethics of the information ecology entails confronting the infosphere as a biosphere which contains its own resources, services, and scourges. The "matter" of this ecology is, moreover, not simply technical or scientific; the infosphere is a resolutely social and human phenomenon. The ethics of information society is born from within the interstices and interface of human beings, human values, and technology. It cannot be denied that the deep embedding of the human in techno-machinic fluxes and flows signals not only a new mode of post-industrial flexible capitalism, but also a recalibration of human subjectivity in its corporeal, political, and epistemological dimensions. While the discourse concerning the information society as a definitive historical "rupture" should be regarded with some suspicion, an information-dependent human economy and ecology creates, as Manuel Castells has suggested, an information society that has its own principles of social and economic organization and cultural practices. Such a new social organization immediately gestures towards a new ethical paradigm, one which departs from conventional models of communication theory in order to assess the concrete realities and socio-political implications of technological use and misuse. That is, normative communication ethics, by and large, does not foreground the centrality of technological mediation and its capacity to not only establish the parameters of the message, but also circumscribe the knowledge and ethical substrate of a given society.

[12] Floridi, L., 2001. Information Ethics: An Environmental Approach to the Digital Divide, *Philosophy in the Contemporary World,* Vol. 9:1, Spring/Summer, p. 3

However, the elaboration of such a new ethical paradigm also forces us to rethink what "ethics" really is and what are approach to them should be. One can argue that ethics is the crtical engagement with the moral systems and foundations that inform the choices humans make as they move through the world with each other. Yet, when grafted onto the information society, the parameters of the human and his potential are radically transformed and with it, our confidence in the perennial nature of ethical theories that, more than often, depend on unchanging notions of human essence, human activity, and human aspirations. In other words, an ethical approach to the information society needs to identify what constitutes the human, its changing ontology (or lack of thereof), and reflect upon how notions of human dignity, choice, freedom, and personhood are transmuted, perverted, and reconfigured in the information society. In redefining the contours of the human in relation to the information society, one must also interrogate the new choices that such a human faces and also ask how such choices reconstruct his or her "humanity." Such inquiry can, moreover, not be developed in isolation. Rather, it must lodge itself within the transnational political landscape that girds the global information society, precisely where ICTs become vessels for competing universalisms and moral antagonisms – precisely where the nature of the "choice" and the "right action" are rendered ever-more opaque. While it is clear that our ancestors had similar moral dilemmas, we cannot say that the occupied a universe of accelerating globalism which requires rigorous reflection on how ethics and pluralism can be properly reconciled.

The mediasphere and infosphere are produced from within a rich and multi-leveled series apparatuses (governments, corporations, networks, and cosmopolitan regimes of action and knowledge). As such, the information society also denotes a set of soft and hard technologies which inscribe human agents in a field of power where there is no definitive barrier between the political and the non-political. Amongst the many questions that arise in a transnational gloss of the ethics of the international society, one finds inter alia: What kinds of ethical decisions can be made when there are imbalances in information? And if ignorance is not an excuse, how much information does one need to acquire before one can act "ethically"?

UNESCO's ethical mandate and on-going collaborations with IFAP and the WSIS Forum (endorsed by the UN General Assembly[13]), put it at the forefront of ethical reflection on the information society and as a global laboratory of ideas and competing universalisms also position UNESCO as the site where the shared values of this information society are refracted, distilled, and negotiated.

This report builds on the WSIS process and the UNESCO report of 2007. It seeks to trace the ethical implications of the new interface between human actors and the technological landscape. It asks specifically where and how values are articulated, perverted, or complicated within this interface. Reaffirming technology to be a social fact, this report assesses how technological innovation both advances human rights and human development and impinges on them by creating new modes of unequal technological distribution and misuse that threaten to scour global society of its ethical nucleus.

Two components are essential to this task. The first is a retrospective exploration of how the technologies identified in the 2007 study have evolved over the last 5 years. The second is the mainstreaming of a foresight approach which anticipates the next chapter of the technologies story and examines the ethical ramifications of trends in cyber- and information technology. This two-tiered temporal approach identifies the gaps in information society policy and the regulation of technological innovation with a view to evaluating to what degree ethical concerns come to

[13] See http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf

bear on these frameworks. Hence, this report also aims to raise awareness and bring the ethical nexus of the information society to the attention of key stakeholders. This is the beginning of a conversation where stakeholders find themselves better equipped to focus on the ethics of information society so that such concerns become the centre of the policy process and the larger public debate. This debate may then have repercussions for the science and technology world and further streamline ethical and human rights' concerns in the creation and design of new information technologies. It will, presumably, also bear on regulatory frameworks and illuminate where ethics and regulation sufficiently interface or not.

Of equal interest is the role that emerging information technologies play in the development of social and political transformation. Of course, social and political transformation are just other names for history and it would misguided to assume that contemporary societal tumult is intrinsically bound in or engendered by emerging technologies. Nonetheless, one cannot surmise that emerging information technologies have not had important roles in the organization, management, and exacerbation of social ruptures and transitions. This report thus examines how social and political actors find themselves alternately using and being interpolated by emerging technologies and the respective ideologies and interests that define their functions and content. It examines how social and political movements are technologically mediated and asks whether the technologies shape the ethos and aspirations that guide such movements.

This report will also touch on the ethical implications of emerging information technologies for the constitution of subjectivities in their social and psychological dimensions. Other questions concern whether the effects of technology are embedded in the design of both hardware and software thus problematizing claims concerning technological neutrality. While emerging technologies may be embedded in a evolutionary heuristic which does not oppose them to nature, but rather engages them as a second or other nature, the repercussions of this heuristic on security, privacy, and sense of self pose ethical questions that cannot be disengaged from some normative sense of what a body, what a society, and what communication should be.

In posing these questions, human rights-based approaches to ethics are essential. Mainstreamed throughout the report's methodology is an attentiveness to ICTs both for and against human rights. The report will seek to identify key areas where urgent policy discussion and attention is required in the post-2015 WSIS process.

II. REASSESSING THE LAST FIVE YEARS OF THE "TECHNOLOGIES STORY"

In the 2007 report on "Ethical Implications of Technologies: A Survey," Mary Rundle and Chris Conley argue that technology and society's rapid "technologization" move in phases, forming a narrative of the socio-techno interface in which technology is embedded firmly in historical and social transformation. In other words, modernity, post-modernity, and multiple modernities cannot be assessed purely in terms of critical historicism, class relations, dialectics, or the myth of progress. Human history is the history and story of technology. The most recent chapter of this story is that of information society. As Rundle and Conley emphasize, "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 world."[14] Over the course of the last five years, "cyber" has ceased to be an isolated domain or a "space" set apart. Fully implicated in daily global life, it shapes not only the physical world in concrete ways, but also human beings' reception, imagination, and sense of the physical world – a world fully mediated, virtualized, and cast into a spiral of simulation, data, anonymous exchange, second lives, and techno voyeurism for some people; a world of greater productivity, greater intimacy, and greater ease for others.

The "technologies story" has grown ever more complicated. Human beings' find themselves in its second (or potentially third phase). After the giddiness of connectivity, the dreams of a new technological humanity have been supplanted by fears, anxieties, and phobias about the information society's capacity to reshape the "natural" and create the conditions for new forms of harm. While these anxieties are not necessarily new and find their origins in the rapid technological transformations of the 1970s, they have become more pronounced, more apocalyptic, and more pervasive. The technologies story has taken a radically dramatic turn, particularly in relation to new modalities of surveillance, identification, profiling, and security (which, in this context, is both a geopolitical concept as well as one that bears on individual identity and well-being). Yet, one is at pains to say that the world has been reduced to an Orwellian dystopia; indeed, regardless of technological advance, life still goes on as it always did.

Nonetheless, things have become more complex and. as the story gets more complicated, so too do the ethical and info-ethical challenges of the technological landscape. For instance, five years ago developments as the Facebook and Twitter revolution, the altering of cognitive memory capacity by Google, the relationship between cyber-bullying and teen suicide, the question of hate speech and technological mediation, and the waging of war through drones and other non-human "actors," received little attention (as did the ease of electronic banking, digital libraries, skype, and various open-access sources). However, before turning to the societal shifts effected by these new phenomena, it may be useful to re-examine the evolution of the technologies first explored in the 2007 report in terms of both policy developments and evolving challenges. Of particular interest is the reassessment of digital identities, RFID, sensors, ICT for human rights, and the larger transformations of security and freedom in the information society.

[14] Rundle, M., and Conley, C., 2007, *Ethical Implications of Emerging Challenges: A Survey,* Paris: UNESCO Press, see http://unesdoc.unesco.org/images/0014/001499/149992e.pdf, p. 8

II.1 Digital Identities

Embedded in social life, information technologies and cyber technologies are not simply lines of passage for personal information, but sites of construction for new digital personae that often bear little resemblance to the characteristics and subjectivity of their embodied point of origin. The space between digital identity and "real" identity is not arbitrary or simply structural. On the contrary, it is from within these interstices that important ethical questions are posed. They relate, for instance, to how and whether the ethical frameworks that gird the "physical" world should carry over to the cyber world (particularly when their boundaries are blurred).

As indicated in the 2007 report, the infoethical dimensions of digital identity can be classified along two poles of possibility: On one hand, digital identity management can serve to enhance privacy and security, bolster freedom of assembly, and encourage new modes of communal life based on collective affinities. On the other hand, this technology can engender profiling, new forms of government-centric and commercial surveillance, discrimination, security risks, and the subjugation of "subjects" and their agency to machines.[15] While policy has not entirely lagged behind, there do not exist common global or European approaches to the question of digital identities. Yet steps are being taken to lay the groundwork for a more unified approach and regulatory frames have slowly begun to emerge.

The OECD's March 2011 report on "National Strategies and Policies for Digital Identity Management in OECD Countries," for instance, examines the policy-related and ethical implications of digital identity with a view to identifying the obstacles to robust digital identity policy on the national level. Hence, according to the authors,

> Developing and implementing a national digital identity management strategy covering an entire country's population is inherently complex and requires time. The nature, scale and complexity of challenges such as interoperability, security and privacy are related to the core objectives supporting the strategy (e-government, cybersecurity, broader Internet innovation). It is not realistic to target and address all core objectives and all challenges in parallel and with the same degree of priority. The more extensive the core objectives, the greater the number of challenges to overcome. Most countries probably try to strike a balance between objectives that match their broader national priorities and the challenges they can manage in the short term. They recognize that there are limits to what their policies can do to support their strategy: what is possible in the short term is not necessarily what they would like to achieve in the long term. Digital identity management at the national level is a journey.[16]

In other words, digital identity policy, if it is to be properly infoethical, needs to be broken down into sub-objectives which identity key concrete areas of possible implementation and good practice. A more holistic approach to the information society should certainly guide our reflection here, but ethics cannot engage the "whole" in any systematic manner and remain practical and effective. . According to the 2011 OECD report, infoethical policy in relationship to Digital Management should target the following six areas of policy and of user empowerment:

1) *A citizen registration policy* which can provide the basis for the bond and legal binding between the individuals and their electronic identity.
2) *Adoption of the citizen credentials* (mandatory or voluntary): Governments have adopted various means, from persuasion to coercion, to encourage or mandate the use of digital citizen credentials by individuals and service providers.

[15] Ibid., p. 73
[16] See http://www.oecd-ilibrary.org/docserver/download/fulltext/5kgdzvn5rfs2.pdf?expires=1351761302&id=id&accname=guest&checksum=DDFD5BC8790AA121FF020BBA993ACB21, p. 20

3) *Interoperability policy*: For example, in a country with a decentralized IdM citizen registration policy such as Canada, interoperability is promoted in the context of federation agreements. The common policy objectives are described independently of the possible technical solutions to achieve them. Organisations participating in a federation agreement have the maximum flexibility regarding how to technically achieve the objectives. In contrast, countries following a centralized citizen registration policy are likely to adopt a more prescriptive approach regarding policy and technical choices.
4) *Security Policy*: One hypothesis is that IdM security stems from broader government information security policy and is not specifically addressed by governments at a policy level. An interesting observation is that the central and critical nature of the IdM function within the broader e-government infrastructure is not mentioned by respondents as requiring specific policy attention.
5) *Privacy Policy:* Countries with a centralized registration policy are more likely to require specific measures to protect the national identifier, access to the population register, and the use of the national or citizen card when they have one. Technical privacy protection measures can be seen as an efficient way to address legal privacy issues and are also important to enhance trust in and acceptance of the IdM framework.
6) *User Empowerment*: The promotion of "usability" through awareness raising, helpdesks for identity fraud, and innovative applications such as the Korean Digital Identity Wallet system which enables users to log in to Web sites without filling in ID and password information.[17]

What is, however, absent from the OECD analysis is an argument for digital identity as a zone of agency and self-determination which needs to be protected so as to assure not only personhood but also identity integrity. The question remains as to whether a rights-based approach will offer more identity assurance and strengthen the ethical nexus of the digital identity landscape. Such an approach may merit further reflection insofar as digital identity management cannot simply be reduced to password cracking or credit card fraud. On the contrary, as Elisa Bertino has noted, the implications of the digital identity world extend all the way to new processes of social engineering that could have massive impacts on not only the digital identity federation and governance but global citizenship at large.[18]

Yet another frontier of the ethics of digital identity is located in its impacts on the daily lives of young people, for many of whom the construction and use of digital identities and multiple virtual identities appear quite natural let alone banal. However, as is well known, in light of the ethical implications of the misuse of IdM, the apparent ease with which young people create and live in their digital identities is far from innocent. The Institute for Prospective Technological Studies, in a 2009 research report, concluded that, while young European Union citizens are incredibly tech savvy, their "... knowledge about data protection laws is very low. Paradoxically, more knowledge seems not to breed more positive attitudes … experience may matter more than the understanding of the legal system. Therefore, it is not surprising that young people should ask for *hands-on regulation.*"[19] However, even from a policy-based perspective which places ethics at its centre, it is not at all clear what such hands-on regulation might look like. In addition, it is not clear whether, and how, cyber ethics and info-ethics should be mainstreamed into school

[17] Ibid., pp. 20-27
[18] Bertino, E., 2004, *Digital Identity Management,* see http://www.itu.int/dms_pub/itu-t/oth/06/04/T06040040001PDFE.pdf
[19] Lusoli, W., and Miltgen, C., 2009. Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risk, in eds. Lusoli, W., Compano, R., and Maghiros, I., *Young People and Emerging Digital Services,* JRC Scientific and Technical Report, JRC-European Commission, see http://ftp.jrc.es/EURdoc/JRC50089.pdf, p. 59

curricula in the name of a new type of civics which understands well-being and citizenship to not simply be social or national questions but techno-social and global in nature.[20]

II.2 Biometrics

Closely aligned to digital identity management are trends in biometrics. In a general sense, biometrics is the science and technology of measuring biological and statistical data. Such technologies thus create vast repertoires unique of individual characteristics, ranging from facial structure to fingerprints, to the iris and voice. The "good intentions" of the biometric breakthrough, which we can roughly locate in the mid 1990s, were intended to foster greater identity integrity, stop fraud, and aid nations in confronting security threats of all kinds. However, biometrics is the technology par excellence for new forms of surveillance that not only impinge on rights, privacy, expression, and well-being, but also create new governmental monoliths of identity administration laden, of course, with the potential for corruption and the abuse of power. Biometrics presents a series of intrinsically ethical issues: it is "intrusive" on body, and psyche of their recipients; it creates an ambiance in which everyone is potentially a criminal or suspect (thus, creating new forms of collective moral panic, fear, and paranoia); it impinges on dignity and often, as in the case of airport body checks, are the grounds for humiliation and embarrassment; it also create various "states of exception" where biometrics can be instituted as a practice that does not require the consent of those it targets. Yet, the ethics of biometrics also extend well beyond offenses to the person. A series of other ethical questions are posed regarding what is done with the information accrued from biometric technology -- by whom, and for what purposes? Who has access to such data and how is it protected?

In his 2003 study on ethical issues in biometric identification, Anton Alderman argues that "privacy is control over how and when we are represented to others. The proliferation of representations that identify us uniquely thus involves a loss of privacy, and a threat to the self-respect which privacy rights preserve…the metaphysical 'piece of yourself' that is offered up may be important to retain control over and hard to recapture once it is put in the form of a proprietary digital image."[21] The ethical nexus of biometrics is thus found in the confluence of property (myself/my body), privacy (my right to choose how to re-present myself), and control (the loss of my own representation of myself). Ultimately then, biometrics poses the question of the uses of selves by others and particularly the use of data of ourselves, which far from being simply "statistical" has explicit ethical value. Turning to policy, Alderman adds that "it cannot be acceptable social policy to curtail privacy rights in the absence of compelling arguments that show such curtailment to be the best of all feasible alternatives. I know of no convincing argument of this sort that would justify mandatory biometric identification for any general social benefit."[22]

---

[20] Frameworks for cyber-education and social informatics have, nonetheless, been proposed by Richard Taylor, Penny Duquenoy, and Bern Martens. See Taylor, R., 2012, ITGS - A Blueprint for a Social Informatics Course in Pre-university Education, in *ICT Critical Infrastructures and Society* Vol. 386 Duquenoy, p., 2008-2011, "Protecting Children in online social networks", EPSRC Grant reference: EP/F035454/1, and Martens, B., 2007, IT, Ethics and Education: Teaching the Teachers (and their Pupils), in Goujon, G. et al. (eds.), *The Information Society: Innovations, Legitimacy, Ethics and Democracy,* Springer, Boston.

[21] Alderman, A., 2003, 'A piece of yourself': Ethical issues in biometric identification," *Ethics and Information Technology* 5, p. 143. The implications of this become all the more complicated when the circulation of "pieces of yourself" is actually voluntary. The recent trend of "sexting" wherein many young people exchange naked images of themselves on line and through ICTs is but one example of this.

[22] Ibid., p. 148

Yet, what constitutes a compelling argument? Can we simply reduce this argument to major crime, national security, and geopolitics? Or is the "compelling argument" tied to inter-personal ethics, let alone going through security, and electronic metro passes? Moreover, how can we assure, as Jeremy Wickins suggests, that biometric data is not used to promote new paradigms of social exclusion which are in and of themselves unethical. Can biometrics be used to re-entrench racism, discrimination against homeless people, elderly people, and people who are mentally disabled, and also begin cull data about what people believe?[23]

Biometrics policy has made great strides, but has yet to foreground adequately the ethical challenges of the biometric nexus in its considerations. Since 2007, the ethics and policy of biometrics has become an important sub-field in both moral philosophy and policy studies. For instance, a 2010 text, *Ethics and Policy of Biometrics*, edited by Ajay Kumar and David Zhang, that brings together new perspectives by policy-makers, ministers, and ethicists, has been vital in reshaping the debate. According to Roderick B. Woo, biometric policy and good practice must begin by taking seriously the following questions which it all too often evades in the name of various "compelling arguments":

1) What is the scope of the practice?
2) How many people will be affected?
3) The vulnerability of the people who will be affected?
4) Will biometric data be transferred to third parties?
5) What are the risks of identity theft?
6) How long will the data be retained?[24]

These seemingly elementary questions open up to a multiplicity of highly sensitive ethical concerns, particular in terms of the practice of the regulation of biometric technologies. It is important to cease to treat biometric data as a series of numbers and figures and understand that while "personal data" can be quantified and analyzed algorithmically, the content of that data eclipses its very form as a number or box to be checked. Those people who have their data voluntarily or involuntarily taken should be able to demand greater transparency on the part of the data collectors. But in speaking of "people," we must also be cognizant of the implications of data mining on the newly born and the dead for where it is not entirely clear who acts on their behalf and how. Following from this, the juridical-legal dimensions of consent and non-consent in biometric information-gathering need to be reassessed with a view to bringing them into greater synchronicity with the rights to privacy, security, and expression. It is essential to strive for greater equity and fairness in the process of gathering biometric data (which may necessitate the existence of neutral regulatory bodies and other forms that insure proper checks and balances). The international community must also begin to reflect on the calculus of "intrusion" and "compelling argument" with a view to establishing potential parameters on how far biometric technologies should go and under what conditions and in what context. Further reflection needs to given to what it means to collect personal data for "lawful" purposes. In a more general sense, data should only be collected when the parties involved can and are able to comprehend what Woo, for instance, calls the "privacy impact." These reflections may serve as a potential first step in thinking through the challenges of biometrics in ethical policy and practice.

Biometrics, like a host of new surveillance and data-mining technologies, foregrounds how new technologies can serve to "subjectivise" or "reify" otherwise free persons. Indeed, the larger

[23] Wickins, J., 2007, The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification," *Science Ethics* 13, pp.50-52

[24] Woo, R.B., 2010, Challenges Posed by Biometric Technology on Data Privacy Protection and the Way Forward, in eds. Kumar, A., and Zhang, D., *Ethics and Policy of Biometrics,* Berlin: Springer-Verlag, p. 4

question is what constitutes individual freedom in the information society and how this freedom is at once, conditional and increasingly curtailed.

II.3 RFID

Surveillance and profiling issues are also central to the new uses of Radio-Frequency Identification (RFID) and, particularly, in relation to the implanting of RFID in human subjects. It would be misguided to assume that the world of the "implants" is the stuff of science fiction or Hollywood cinema. The technologies that are used to track products and goods can easily also be used to track human beings, verify identities, and control access and movement. With RFID, there is a trajectory that spans from accounting to cargo, to the tracking of employees (through RFID that are embedded in uniforms) to the implantable chip used for security and reconnaissance. This is a trajectory that leads from Chronopost and Wal-Mart to the war on terror (from the benign to the less benign).

RFID technology has been available and used for over 30 years as a small and cheap means of tracking and identifying products and goods. Used for logistic purposes, initially, it was simply treated as a useful technology to render public services and commerce more efficient. However, as Conley and Rundle argued in the 2007 UNESCO report, "several corporations have begun embedding RFID tags into employee uniforms or identification badges, allowing an employer to trace the whereabouts of an employee at all times or restrict access to areas of buildings … RFID chips are also being implanted in people. These devices are currently the size of a grain of rice and are said to last 20 years."[25]

Implants also have a series of "good" and potentially "bad" uses: they can be used to store the medical data of people who are unable to communicate; they can allow employers and governments to control access to high-security areas (including military sites, sites of various catastrophes, and chemically or environmentally toxic sites); they can be used for immigration control and guard against the uses of forged documents and passports.[26] However, one should not assume that RFID use is restricted to niche security, medical, and commercial markets. While it may improve productivity, law enforcement, and delivery services, RFID certainly has the capacity to impinge on the human rights of people at their jobs, in their homes, at school, and during their leisure time. In Saudi Arabia, women can now be "chipped" and monitored by a massive electronic system that can detect "cross-border movement" – According to the Telegraph-UK, "Their "male guardians" receive text messages on their phones informing them when women under their custody" leave the country, even if they are travelling together. -- "The authorities are using technology to monitor women," said columnist Badriya al-Bishr, who criticised the "state of slavery under which women are held" in the ultra-conservative kingdom.[27] The chipping system was implemented following reports in November of 2012 that a Saudi women had converted to Christianity and fled to Sweden. However, such phenomenon is not restricted to patriarchal or misogynist social systems. Indeed a similar scandal recently took shape in the USA. In September 2012, a San Antonio, Texas, US, high school student created a controversy by refusing to let her high school oblige her to forcibly wear RFID tags in order to be tracked on campus. In what has been referred to as the "Showdown in San Antonio," the

[25] Rundle, M., and Conley, C., 2007, p. 42-43
[26] Ibid., pp. 43-44
[27] O'Mahoney, J., 2012, Saudi husband's alerted by text if their wives leave the country, *The Telegraph*, see http://www.telegraph.co.uk/technology/news/9698071/Saudi-husbands-alerted-by-text-if-their-wives-leave-the-country.html

student, Andrea Hernandez, refused to place a tracking beacon around her neck, claiming that it conflicted with her Christian beliefs (the tracking device being associated with the "mark of the beast"). Hernandez elicited the support of her family and other members of community. As a result, many people "expressed heightened concern about student safety since the microchip devices chosen by the district actively beam a unique identification number up to 70 feet, which could put students at risk from stalkers and pedophiles. The devices are always "on," even when students leave campus."[28]

Bolstered by protestors with signs reading "kids are not cattle[29]," "I am not a number," "RFID Chipped: Prepare the global prison system," RFID has received renewed attention as a potential threat to mainstream society, where all stand to be potentially turned into "cattle." This anecdote reveals the deep ethical challenges of RFID through which, in the name of security and governance, citizens come to feel "domesticated."

Unfortunately, RFID policy still, by and large, is limited to commerce and defense: for instance, the EU's basic approach to RFID, like much of the policy developed in the context of *Europe 2010* and the *Digital Agenda,* is embedded in the discourse of technological innovation, market drivers, low-cost measures and harmonizing frequencies.[30] The US Department of Defense, the other great proponent of RFID, focuses almost solely on the creation of the "dynamic battlefield" and "logistical transformation" (war is, above all, a game of logistics," and efficient "supply chains.")[31] Ethical considerations, and certainly those concerning the public are given little, if any, attention at all in these treatises. In 2008, however, the OECD published a report on RFID policy guidance. Although the term "ethics" or "infoethics" appears nowhere in the document, the report does examine at length the "privacy challenges" created by RFID (such as the invisibility of data collection, tracking, interoperability, and intrusion). It argues for a series of "safeguards" which may be used to confront these phenomena including privacy and security guidelines as well as new means of thinking about consent and privacy impact assessment. The report ultimately concludes that

> Like any information technology, if RFID were implemented without appropriate consideration of how to address privacy and security risks, it might damage the organisation that has deployed it, and cause harm to the individuals involved. Should significant risks be detected in existing or planned sensitive (e.g. passports, credit cards), large-scale (e.g. transportation systems) or striking (e.g. RFID implants) RFID systems, there would be a risk that RFID "hype" becomes RFID fear, damaging the perception of the technology by the general public and handicap its promising future. Such a scenario has already arisen. A number of RFID systems have been deployed without sufficient consideration for security and privacy, have been the target of severe criticisms by privacy and consumer organisations and have led to the creation of opposition or anti "spychips" groups. On the other hand, the industry, public and privacy and consumer organisations have initiated a dialogue towards the development of privacy and security best practices. *Transparency requires that individuals understand what the technology can do and cannot do. Raising awareness about technology capabilities and limitations may be essential to prevent individuals*

[28] Spychips.com, 2012, Showdown in San Antonio, see http://www.spychips.com/school/NorthsideBoardMeetingReport.html
[29] For some decades, cattle have been "implanted" or "chipped."
[30] German Ministry of Economics and Technology, 2007, European Policy Outlook: RFID, see http://www.statewatch.org/news/2008/jul/eu-rfid-of-things-germany.pdf
[31] Tsoungas, N., 2004, DOD RFID Policy: Leading the way in two worlds – Active and passive RFID, US Department of Defense, see http://www.astm.org/COMMIT/F34_RFID-NDIA.pdf

and organisations deploying RFID from perceiving risks that do not exist or neglecting risks that actually exist, and to help them make appropriate choices.[32]

"Spychips" groups[33] and RFID guardian projects are forums for popular reflection on the ethical challenges of RFID. In the name of "fighting back," Spychips offers council to consumers, lawmakers, and producers, of the risks of unregulated RFID societies. Eschewing common "awareness raising" in favour of a radical mode of transparency, Spychips is renowned for its drafting of the "right to know" act which assures that the public is cognizant of all of its interactions with RFID technologies and their impacts on their health and lives.[34] The next step in the infoethics of RFID appears to thus depend on the creation of a conversation between civilian activist groups and their ministerial and governmental counter-parts.

II.4 Sensors

Sensors introduce a series of other ethical challenges to the information society (as a surveillance society). Indeed "inexpensive, ever-watchful digital sensors are now ubiquitous."[35] In addition, private citizens have often unknowingly become the key purveyors in the circulation of digital sensor use. With the 2007 introduction of the Iphone into the mobile marketplace, smartphones have gone global. As a result, devices that can gather sensory data have become the norm for mobile consumers, whether they are tech-savvy or not. In turn, sensors are evermore present in the public sphere while their implications remain largely overlooked. Beyond smartphones, other innovations in technology such as tablets, camera-equipped computers and laptops, vehicles with built-in GPS, and soon, Google glasses, have created not just an information society, but a sensored society wherein monitoring and communication are one and the same thing. A 2011 USA Today article on sensors bordered on the dystopian: "Odds are you will be monitored today – many times over…Several developments have converged to push the monitoring of human activity far beyond what George Orwell imagined. Low-cost digital cameras, motion sensors and biometric readers are proliferating just as the cost of storing digital data is decreasing. The result: the explosion of sensor data collection and storage."[36] An ethical quandary is immediately posed by the fact that people's telephones can *identify* them, and the technology that people use to communicate, write, and function may constitute a breach of privacy. The information society creates connectivity, flows, and new forms of knowledge. However, it is also a society which effaces classical boundaries between the private and the public, a society where one will always be under surveillance (with no respite), where machines know who you are, where you are, and what you are doing. One can, moreover, imagine multiple "sensor scenarios," all with deep ethical ramifications: On the one hand, sensor data could be used to manipulate consumers, stock sensitive bio-data and create new forms of exclusion, effect employment practices and access to social institutions, and corrupt bank accounts, credit ratings, and health insurance coverage. On the other hand, as

[32] OECD Ministerial Meeting, Seoul, Korea, 2008, RFID: OECD Policy Guidance – A focus on information security and privacy, applications, impacts, and country initiatives, seehttp://www.oecd.org/sti/interneteconomy/40892347.pdf, pp. 66-67
[33] See http://www.spychips.com/
[34] See http://www.spychips.com/press-releases/right-to-know-bill.html
[35] USA Today, 2011, *Hello big brother: Digital Sensors are watching us*, see http://usatoday30.usatoday.com/tech/news/2011-01-26-digitalsensors26_CV_N.htm
[36] Ibid.,

many pro-sensor advocates argue, sensors ultimately allow society to capture the “bad guys” and, if you are not a bad guy, what do you really have to worry about.

The policy impasse, of course and once again, concerns the lack of clear regulatory policy regarding the use of commercial and military sensors. In other words, rapidly evolving technology that is capable of collecting sensory data and communicating that data with other sensory capable devices are multiplying in an unregulated cyber universe. Although Kris Pister’s brainchild, “smart dust”, still exists only in theory, there has been an explosion of researchers, scientists and commercial companies trying to advance and innovate sensor technology in recent years to that end. Industry-specific/targeted sensor devices are also, however, being created and promoted in an effort to advance public and environmental well-being.

That is, sensory data is not without its beneficial uses. “Real-time” sensory data is helping researchers advance green causes and promote sustainability globally. Sensory data has been used to monitor energy use, natural disasters, population patterns, and ecosystems. European cities have already started trials implementing sensors in parking lots that monitor vehicle activity.[37] In 2010, Hewlett-Packard announced its plans to create a “Central Nervous System for the Earth.” The multifaceted purpose of this ambitious project is to monitor the health of the natural planet, energy consumption and human patterns of movement.[38] Pete Hartwell, Senior Researcher for Hewlett-Packard, suggested that “the motives behind smart dust are altruistic.”

However, altruistic motives and purpose-driven advancements to sensor technology provide little solace to civil libertarians who see cyber-progress as eroding our fundamental rights to privacy and anonymity. Indeed, privacy advocate and attorney at the Electronic Frontier Foundation (EFF), Lee Tien, explained to CNN in 2010: "It's a very, very, very huge potential privacy invasion because we're talking about very, very small sensors that can be undetectable, effectively."[39] Tien further explained that, "[Sensors] are there in such numbers that you really can't do anything about them in terms of easy counter-measures."[40] Like Tien, privacy attorney Chris Wolf, believes that the expanding reach of sensors will directly impact human behaviour in the future: “Losing the right to anonymity … could ‘really have a chilling effect on where we go, with who we meet and how we live our lives.’”[41]

How do governments then begin to regulate ethically an unregulated and unchartered marketplace? One key proponent of the collection and “capturing” of “real-time data” is the European Commission, which aims to use innovations in sensor technology to revitalize the European technology industry.[42] The European Commission has also recognized the need to urgently address the implications of the vast amount of data that is continuously being collected by these sensors:

In the spring of 2012, the European Commission launched a consultation programme to work out how to update the extant Data Protection Act to cope with the Internet of Things. The first step is a survey to try

[37] See http://eandt.theiet.org/magazine/2012/06/smart-dust.cfm. Please refer to the Smart Santander project.
[38] See http://articles.cnn.com/2010-05-03/tech/smart.dust.sensors_1_smart-dust-sensors-kris-pister/3?_s=PM:TECH
[39] Ibid.,
[40] Ibid.,
[41] USA Today, 2011, *Hello big brother: Digital Sensors are watching us*, see http://usatoday30.usatoday.com/tech/news/2011-01-26-digitalsensors26_CV_N.htm
[42] Edwards, C., 2012, Smart Special – Smart Dust, in *Engineering and Technology*, vol. 7, issue 6, see http://eandt.theiet.org/magazine/2012/06/smart-dust.cfm

to work out how much privacy people will give up to support aims such as greater energy efficiency and what safeguards might be needed. Given the rate at which multinational online corporations such as Facebook and Google have acquired massive quantities of data on the population, the question is whether Europe and national governments can update their laws quickly enough to make a difference.[43]

The fact of the matter is that most people have *already* given up their privacy unwillingly[44] and have contributed to the massive amounts of digitally collected sensor data while continuing to believe that they have privacy in their daily lives. In line with the activities of the European Commission, governments, privacy and civil liberties advocates must now focus on how data is being collected, stored and shared both by human beings and artificially. This necessitates an ethical policy-based reflection which attempts to retrieve what is considered to be "private" and identify clearly when the sense of privacy is not that private at all. In addition, such a reflection must ask whether the data collected itself is public or private? Is the data being "mined" and to what end? Is regulation possible? What normative frameworks (if any) can be put in place to assure that government agencies and private companies do not have carte blanche to do what they will with the data that is collected? Should Amazon and Google be told to not customize itself to the consumer's profile or are their also innocuous forms of "recognition"? How can sensors be used to only fight the "bad guys?" But does this not also entail asking what a "bad guy" really is. It is in this latter question particularly that the ethical stakes of sensor technology is most powerfully articulated.

II.5 Security and Freedom in the Information Society

The ethical implications of these various evolutions in technology can broadly be mapped across a spectrum ranging from a vision of radical freedom to a vision of radical security. Among the dominant paradigms in the ideology of globalization and global technologies is that greater and more rapid connectivity inevitably lead to new forms of democratization, intimacy, and solidarity. Conversely, in contrast to the utopia of information society's bountiful promises, the repercussions of heightened surveillance, privacy breaches, and new forms of technological harm create a global information society typified by new fears and new panics. The salve for such panic is paradoxically greater security and regularization. These all too often lead to new forms of surveillance and intrusion. The freedom that emerges from the virtual world of strangers is concurrent with a deepened anxiety about those strangers and the impacts of the strange new machines that human beings plug into and plug into us. One wonders if the internet and the array of emerging technologies are training human beings to be good soldiers for the war to come? The information society, where pleasure, "friendship," knowledge, personal data, and drones all circulate, emerges as something of a fortress in and of itself. "Freedom" is a relational concept (never absolute) and is embedded in new forms of securization and militarization and in new forms of "soft control" which shape subjectivities and bodies through their "innocent" forms of use. As Zygmunt Bauman argues,

> Every coin has two sides. The fact that you can communicate via the internet with someone based in New Zealand and discuss the details of some sort of project also has its dark side. Not only terrorist activities, but virtually every criminal activity, could be based on this global net. In this context, a monopoly on the use of force – which, according to Max Weber, formed the basis of the modern state – ceased to exist long ago. In the past, sovereignty and authority were defined territorially, and the state-run military force was a sort of guarantee for this order. Today's terrorism, being a phenomenon of the era of globalisation,

[43] Ibid.,

[44] This must, however, be understood as a matter of degrees. There is a vast spectrum of intrusion that runs the gamut from the casual use of email to being the subject of sustained sensory tracking.

is by definition extra-territorial, and it thus eludes such a definition. The most powerful armed forces of all time, using the most sophisticated technical equipment and having at their disposal the greatest budget in history, are helpless against the individual using pocket-weapons weighing a pound. This is a very peculiar military adversary; it has no headquarters, no military base, no barracks to be bombed. This military force appears from nowhere and then disappears into thin air. Its organisational structures are of only theoretical importance. There is no commander; there are no orders or hierarchy; yet for some reason so many separate individuals follow the same path, even move in a similar way.[45]

The information society engenders and imposes a new type of "freedom" on consumers and citizens. If refused, it potentially leads to alienation, marginalization, and "disconnectedness." This is a freedom to be taken for granted, one which is, nonetheless, once again, sutured into every moment of daily life. However, it is tinged with the simultaneous threat of absolute insecurity or a rather insecure freedom. In other words, the frenzy of the information society contains carnivelesque dimensions which have to be secured; information society necessitates the managing of new techno-forms of mixophilia and mixophobia. It is replete with zones of disorder, encounters, interpolations, crowded spaces, intruders, stalkers, and meddlers of all sorts. In such a world, one wonders whether the feeling of "common identity" is cut through by an inverse dread of intrusion and whether, indeed, the information society has something else in mind for all who occupy it. Perhaps the information society is informed by a wholly other ethics that is alien to any semblance of the good that was theorized by moral philosophy? Thus, the changes that guide the information society demand epistemological and ethical changes. These concerns should guide us in our examination of the social transformations that accompany the development of the information society, particularly as they apply to shifting notions of the public sphere and its human dimensions.

II.6 ICTs for Human Rights

All apocalypticism aside, we should take seriously the capacity for ICTs and sensors to both secure human rights and function as ethical loci for better social health and well-being. This entails, among other things, considering emerging technologies from the vantage point of social transformation and "science-linked rights." For Richard Claude, for instance, the connection between human rights and science and technology concerns the formulation of "science-linked rights" These should reconnect the practice and implementation of science within a normative human rights framework and affirm that science, as a man-made product, must work vigorously for the betterment of human kind. The development of a normative protocol that assures such betterment is the horizon of the international system's relationship to science, technology and development. Furthermore, for Claude, scientists are also people who depend on human rights to protect their scientific freedom in order to promote humankind and human rights themselves.[46] The ethics of the information society is thus, also a science ethics which concerns the responsibilities of researchers in relationship to the technologies they design.

The right to the benefits of science and technology also extend to the world of ICTs. The right to access to scientific knowledge and the "right to communicate" figure among the most important of science-linked rights. Audrey Selian of the International Telecommunication Union has demonstrated the deep connection between the right to ICTs, social change, and the securing

[45] Bauman, Z., 2005*, The Unwinnable War*: an interview with Zygmunt Bauman, Open Democracy, see http://www.opendemocracy.net/globalization-vision_reflections/modernity_3082.jsp

[46]Claude, R., 2002, *Science in Service of Human Rights*, Philadelphia: University of Pennsylvania Press, pp. 14-17

and promotion of human rights on both the local level and throughout the international system[47]. From e-Government to electronic participatory forums, from virtual presses to the consolidation of virtual power and networks, ICTs are instrumental in the future of democratic practice and the human rights-based democratic paradigms.

Access to information and the capacity to be able to enjoy the "right to communication"[48] are essential to the achievement of greater equity in a global society. Information and communication are "what we do," but they are also "resources" whose ethical usage and distribution create the conditions for democracy and greater well-being. They are also the building blocks of UNESCO's vision of the inclusive knowledge society to come, a matrix of governance, indigenous culture, and human capital typified by ICT accessibility, collective innovation, and the free flow of global knowledge. In such a society, information and communication would, in fact, cease to be simple "resources" or "affordances," but would function as the grounds for shared global life.

However, the right to communication and the free access to be information can be quashed through inter alia political censorship, filtering, under-development and cyber-red lining or the deliberate marginalization of populations through the barring of access to ICTs. The global digital divide is therefore the site from which new forms of exclusion emerge and find themselves contested. In other words, ICTs and the formation of responsible cyber-citizens/outlets are intrinsically ethical *and* human-rights based issues.

Conversely, new ICTs can also be used to identify and track human rights' violations. Geo-spatial, satellite imagery, and geographic positioning systems are important tools for monitoring how human rights violations occur on a scalar and bio-political level. Amnesty International has recently created the Science for Human Rights Project where geo-spatial technologies are used actively to "gain access to previously inaccessible conflict zones, provide compelling visual evidence and present information in a new and engaging way, all of which assists our activists in their campaigning efforts."[49] Insofar as "proof" can be offered of mass human rights violations, this particular human rights-based approach to science and science for human rights can potentially have enormous impact on the legal and juridical treatment of human rights violations and international law. What remains to be examined thoroughly, however, is the status of geo-spatial data in national and international human rights tribunals, the socio-political generation of the data itself, and the position of the stakeholders who read it and the nature of their "reading practices." Amnesty's recent work in Syria, "Eyes on Syria" [50] illustrates the breadth of technologies which can, with great precision, track unlawful executions, cases of torture, and the destruction of property. The American Association for the Advancement of Science has also emphasized the importance of geo-spatial technologies which, according to Susan Wolfinbarger and Jessica Wyndham, can allow "unprecedented visual access to remote and dangerous locations," can enable "experts to analyse and quantify levels of destruction," and provide "the means to communicate otherwise complex and/or abstract information in a way that can prove powerful whether in advocacy campaigns, policy debates or litigation. With the increasing availability of satellite imagery and innovative approaches to the collection, analysis and display

[47] See http://www.itu.int/osg/spu/wsis-themes/humanrights/ICTs%20and%20HR.pdf

[48] It should be noted that this concept remains part of an unresolved debate in the WSIS process wherein it remains unclear whether standard notions of freedom of expression should also include reciprocal notions of the right to receive information. The "right to communication" cannot be assumed to be in any way given or universally agreed upon.

[49] See http://www.amnestyusa.org/research/science-for-human-rights

[50] See http://www.eyesonsyria.org/

of information, it will be vital for the community of scholars, organisations and advocates concerned with displacement to come together with the technology community to identify areas of current need to which geospatial technologies and techniques can provide increasingly vital input." [51] Indeed geo-spatial technologies stand to powerfully recast the international community's many campaigns against human rights violations.

[51] Wolfinbarger, S., and Wyndham, J., 2011, Remote visual evidence of displacement, *Forced Migration Review*38, see http://www.fmreview.org/technology/wolfinbarger-wyndham.html

III. INFORMATION ETHICS AND SOCIAL TRANSFORMATION: THE PUBLIC SPHERE

III.1 Of Rules and Norms

The public sphere is a techno-system or field of information circulation. In it, discourse and machines merge to create new forms of hegemony and new forms of resistance. Information is the medium of the public sphere, the ground on which social relations are structured and organized. As media, and the primary phenomenon of "mediation," the information flows of the information society circulate through telephones, books, magazines, newspapers, radio, film, television, iPods, cell phones, video games, and, of course, computer and cyber-technologies. While communication, information, and media are not new, new ethical questions are posed by their embeddedness in new and emerging technologies. In other words, one must ask how the media interacts with the message and how the space of this interaction is charged with ethical concerns. On one hand, one may argue that technology is neutral and that the primary ethical agent of the information society remains human will and intention. On the other hand, such "techno-libertarianism" can readily be called into question by a more "materialist" thesis which argues that the conditions for new types of harm and ethical infraction exist within the technology itself. This shifts the locus of ethical responsibility from users to the nexus of user/technology/receiver/society. Any ethical approach to information society would thus have to ask the following kinds of questions:

- How do new technologies forge anew people's subjectivities and our collective "reading" practices?
- What are the cognitive and humanistic implications of the information society?
- Who attempts to persuade and coerce whom through new technologies?
- How is the efficacy of such coercion affected by the parameters of the technology itself?
- How does technology "act on" society?
- How can technology destabilize the conventional dichotomy between human subjects and technological objects?
- How exactly do new technologies reshape the contours of natural and daily reality?
- What are the ethical repercussions of such a reshaping?
- What groups, agents, and institutions are responsible for the narratives that produce the information society?
- How does technology work for us? Conversely, how do we "work" for technology?
- Who "wins," who "loses," who is harmed?

In posing these questions (which inevitably give rise to other questions), the information landscape is revealed as a site of agon between "human values" and a new set of values which emerge from within the socio-techno interface. Here, ethicists are charged with the task of

clarification and distillation of human beings' values and what they should be in relation to the information society. Such a clarification inevitably becomes complex when it attempts to unravel the dividing lines between human mastery, technological mastery, and their respective blurrings and "mediations."

As David Gleason has noted, "examples abound on how the Internet has changed the rules. From iTunes to Amazon.com, the impact on trade has been enormous. Encyclopedic information, opinions and chat are clicks away. And yet, the rules are nebulous, uncertain. We may think we know what is bad, but we have not yet codified it. The same person who would never steal from a store might download a song without a second thought. Many people are struggling to inject norms of behavior into this environment. The financial and personal stakes are epic."[52]

Infoethics is precisely where reflection on such norms can begin. Its task is not to "make the rules," but rather to examine where old rules may no longer apply and where new rules might need to be made. However, rules evolve with societal and technological shifts. Info-ethics must therefore explore the new trends in the information society with a view to examining the concrete domains where norms are called into question and recalibrated and, with them, the very thing we call the public sphere.

III.2 E-Governance

Among the most heralded innovations of the cyber and virtual world is the construction of new political communities and fora where citizens can either anonymously or in their own names contribute to vital political discussions, engage in both constructive and corrosive criticism, reflect on institutional politics, distil their social concerns, and find other likeminded thinkers and activists. The virtual political world is thus theorized as an important tool where everyone who is connected by internet can perform their duties as citizens and, in a thoroughly populist manner, engage with pressing social issues. However, the question remains as to whether such modes of virtual discourse are as participative as they claim to be or are mere distractions for citizens (who are made to "feel political" on-line while they have little impact on the nature of real policy implementation). On one hand, new virtual political communities have been praised as the future of the public sphere and deliberative democracy, a new space where citizens can sensitize themselves to contemporary issues and find the information they need. On the other hand, as Anthony G. Willhelm has noted, "technologies as currently used largely unravel the democratic character of the public sphere, they are framed largely as threats … they remain challenges insofar as political actors and the public fail to press simultaneously for substantial media reform and for substantial public-interest values in order to realign the aims of communications infrastructures with the needs of a democratic polity."[53] Such realignment, an implicitly ethical and policy-based challenge, is complicated by the material nature of virtual deliberation. e-forums allow the user to chime in and exit at will. This renders virtual politics not only temporal, but the site of fragmented participation; much of what constitutes speech in the virtual public sphere is ad hominem, unserious, and often vindictive; serious political fora demand a certain type of political literacy which is not available to all and is forged by the general framework of the virtual political arena. Hence, both the design and practice of e-politics creates its own set of

[52] See http://www.info-ethics.com/Legal_Policy.htm

[53] Willhelm, A. G., 2000, *Democracy in a Digital Age: Challenges to Political Life in Cyberspace*, London: Routledge, p. 10

impasses which dramatically diminish what it means to have a voice heard, particularly if that voice is lost in the midst of millions of blogs, comments, and responses.

Digital or "e-governance" has emerged as one means of confronting these issues from an institutional and governmental perspective. From its inception, e-governance aspired to tap into the non-hierarchical, open, and free flow of information exchange that characterized virtual political community and bring it to bear on policy-building. The original assumption underlying the dominant paradigms of e-governance was relatively simple: the radically deliberative and democratic nature of cyber-politics could cross over into the sphere of policy production, and render policy creation more deliberative and democratic.

As noble as these intentions may have been, they failed to grasp the deep ethical problems of digital governance and administration, a lacuna which still permeates the e-governance world. Several issues are important: access, security, data management and the role of policy development overall.

Access remains an issue. The idiosyncratic nature of many e-fora does not take into account the multitude of voices that are left out of the conversation, often deliberately. Security continues to be an issue, insofar as e-governance almost always requires some sharing of personal information and data. Once again, the management of voices, data, and opinions inevitably activates fears about where the information is actually heading. There is a possibility that a hidden hierarchical paradigm floats underneath the apparently neutral or open cyber-systems. Hilary Mullen and David Horner, for instance, insist on the need to develop urgently new rules and models for ethical behaviour in e-government. Following the work of Pouloudi and Papazafeiropoulou, the authors map the ethical e-governmental terrain through the following questions of trust, social justice, and digital divides:

- Is governance about protection or restriction?

- What is more important property protection or the free exchange of ideas and data?

- Should self-regulation prevail in various industry sectors or should regulation be the responsibility of national governments or international organisations?

- Should governments give priority to national competitiveness or to international compliance and protection of national identity?

- Should governments promote their own interests or provide assistance to developing countries?[54]

When posed in the context of the electronic environment, the ethical challenges of these questions immediately have clear implications for the private sector, citizenship, and geopolitics at large. Policy also has yet to "catch up." As Juliet Lodge suggests, in her 2009 report for the European Commission on "ICTs and Science for Society and Ethical e-governance", the challenges of e-governance in the years to come are inherently ethical:

How we govern ourselves reflects not simply constitutional practices and arrangements but increasingly relies on technological tools for administering services to citizens. Reliance on technology for

[54] Mullen, H., and Horner, D.S., 2004, Ethical Problems for e-Government: An Evaluative Framework, *Electronic Journal of e-Government Volume 2 Issue ,* p. 193

administration poses ethical considerations that have been overlooked as policymakers, ICT developers and vendors and the public have become mesmerized by gadgets and applications derived from scientific and ICT advances …[55]

In this analysis then, the advances that accompany the advances of E-governance actually delimits human beings' attempts to reflect on the ethical challenges it poses and, for instance, begin seriously thinking about democracy as not simply the collection of a citizen's "political data."

III.3 The Social Media Revolution Reconsidered

At the time of the drafting of the 2007 UNESCO report on the Ethical Implications of Emerging Technologies, Facebook was only three years old. It was still considered a minor phenomenon, an extravagant form of email that was restricted to young college students and members of Generation Y. By mid 2011, during the beginning of the Arab Springs, Facebook was redubbed a tool for revolution. Mark Zuckerberg, a self proclaimed geek from Harvard with an eye for profit and a specific vision of the community to come, was praised as the inventor of a new revolutionary post-politics. One Egyptian militant went so far as to name his newborn daughter "Facebook."[56]

While there are certainly "applied" ethical concerns about new social media and its effects on the "social" and the subject, assessing the ethical implications of Facebook and Twitter also means examining how they unveil a new political horizon for demands for social justice, equity, recognition, and sustainability. Of course, revolutions, revolts, and insurrections have always relied on communicative networks, logistics, and codes for their efficacy. The questions, of course, are whether the technology of social media has radically recast the traditional role of political communication and, in doing so, has it opened up a new field for grassroots criticism of traditional modes of power. In other words, do the messages that buzz around the blogosphere really affect the distillation of democratic principles or are they mere communicative tools that signal a simple evolution of the role of newsprint, radio, and pamphlets.

Media critics and ethicists still remain divided on the question of the impact of social media in politics. There are several problems with the critical discourse concerning the politico-ethical implications of social media. First, is the tendency to fall prey to the delirium of the "Facebook Revolution" and the enthusiasm that casts it as a sign of a definitive rupture in the history of global politics. Second, however, is to submit to a reactionary tendency which, in dismissing social media, also downplays the role of youth in social and political innovation.

Like any technology, social media can be used to advance democratic ideals, but also, and in the most democratic of manners, rally against them. For each Arab Spring, there will also exist the blogospheres of terrorist organizations, white supremacists, and fundamentalists of all stripes. Before hailing Facebook as a new site of resistance and micro-politics, let us not also forget that for every "revolutionary tweet" and message, social media is more or less still defined as a site of cool hipster irony, new narcissism, and self-branding.

[55] Lodge, J., 2009, ICTs for society and ethical egovernance, Reflection Group on the Future of Europe – European Commission, see http://ec.europa.eu/education/jean-monnet/doc/future/lodge_en.pdf, p. 3
[56] Murphy, D., 2011, Egyptian man names daughter 'Facebook', *PCmag*.com, see http://www.pcmag.com/article2/0,2817,2380670,00.asp

All this not withstanding, New York Times journalists David Kirkpatrick and David Sanger, maintained that:

> The exchange on Facebook was part of a remarkable two-year collaboration that has given birth to a new force in the Arab world – a pan-Arab youth movement dedicated to spreading democracy in a region without it. Young Egyptian and Tunisian activists brainstormed on the use of technology to evade surveillance, commiserated about torture and traded practical tips on how to stand up to rubber bullets and organize barricades. They fused their secular expertise in social networks with a discipline culled from religious movements and combined the energy of soccer fans with the sophistication of surgeons. Breaking free from older veterans of the Arab political opposition, they relied on tactics of nonviolent resistance channelled from an American scholar through a Serbian youth brigade – but also on marketing tactics borrowed from Silicon Valley.[57]

Hagiography of this sort remains the rage in assessing the events of 2010 and 2011. Little attention is paid to how, in parallel with this movement, the Muslim Brotherhood was orchestrating its own social media revolution and taking full advantage of Silicon Valley's marketing tactics to persuade, proselytize, and coerce.

The ethical challenges of the Facebook revolution go well beyond who is using the technology and how. Rather, they concern what role such technologies really have in the constitution of political communities and in the forging of new forms of solidarity. Malcolm Gladwell, for instance, reminds his readers that the great revolutionary movements throughout time never needed Facebook and Twitter and probably still do not. Rather what they need is shared experience, common bonds, trust, and a sense of collective destiny that cannot be created on line. These expressions are, in many ways, too tactile for the liquid world of Facebook. Hence, in recalling the Civil Rights movement in America, Gladwell notes:

> Thousands were arrested and untold thousands more radicalized. These events in the early sixties became a civil-rights war that engulfed the South for the rest of the decade – and it happened without e-mail, texting, Facebook, or Twitter…why does it matter who is eating whose lunch on the Internet? Are people who log on to their Facebook page really the best hope for us all? [58]

The fact of the matter is that revolt, disobedience, and resistance continue in many places where few people have Twitter accounts and are not updating their Facebook status on an hourly basis. It is interesting to note that "If Martin Luther King Jr. had tried to undertake a wiki-boycott in Montgomery in the US, he would have been steamrollered by the white power structure. And of what use would a digital communication tool be in a town where 98% of the black community could be reached every Sunday morning at church? The things that King needed – discipline and strategy – were things that online social media cannot provide …"[59] The ties that united the members of the black community in the US in the 1960s were far more visceral and "felt" than the weak bonds that pass for friendship on Facebook. The upshot of all of this is that perhaps emerging technologies will not be the harbingers of systemic change and perhaps, "the message is not only about the medium."[60]

---

[57] Kirkpatrick, D., and Sanger, D., 2011, A Tunisian-Egyptian link that shook Arab history, New York Times, see http://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?pagewanted=all

[58] Gladwell, M., 2010, Small Change: why the revolution won't be tweeted*, New Yorker*, see http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell

[59] Adams, T., 2010, Twitter and Facebook cannot change the real world says Malcolm Gladwell, *The Guardian*, see http://www.guardian.co.uk/books/2010/oct/03/malcolm-gladwell-twitter-doesnt-work

[60] Ibid.

Nonetheless, social media and the blogosphere (which are not to be necessarily equated) do have tremendous populous potential and embolden the right to communication by allowing all who have access to the technologies concerned to speak their minds in "public" as they see fit. The future of social media may indeed move people from social media solipsism to greater social media activism. Hence, as W. Lance Bennett suggests, "the long-term picture of new media/mass media information flows is hard to project with much precision. Mass media news outlets are struggling mightily with changing gate-keeping standards due to demands for interactive content produced by audiences themselves. As consumer-driven content progresses beyond chats and click polls, new possibilities arise for high quality political information governed by more democratic and less elite editorial standards. Technologically savvy activists are writing software that enables automated and democratic publishing and editing. Ordinary people are empowered to report on their political experiences while being held to high standards of information quality and community values. In the long run, these trends (see, for example, www.indymedia.org, and www.slashdot.org) may be the most revolutionary aspects of the new media environment."[61] Yet while the software may have deep impact on bringing ethics to bear on politics once again, the long-term question of moving from frivolous social media use to more serious political mobilization ultimately depends on the larger issue of the creation of political consciousness in an age where it has seemingly been quashed by the forces of consumption, hyper-individualism, and techno-solipsism.

III.4 Blasphemy

The ideological articulations of the so-called "clash of civilizations" (a misguided thesis which aims to reconstruct the world into a new Manicheanism that serves American interests) have arguably reached new points of paroxysm with the Danish and French cartoons of Mohammed and the repercussions of a YouTube clip (posted July 1, 2012) entitled the "Innocence of Muslims. The incidents have not only renewed longstanding debates on freedom of speech, hate speech, and moral harm in the public sphere, but have also inspired a new set of conversations concerning media ethics and responsibility. The cartoon scandals and YouTube controversy have illuminated the very serious challenges of blasphemy in the information society. From the deaths of Pim Fortyn and Theo Van Gogh in the Netherlands to the countless *fatwas* issued every day, the information society has created new paths of expression and new trajectories of harm which have real consequences. The Innocence of Muslims YouTube video has been claimed as being the source of at least 75 deaths[62]. Yet, the causal chain between the images and their content and the actually passage to the violent act on the part of the receiver is not self evident. Moreover, if blasphemy constitutes an ethical transgression, so does killing. In terms of international human rights standards, there can be no justification for violent responses to mere expression. Legal expression that incites violence, or which can provoke risks to public safety, does not displace ethical choice from those who consume or otherwise use it. The IGF, Tunisia's internet authority, for instance, criticized Google for voluntarily blocking access to this video in Egypt and Libya, saying that it was the role of a company to make decisions on behalf of others. In Tunisia's case audiences were held to be "mature enough" to deal with such offensive materials. Avoiding the notion of "maturity", it would rather be important to highlight ethical reading practices in regards to those who engage in identity inflammation (of self and others) to violate human rights. Information may provide affordances such as rioting, but it is (some) actual people who commit the rioting.

[61] Bennett, W.L., 2003, "New Media Power: The Internet and Global Activism," see https://depts.washington.edu/gcp/pdf/bennettnmpower.pdf

[62] See http://rt.com/usa/news/google-muslims-film-garcia-478/

Regardless of these nuances, the debate on the "new blasphemy" has been decidedly un-nuanced. Staunch defenders of freedom of speech have refused to compromise or curtail their interpretations of the right to expression. They maintain that the public sphere of the information society should continue to be a site where everyone can say anything. For them, the essence of democracy is as a field of conflict where actors come together to negotiate their positions through various forms of communicative reason. However, what these new forms of blasphemy have proven is that communicative reason has its limits. It can be eclipsed in the name of harm, attacks on dignity, profanity, and self-interest.

Convinced of the limitations and conditionality of freedom of speech and the right to communication, a more moderate and realist view of the information society has also emerged. Countering the radical libertarianism that freedom of speech advocates espouse, it argues that the exercise of such freedoms will inevitably lead to irreparable injury and plunge the world into a cycle of harm and vindication. Compromises are thus the order of the day. Yet, how much compromise is appropriate, and how much compromise will threaten the critical function that makes a democratic society what it is? Will the tempering of freedom of speech to avoid insult, and accommodate the dignity of the other, not roll back the very notion of freedom of speech? How free is a person to speak when censorship becomes obligatory in certain moments and in certain contexts? Conversely, what, if any, limitations should be set in place when media outlets aspire to deliberately harm others in the name of freedom of speech and the right to communication – and when such liberties are brandished in the name of provocation?[63] In other words, the information society becomes the field in which religious and secular politics and values collide through emerging technologies and social media.

Of course blasphemy and the calculus of hate speech and harm is nothing new. However, emerging technologies enable blasphemy to circulate at greater speed and with greater scale, creating new global conditions for mass outrage, collective wounding, and spectacular symbolic desecration. While hate speech and insult have existed from the beginning of time, their mediatisation through social media creates new possibilities for malice. According to Saba Mahmood, "what is at stake is a moral impasse between what the European Muslim minority community regards as an act of blasphemy and the non-Muslim majority considers to be an exercise in freedom of expression, especially satirical expression, so essential to a liberal democratic society."[64] In response to the publication of the Danish cartoons representing Mohammed, Mahmood sees two poles emerging:

> …many claimed that Muslim outcry had to be disciplined and subjected to protocols of free speech characteristic of liberal democratic societies wherein all figures and icons, no matter how sacred, might be caricatured, satirized, or ridiculed without regard for people's feelings. Critics of this position, on the other hand, claimed that freedom of speech has never simply been a matter of the exercise of rights. It also entails the civic responsibility not to provoke religious or cultural sensitivities, especially in hybrid multicultural societies. These critics charged that European governments employ a double standard when

[63] In December 2012, it was revealed that many Australian radio stations thrive on making fun of or mocking innocent people. In the case of the mimicking of Queen Elizabeth and Prince Philip (of the UK), this has led to the much publicized suicide of the nurse who took the crank call, transmitted on Australian radio and more globally on international television channels. The nurse, of Indian origin, supposedly felt herself to be "shamed" and publically humiliated, leading the less culturally sensitive to argue that such feelings are pathological, that she should have simply "gotten over it." One wonders who really is sick here, the crank callers or the shamed nurse? Debates continue to abound concerning the causal chain between the crank call and the suicide wherein culture, pathology, and the tenets of western democracy all collide in various manners.

[64] Mahmood, S., 2009, Religious Reason and Secular Affect: An Incommensurable Divide?, *Critical Inquiry 35*, p. 836

it comes to the treatment of Muslims; not only is the desecration of Christian symbols regulated by blasphemy laws in countries like Britain, Austria, Italy, Spain, and Germany, but the media often makes allowances to accommodate Judeo-Christian sensitivities. Given that most Muslims regard pictorial depictions of the Prophet as either taboo or blasphemous, these critics attributed the gleeful display and circulation of the cartoons to the Islamophobia sweeping North America and Europe following the events of 9/11. For some, this was reminiscent of the anti-Semitic propaganda that portrayed Jews as a drain on Europe's land and resources. For many liberals and progressives critical of the Islamophobia sweeping contemporary Europe, Muslim furor over the cartoons posed particular problems. While some liberals could see the lurking racism behind these cartoons, the *religious* dimension of the Muslim protest remained troubling.[65]

Mahmood's particular understanding of responsibility in the information society hinges on a plea for the tolerance of the *reading practices* of others. In other words, it is impertinent for a western liberal to chide a Muslim for taking an image or a film too seriously, precisely when the Muslims share a particular intimacy with Mohammed which defies the secular logic that dictates "it's only a picture." Such secular logic also fails to see how the appeals to freedom of speech in such instances also naturalize the sub-textual racism or "ocular colonialism" embedded in blasphemous images and representations. Hence, the ethics of the information society not only necessitate new modes of responsibility which engender modes of deep reflection on and auto-criticism of the implications of each enunciation, but also a sensitivity to how the enunciation will be "read" by the members of the global community. However, as Christopher Hitchens has argued, such sensitivity to "reading practices" inevitably leads to dangerous forms of self-censorship and piety:

> Put the case that we knew of a highly paranoid religious cult organization with a secretive leader. Now put the case that this cult, if criticized in the press, would take immediate revenge by kidnapping a child. Put the case that, if the secretive leader were also to be lampooned, two further children would be killed at random. Would the press be guilty of "self-censorship" if it declined to publish anything that would inflame the said cult? Well, yes it would be guilty, but very few people would insist on the full exertion of the First Amendment right. However, the consequences for the cult and its leader would be severe as well. All civilized people would regard it as hateful and dangerous, and steps would be taken to circumscribe its influence, and to ensure that no precedent was set. The incredible thing about the ongoing *Kristallnacht* against Denmark (and in some places, against the embassies and citizens of any Scandinavian or even European Union nation) is that it has resulted in, not opprobrium for the religion that perpetrates and excuses it, but increased *respectability*! A small democratic country with an open society, a system of confessional pluralism, and a free press has been subjected to a fantastic, incredible, organized campaign of lies and hatred and violence, extending to one of the gravest imaginable breaches of international law and civility: the violation of diplomatic immunity. And nobody in authority can be found to state the obvious and the necessary – that we stand with the Danes against this defamation and blackmail and sabotage. Instead, all compassion and concern is apparently to be expended upon those who lit the powder trail, and who yell and scream for joy as the embassies of democracies are put to the torch in the capital cities of miserable, fly-blown dictatorships. Let's be sure we haven't hurt the vandals' *feelings*.[66]

The YouTube affair, however, exploded the robustness of the US First Amendment and forced the hand of many of its most steadfast supporters who found themselves forced to defend free speech while also conceding the need to *respect* others and foster heightened responsibility. While "YouTube ethics" has yet to become a scholarly discipline, the repercussions of the "Innocence of Muslims", a low budget, sub B movie, of 14 minutes directed by Egyptian born Nakoula Basseley Nakoula, have illustrated YouTube's capacity to enrage, outrage, and drive

[65] Ibid., p. 840
[66] Hitchens, C., 2006, Stand up for Denmark!: Why are we not defending our ally?, *Slate*, see http://www.slate.com/articles/news_and_politics/fighting_words/2006/02/stand_up_for_denmark.html

populations to violence. The film which blasphemes Mohammed in every possible way created widespread rioting and demonstrations throughout the Islamic world and is further, and perhaps mistakenly, identified as one of the key causes for the armed attack of the U.S. Diplomatic Mission in Benghazi, Libya on September 11th 2012, resulting in the deaths of the US Ambassador to Libya and three others. Moreover, while one might be tempted to read the affair as yet another example of secular western democracy provoking Islam, we should not overlook the uses of the clip and other social media internal to Islam itself. As Hussein Haqqani recounts:

> Thousands of cellphone subscribers in Pakistan received an anonymous text message recently announcing a miracle: an earthquake on Tuesday, Sept. 18, had destroyed the Washington, D.C. movie theater that was exhibiting *Innocence of Muslims*, the controversial film that has triggered violent protests in several Muslim countries. An email version of the text message even included a picture of a mangled structure. Allah, the texter claimed, had shown His anger against the movie's insult to Islam and Prophet Muhammad, and with Him on their side the faithful should not be afraid to vent their anger against the West, which belittles Islam and abuses Islam's prophet. There was, of course, no earthquake in Washington, and no movie theater had been destroyed. In fact, the movie has never made its way beyond YouTube…The Islamists first introduced the objectionable material to their audience and then instigated the outrage by characterizing it as part of a supposed worldwide conspiracy to denigrate Islam. The emergence of social media and the swiftness of international communications have made it easier to choreograph global campaigns, and in Muslim-majority countries, Islamists tend to be among those who are most effectively organized to take advantage of technology for political ends.[67]

YouTube soon blocked access to particular videos in a host of Arab countries while local governments elsewhere either blocked YouTube or began negotiations with Google Inc. to inaugurate new censorship policies which reinterpreted what constituted objectionable content. The Obama administration then intervened by asking Google and YouTube to "reconsider" the inclusion of the video on its site. After reconsideration, on September 24th 2012, Google "determined that the video did not violate its terms of service regarding hate speech. In this case, the video stays up because *it is against the Islam religion but not Muslim people.*"[68] In President Obama's speech to the UN on September 25th 2012, he defended the freedom of speech but he also noted that provocation and the spread of moral harm would not be condoned or supported. On November 7th 2012, Nakoula Basseley Nakoula was sentenced to one year in prison for probation violations connected to previous credit card fraud.

The YouTube affair asks that human beings engage in further ethical reflection not simply on the challenges posed by an incendiary film, but an incendiary film that viewers throughout the whole world can see over and over again. It also necessitates further study on the intercultural and inter-religious ethics of the information society.

III.5 Intercultural Information Ethics

The nascent discipline of intercultural information ethics asks how diversity and difference can be safeguarded in a technological landscape defined by homogenization, "leveling," and mass

[67] Haqqani, H., 2012, Muslim Rage is about politics not religion, *The Daily Beast*, see http://www.thedailybeast.com/newsweek/2012/09/30/husain-haqqani-muslim-rage-is-about-politics-not-religion.html

[68] Cain Miller, C., 2012, Google won't rethink anti-Islam videos, *The New York Times*, see http://www.nytimes.com/2012/09/15/world/middleeast/google-wont-rethink-anti-islam-videos-status.html (my emphasis)

consumption. This is a humanistic approach to the information society that treats cyber-space and the techno-sphere as a global domain where questions of identity, otherness, and recognition resonate with the same force that they do in the "real" social and political world. In other words, the digital environment is a seismograph that records the identity-related conflicts and tensions between the local and the global that animate the non-digital world.

Intercultural information ethics therefore seeks to examine the conditions for humane and ethical cross-cultural exchange in the virtual world. It attempts to locate the ethical frameworks necessary to establish the virtual universe as a space of decency, respect, and dialogue. It asks, for example, how do local and indigenous groups maintain the identity of their integrity in the virtual world? How does the virtual emerge as a place of strangers, a place where others are constantly interacting? How can ICTs bolster diversity, development, and economic equity as opposed to shaping the world in their own image?

Among the most prominent figures in this new discipline is the ethicist and philosopher, Rafael Capurro, who sees the virtual world as a new space for democratic consultation and the polyphony of cultures. As he emphasizes:

> It is indeed necessary to undertake an intercultural dialogue on information technology which means not only to become aware of the conditions under which different lifestyles and life projects can coexist within the new digital environment, but also in order to explore how it effects and is being appropriated by different cultures particularly as they are conditioned by this new environment…As far as I can see, the impact of information technology on a global scale and on all aspects of human life gives, on the one hand, a plausible argument in favour of the uniqueness approach not only with regard to the subject matter but also to the theoretical approaches so far. But this does not mean that, on the other hand, the moral code itself and its ethical reflection will be superseded by another one. The basic question concerning the status of moral persons, their respect or disrespect, remains unchanged although we may discuss as to what are the candidates and what this respect means in a specific situation. We may also discuss as to how this code has been interpreted (or not) within different ethical and cultural traditions and how it is being conceived with regard to the challenge of information technology.[69]

Reflection on the moral code(s) of the information society was initiated during the first phase of the WSIS process, particularly in relationship to issues concerning the digital divide and the right to communication. Essential to such reflection is the examination of how existing normative frameworks on cultural diversity can be translated into the challenges of the information sphere with a view to constructing a more inclusive digital landscape. This means not only bridging the digital divide but also, as Capurro suggests, overcoming "the isolation of moral traditions with regard to the internet," and providing "a platform for pragmatic action, for the kind of declarations and (quasi-) legal agreements that can be used as a framework for preservation and fostering of cultural differences in the new digital environment."[70] Part of the challenge here is to create a cyber-world which does not simply reflect the age-old political and philosophical struggles between the local and the universal, but rethinks the digital landscape as a more dialectical and fluid construction which potentially surpasses these binaries in favour of new paradigms of diversity and democracy. The history of social theory and moral theory cannot simply be translated into the digital world. The ethical question is how to take advantage of the new possibilities presented by the digital world to recalibrate and rethink the boundaries of freedom, justice, and diversity.

[69] Capurro, R., 2007, Inter-cultural Information Ethics, see http://www.capurro.de/iie.html
[70] Ibid.

Moving through the digital world is also a means of *acting* on the world. From a virtue-oriented ethics such "acting" should necessarily lead to greater forms of human flourishing, excellence, and interpersonal solidarity. Pak Hang Wong theorizes that the horizon of intercultural information ethics is a domain of inquiry into the "good life" and human well-being. According to Wong:

> In the West, philosophers have elaborated three major theories of the good life, i.e. hedonism, desire theories and objective-list theories. These theories allow researchers in Information Ethics to evaluate the impacts of ICTs and ICTs-related activities on individual's well-being; and, also allow them to offer positive recommendation based on the theories of the good life they maintain. Unfortunately, there are relatively few contemporary philosophical studies on the non-Western theories of the good life. Hence, to embark on the new agenda of IIE, the first step is to systematically investigate the non-Western theories of the good life. Once the non-Western theories of the good life are elaborated, researchers in IIE can begin to compare and contrast how different ethical and cultural traditions perceive the impacts of ICTs and ICTs-related activities on the good life. Researchers in IIE, then, will be better equipped to offer positive recommendation with respect to the good life in inter-/cross-cultural settings.[71]

Hence, on one hand, ICTs promote greater cross-cultural dialogue on what constitutes the good, the global good, and the common good.[72] On the other hand, from a more critical perspective, the good stands must be defined in relation to our embeddedness in the digital world and our uses of ICTs. In both cases, the digital world is one platform from which new ethical paradigms for a collective and shared life will be negotiated. Our relation to the digital is therefore also enmeshed in the practice of the good life and the bad life *vis à vis* who we want to become. Notions of culture are inherently connected to the nexus of culture and technology. This entails that human beings should begin to reflect on the information society beyond its strictly juridical and economic frames and start to examine how the "inter-cultural crossings" in such a society function as new laboratories for the distillation of ethical principles. The information society is therefore not a simple extension or mirror of "real" societies, but is also a site for the creation of new forms of mutuality and exchange and new forms of re-presenting selfhood and common aspirations.

Intercultural Information Ethics concerns our 'right' to be (become) ourselves as "selves" which are not self-enclosed, isolated from others, and detached from nature and the live world. Selfhood is dialogical here and not "fixed." Moreover, the protection of diversity in the infosphere, is less an issue of toleration and respect for difference, than the creation of conditions in which selves are free to become what and who they want to be. As a framework or set of conditions for relating, Intercultural Information Ethics aspires to construct a free space for dialogue and recognition of our mutual identities based on mutual 'evaluation' about who we are, what we do, what we can (or not) etc. This includes also a 'mirroring' of the common world and all kinds of 'positive' and 'negative' forms of mutual (e-)valuation so that common values are (or arise) out of this interplay. However, as Capurro emphasizes, this space of interplay should not be confounded with simple paradigms of multiculturalism and relativism or reduced to an abstract discourse of human rights. On the contrary, it is a space for reflection and a series of practices about ourselves (and our selves) in a common world. The interplay is what gives values their 'foundation' and simultaneously avoids the lapse into fundamentalism, superficial good-feeling or ideological dogmatism.[73]

---

[71] Wong, P-H., 2010, The 'Good' life in inter-cultural information ethics: a new agenda*, International Review of Information Ethics*, Vol. 13, see http://www.i-r-i-e.net/inhalt/013/013-full.pdf

[72] The good is, of course, contingent and actually comprised of a series of "goods" which depend on our styles of mirroring others and the natural world.

[73] Personal Communication, Rafael Capurro, December 18th, 2012.

When examined from the perspective of developing countries, other dimensions of this interplay must also be engaged with in relationship to development itself. The expansions of the information society may actually adversely impact sustainable social transformation if they move in a monolithic manner which does not adapt itself to the need to preserve indigenous cultures and traditions. Moreover, often, the less modern a society is, the more conservative the members of that society will be. This usually also goes hand in hand with a more holistic and integrated approach to culture, customs, and behavior. The transformation of developing communities on the level of ICTs necessitates that the development actors reflect on how they position their ICT-oriented development frameworks in relation to these holistic approaches. The notorious blindness of technological development to indigenous cultures creates a viscous cycle wherein local actors become increasingly suspicious of development agencies (often refusing to engage with them at all) while development agencies become more and more disconnected from the demands for recognition coming from indigenous communities.

III.6 Privacy, Harm, and Libel

Cyber-security are intrinsically tied to new forms of malice and the capacity for people to use ICTs to provoke real, symbolic, and/or moral harm deliberately. Such harm can is the result of an absence of thorough reflection on the unintended consequences of a person's cyber-behaviour in the way in which it touches on the loaded questions of hate speech, libel, slander, obscenity, cyber-bullying, cyber-vandalism, and harassment. On one hand, “malice” can be politically directed and used as a critical tool with which to deconstruct and denude oppressive power. On the other hand, it can become an oppressive power which can marginalize peoples, tarnish their well-being, and inflict trauma. What therefore constitutes malice? What are its repercussions in inter-personal, social, and political cyber-contexts? More importantly, do the technologies that comprise the information society facilitate harmful behaviours? Do they allow people to engage in new forms of harm and, indeed, act in a more harmful way than before?

One fundamental guideline in thinking about “malice” in the digital world is through the optic of privacy violation, libel, and defamation (which are all intrusions in one way or another). Although the cyber-privacy act (2009-2010)[74] indicates a step in the right direction, as many critics have noted it is simply not specific enough. It just creates a clause wherein users whose personal information has been hacked or unfairly used by others may ask websites to remove their information. But in many ways such a demand comes too little too late. The mere act of surfing the net is nothing short of a constant exercise in the loss of privacy. Users of the internet do not know how many trails of information have been left by them.

Privacy violations and defamation are nothing new. However, the digital community creates new forms of harm ranging from trolling to cyber-stalking which have a range of unexamined ethical consequences. The entire internet community can indulge in defamation and bear witness to it in real time. Hate campaigns can be generated within an instant and attract the attention of a global cast of followers. Young people are particularly vulnerable as they are often not prepared for the pain and humiliation that comes from on-line defamation by their peers. They are both less-experienced with the harshness of the world and amongst the greater uses of social media. Social media, moreover, has become a chosen means for pedophiles and other sex offenders to seek out their next victims. Reputations and job prospects have also been destroyed by on line defamation and scandal. Suffice it to say that the repercussions of cyber-libel and privacy

[74] See http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.5108:

violation can have deep impacts on people's feelings of security, well-being, and integrity and have been known to lead to suicide and self-harm.

A 2012 New Zealand Ministerial Briefing telescoped the new risks that emerge from "Harmful Digital Communications", the relative lack of understanding of what constitutes such communication, and the concurrent lack of strong regulatory measures. According to the report, while "global internet companies such as Google and Facebook provide users with tools to report content which is offensive and which breaks their terms of use … as yet there is no independent means of assessing how frequently these tools are used and to what effect. The lack of consistent measurement and reporting of incidents involving communication abuses presents a challenge for policy makers..."[75]

Self-regulatory paradigms and various incarnations of NetSafe are simply not capable of securing the cyber-world (a world whose integrity is bound in its non-regulated status). Moreover, it is not in the interest of internet providers and web players to enforce regulation since the internet provides their subsistence and depends on the constant information exchange which is impossible to fully track (for example, over 60 hours of video are uploaded every minute on YouTube).

The democratic ethos of the digital world is constructed in fierce opposition to censorship. Yet, as incidences of digital harm attest, this public sphere cannot auto-gestate nor auto-regulate. Twitter's policy on harmful materials, which by and large reflects the attitudes of other platforms, reveals the ethical difficulties of the regulation of digital harm:

> We reserve the right at all times *(but will not have an obligation)* to remove or refuse to distribute any Content on the Services, to suspend or terminate users, and to reclaim usernames without liability to you. We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.[76]

In these regulations, public outrage apparently has its limits. It is the platform itself which "reserves the right" to do what it desires with its content. The implicit norms and "ethics" of the company are thus clouded by a lack of clarity, not only about what digital harm regulation should be but also who should be enforcing it. The neutrality of the digital state resents normativity, but normativity seems inevitably necessary when a simple tweet can destabilize a livelihood. While the internet gives great control to its users, there is certainly no mechanism currently available that insures that the content which they control abides by any ethical criteria. One can easily imagine a state of digital tribalism where online communities decide on the character of their contents to the detriment of other communities who are engaged in similar behaviour. The ethical dilemma remains how to envision a digital world of free exchange, but one which simultaneously does not enable digital harm. Journalist and technology critic, Denis O'Reilly, however, still believes that the problem is people and that "the fight for an ethical Internet may be a lost cause, if only because people's moral compasses appear to be irreparably

[75] The Law Commission of New Zealand, 2012, Ministerial Briefing Paper: Harmful digital communications – the adequacy of the current sanctions and remedies, See http://www.lawcom.govt.nz/sites/default/files/ministerial_briefing_-_harmful_digital_communications.pdf, p. 30

[76] See <www.support.twitter.com/groups/33-report-abuse-or-policy-violations#topic_166 >.

damaged."[77] The challenge, thus, may have little to do with the codification of a discipline called info-ethics. It might simply be a question of good old fashioned civics.

III.7 Cyber-Bullying

The terrain of the cyber world can be rough and unfriendly. It can be seen as a virtual state of techno-nature where actors can inflict harm in relatively unregulated atmosphere. Seemingly lawless and vast, individuals freely and at times malevolently "live" in the cyberworld. In other words, virtual society has yet to become a civil virtual society. Bullying and related forms of crime seethe through the flows of the virtual world. The question remains whether the relative anonymity, scale, and reach of virtual life makes people more prone to such forms of harm and whether the effects are potentially more damaging and "unregulated" than similar phenomena in the "real" world. And while we may be virtual actors, safe behind our screens, our feelings and sentiments remain, nonetheless, the same.

One could argue that there are stricter boundaries for traditional bullying in the physical world. The first obvious boundary is shown by the fact that victims can face their aggressors and marshal support from their friends, communities, and institutions to defend themselves in a "physical form." The lack of face-to-face confrontation in the cyber-world may thus encourage greater ferocity and daringness and conversely greater humiliation for the victim.

Several high profile and tragic cases have brought cyberbullying into the spotlight and have intensified calls for ethical frames and regulation. Tyler Clemente committed suicide in 2010 after his roommate, using a webcam, posted online private moments between Clemente and another man. The suicides of Ryan Hallegan (2003), Megan Meir (2006), and Phoebe Prince (2010) were all directly linked to various forms that cyberbullying took via text messages and Facebook. After their respective deaths, the cyber-world continued to swarm with defamatory and vulgar remarks concerning their lives and deaths. In all three cases, the tormentors faced prosecution and brought international attention to the cyberbullying epidemic, resulting in the drafting of several new forms of cyber-bullying legislation, among them "Phoebe's Law" in New York State. [78] However, the legislation always appears to emerge after the fact and there is no clear criteria with which to identify cyber-bullying until it is too late. Moreover, it is virtually impossible to track.[79]

Most cyberbullying legislation aims to protect young people. Although no federal law exists in the United States, individual states either have a law, policy or both in place to protect victims of cyberbullying. There has also been a great push for schools to take on greater responsibility to prevent cyberbullying and to protect their students. In June 2012, "the New York State Assembly approved legislation to protect New York schoolchildren from the growing scourge of cyberbullying. The legislation builds on Assembly Member Daniel O'Donnell's anti-bullying legislation, the Dignity for All Students Act, which was signed into law in 2010. The addition of cyberbullying will make New York's anti-bullying protections among the most comprehensive in

[77] O'Reilly, D., 2010, The internet and the death of ethics, *CNET,* see http://news.cnet.com/8301-13880_3-20018998-68.html

[78] See http://www.belfasttelegraph.co.uk/news/local-national/irish-teenager-phoebe-princes-suicide-outrage-sparks-mass-us-backlash-14772114.html

[79] Ford, Z., 2012, New York Legislature Passes Cyberbullying Protections, *Think Progress,* http://thinkprogress.org/lgbt/2012/06/19/502551/new-york-legislature-passes-cyberbullying-protections/?mobile=nc

the nation."[80] The European Union has also launched an educational campaign directed at teens and young adults throughout Europe in effort to empower and educate victims of cyberbullying. Similar efforts are being launched globally. Beyond protecting victims, greater effort is being made to ensure that justice is served through the prosecution and punishment of attackers (as seen in the Clemente and Prince cases).

Unfortunately though, as David O'Reilly remarked, "some people see the Internet as a mirror held up to our culture. If it is, the mirror shows us in an unflattering light. From newsroom staffers caught off guard on camera in a private moment gone viral on YouTube to dorm room trysts streamed live online, people have no shame about the despicable content they post on the Web. Respect and courtesy are quaint, outdated notions to these Internet citizens."[81] In addition, Antonio Marturano confirms that the very nature of communication on Facebook makes the potential for online malice high. As he explains the technology is not neutral: "More challenging is the sense in which we talk about malice in the second sense, that is, when malice stems out from human interaction through computers. In many cases, it is the way in which an Internet website or platform is designed that allows for a higher or lower level of malice in human to human or website-to human interplay."[82] Moreover, in a cultural context driven by reality television, scandal, and explicit public behaviour, people have also become accustomed to the persistence of "shaming" in the media and infosphere. Simultaneously, traditional notions of shame, honor, and propriety have radically shifted and indeed, as seen by the proliferation of celebrity sex-tapes, "exposure" and "embarrassment" are means of attaining fame.

The ethical response to cyber-bullying must be at once social, systemic and technical. It will therefore be essential to create the conditions for virtuous modes of cyber-citizenship which are then strengthened by software and internet platforms that make it, not easier but more, difficult to be malicious towards others.

III.8 Identity-Theft

The information society is a society of simulation and exhibitionism. It is also a virtual plane where misrecognition abounds. Indeed one person can become another through a bit of manipulation, unlocking passwords, and manipulating passports, credit cards and biodata. Insofar as all information exchanged on the internet is capable of being stored on servers for years, people risk not only losing their identity "now," but in the future as well. It should thus come as no surprise that the dead live on in multiple ways in the information society. The process, known as "ghosting," allows 2.5 million people a year to access the social security numbers and credit cards of others, and even create Facebook pages. Cornell University professor, Jon Kleinberg, further suggests, "when you are doing stuff online, you should behave as if you're doing it in public – because increasingly, it is."[83] The ethical implications of the loss of identity are enormous, and privacy should no longer be treated as a personal or private affair. Privacy cannot be reduced to what one does "behind closed doors". In effect, privacy is a rather

[80] See http://assembly.state.ny.us/mem/Daniel-J-O%27Donnell/story/48628/
[81] O'Reilly, D. 2010.
[82] Marturano, A., 2011, Harm and malice in Cyber-Space, WSIS Forum 2011, see http://findpdf.net/pdf-viewer/Harm-and-malice-in-cyberspace-the-Facebook-Case.html
[83] Lohr, S., 2010, How privacy vanishes on-line, *The New York Times,* see http://www.nytimes.com/2010/03/17/technology/17privacy.html

public discursive and technological nexus. As Harold Abelson explains, “Personal privacy is no longer an individual thing.”[84]

Internet users now perform the most mundane real world tasks virtually. eCommerce, online banking, social networking, and even dating have all been neatly replicated in the cyber-world. Increasingly companies are also choosing to do more business online. Their reasons vary from being more “green” and paperless to seeking greater efficiency. Although internet users may take every precaution to hide their internet footprints, internet searches, contacts, “links,” or “friends” on social networking sites, search histories, cookies, and conventional username/passwords all provide pieces of a puzzle that third parties can patch together. An internet user’s larger network may further erode their privacy: “You may not disclose personal information, but your online friends and colleagues may do it for you, referring to your school or employer, gender, location, and interests. Patterns of social communication are revealing.”[85] In addition, as is now well known, the privacy settings on pages on Facebook are never as “private” as their subscribers are led to believe. An entire subterranean industry of personal information exchange by platforms and sites rumbles on underneath the virtual world. Pleas for greater transparency about corporate policy and regularization of data exchange mechanisms are growing more visible, but the relevant industry players are as yet to be fully unlocked by policy makers and stakeholders.

Whether through the sophisticated use of algorithms, data mining software, phishing, hacking or creating fake profiles, researchers, scientists and thieves alike can monitor patterns of behavior on the net, and can piece together relevant information from multiple sites to create a biographical picture of users and patterns of movement with the ultimate goal of committing identity fraud.

Social media sites pose the greatest privacy risks for their users: “Social media sites generate revenue with targeted advertising, based on personal information. As such, they encourage registered users to provide as much information as possible. With limited government oversight, industry standards or incentives to educate users on security, privacy and identity protection, users are exposed to identity theft and fraud”.[86] Those who use “public” profiles are most vulnerable to attack, although no user is entirely safe from the potential threat of fraud. The power of computers to identify people from social patterns alone was demonstrated in 2008 in a study by the same pair of researchers that cracked Netflix’s anonymous database (Vitaly Shmatikov, an associate professor of computer science at the University of Texas, and Arvind Narayanan, now a researcher at Stanford University).[87] By examining correlations between various online accounts, the scientists showed that they could identify more than 30 percent of the users of both Twitter, the microblogging service, and Flickr, an online photo-sharing service, even though the accounts had been stripped of identifying information like account names and e-mail addresses.[88] Even more unnerving to privacy advocates is the work of two researchers from Carnegie Mellon University. In a 2011 paper, Alessandro Acquisti and Ralph Gross reported that they could accurately predict the full, nine-digit Social Security numbers for 8.5 percent of the people born in the United States between 1989 and 2003 – nearly five million individuals. [89]

[84] Ibid.,
[85] Ibid.,
[86] See http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx
[87] Lohr, S., 2010.
[88] Ibid.,
[89] Ibid.,

Rapid changes in the cyber-world and in technologies have made privacy regulations and policies difficult to implement. “In the new technology boom, individuals and technology managers must change their attitudes and behaviours and consider precautionary solutions when using new technology.”[90] But who will be the instigators of such changes and codify the appropriate cyber-ethics that functions as its framework? This remains the pressing task of ethicists and policy-makers alike.

III.9 Genetic Data and Cyber-Genomics

The advent of human genome research has added a further dimension to the breach of privacy – the breach of genetic privacy. While internet-based groups have been therapeutic in enabling people suffering from various conditions or illnesses to locate other people with similar experiences, the relationship of ICTs to illness and the human body become ever complicated by the threats of genetic screening and the digital abuses of genomics. Insofar as genetic data is not simply typical private data (such as credit card numbers, passwords, or consumer choices), its misuse poses a whole new set of dangers. These range from genetic screening to virus creation. Rendering the situation more sensitive is the fact that medical and genetic information is among the most non-secure of information stored in the information society. It is primarily electronic and is kept by hospitals whose databases and digital files can easily be hacked. Hence, while research on genetic information may be vital in warding off disease and epidemics, its circulation could also lead to new forms of personal or collective bio-terrorism. At a more individual level, screening mechanisms could serve to shame, discriminate, and alienate. From genetic spying to genetic data commercialization, in the world of cyber-genomics, medical data may be harder to keep private.

Regulation and ethical policy-based mechanisms have yet to meet the challenges of genetic data breaches. Indeed as Jaylene Stewart and Diem Thy Tran observe, “currently, there are only a handful of federal legislations that address privacy rights on the use of genetic information. ... Current regulations are not enough to protect our genetic privacy against misuse by employers and insurers. Most of these regulations are broad-based legislations that protect only certain classes of people such as federal employees or members of a group policy plan. This evidently creates loopholes for employers and insurers to get around these laws.”[91] More importantly, “privacy” and “genetic privacy” have yet to be adequately recognized as rights in the information society. Nonetheless, there can be no doubt about the fact that "my genes" constitute "my property" – is there nothing more that is “my own” than my genes?

However, the therapeutic dimensions of sharing information about illnesses are also enriched by genomics and “bionetworking” and the appearance of new forms of bio-citizenship and bio-solidarity. Denisa Kera argues that the political repercussions of bio-networking and “genetic alliances” could serve to redefine potentially classical visions of what social institutions are and should be:

[90] Hedayati, A., 2012, An analysis of identity theft: motives, fraud, techniques and prevention, *Journal of Law and Conflict Resolution* Vol. 4(1), pp. 1-12, see http://www.academicjournals.org/jlcr/PDF/pdf%202012/Jan/Hedayati.pdf

[91] Stewart, J., and Tran, D.T., 2007, The ethics of genetic screening, see http://www.ethicapublishing.com/3CH1.htm

Bionetworking interfaces connect scientific facts with social and political structures and actors on a very personal level, redefining our identities and traditional institutions like the family. People sharing personal aspects of their "objective" identity, such as DNA or other biodata, connect online to redefine who their most valuable relations are, making their sense of belonging a game of chance. Together with the real-time data-logging of life indicators, such as temperature, heart rate, heart rhythm, and blood oxygen saturation, biodata can be used for different types of interactions from dating to games, from health services to genealogy, and different forms of collaborative entertainment around new utopian and dystopian communities. We can imagine mobile applications enabling us to meet people with the same rhythm of heartbeat or similar DNA in the subway, so that we can create temporary, ad hoc relations with such "familiar strangers", resulting in a collective heartbeat in a certain part of a city. Dystopian and eugenic societies based on a particular understanding as to what sort of DNA or biodata are the pre-requisites for a peaceful and valuable community are also possible outcomes. The social and political consequences of organising our patterns of interaction on the basis of sharing our DNA or other biodata are already apparent in existing services, which contain hints of both utopian and dystopian versions of the future.[92]

Bio-networking can thus open the way to a new cosmopolitanism and bio-consciousness. Bio-networking will potentially have important effects on social and medical innovation. Most importantly, in redefining the parameters of what a community is, it also functions as the foundation for new ethical paradigms that surpass the burdensome weight of normative notions of the good and the virtuous.

[92] Kera, D., 2010, Bionetworking over DNA and biosocial interfaces: Connecting Policy and Design, Genomics, Science, and Policy, Vol. 6., No. 1, see http://www.hss.ed.ac.uk/genomics/documents/Kerafinal.pdf, p. 53

IV. HUMAN, POST-HUMAN, AND TRANS-HUMAN DIMENSIONS

Any reflection on the ethics of the information society is a reflection on the changing face of the ethics of science and technology. In a general sense, the ethics of science and technology concern the responsibilities of scientists and researchers, the constraints within which they function, and how they bring ethical considerations to bear on their research and the technologies that they develop. However, as a domain of inquiry, the ethics of science and technology also concerns how advances in technology radically alter the categories of the human, the social, interacting with others, and, from a social neuro-scientific and cognitive psychological perspective, the body and the brain. The information society has changed they way that human beings behave as a species.

For instance, Facebook and other forms of social media have created new forms of virtual community, but they have also redefined classical visions of society. These networks, while allowing many people to accumulate millions of connections and “friends”, have also given rise to new forms of solitude. Emails have replaced the written letter. In doing so, they have not only recalibrated the grammar and speed with which people communicate, but have also destroyed a hallowed and archival form of communication. In lieu of assembling the “collected letters" of so and so, there will be a shift to publishing anthologies of the person's collected emails. As Roland Barthes famously noted, there is indeed something strange about tearing up the photos of a loved one and throwing them in the garbage. For Barthes, this was simply because most people assume an ontological identification between the representation and the person represented in the image. One rarely says “this is a photo of my Mom,” but rather “this is my Mom”. However, as many people have noticed, it is indeed much easier to delete a photo of a loved one and send it to the trash can on a computer. While one would be tempted to resurrect the category of “aura” to explain this ease of action, there is no doubt that digital technologies carry with them a certain disposibility that did not characterize the previously “analog world”. Speaking of photos, it is further interesting to note that the photo album has more or less ceased to exist. It can now be asked whether one will pass down one’s hard drive to one’s children to preserve familial memories. Memories and experience are transformed into “items” to be quickly consumed, rather than “treasured” or “preserved”. Moreover, how can it be said that a smart phone or a computer is simply a tool when photos, diaries, works, oeuvres, and the most intimate of data are all to be found on these devices. Computer crashes or thefts have visceral effects on the subjects who experience them. They have introduced a new type of panic into the information society, one where one “loses everything” (and hence, the rise of interest in “clouds” and “cloud computing”). Data, information, and hate speech, like the information society itself, are typified by their transitory natures.

And in the world of future, it is said that, on the one hand, the post-human cyborg to come will be the preeminent creature of the information society. A nano-bio-info-cognitive (NBIC) structure, the post-human cyborg will no longer need laptops, phones, or any such devices, as these mechanisms will be built into his, her or its organism. The cyborg to come will push the concept of the human being well beyond the determinism of race, gender, and identity *tout court,* opening up a new space of emancipation. While technology may be made by humans, the very possibility of the existence of the cyborg calls into question not only the stable limits between humans and machine, but the very notion of human beings and their ethical life. On the other hand, the technological advances that create the new race of cyborgs may also create a sub-race of non-cyborg proles, and open the possibility of greater bio-technological enslavement and domestication.

Yet, advocates of the singularity, like José Cordeiro for instance, insist that the world is only half-built and its beauty only half-achieved. Cordeiro's embrace of the singularity emerges from nothing short of the simple desire to beat back death. He remains convinced that "Humans will reach physical immortality via two fronts: biological replacement and rejuvenation as well as computational uploading and virtual reality …". For Cordeiro, human beings should not count on nature to help either. The heuristic he invokes is neither evolutionary nor dialectically bound to nature. Nature and biological evolution simply move too slow.[93] While death may be considered "bad" and an experience to struggle against, one might want to reflect on the implications of immortality. Beyond the obvious question of human demographics, can one envisage a world where one's parents never die? Can one imagine a world where one could simply develop through various uploading procedures? While one would never have to settle on one career or make irrevocable choices, immortality would certainly have radical implications not only on concepts of time, finitude, and labor, but also on notions such as potential, hope, spirit, aspiration, and success.

In May 2010, a scientist at the University of Reading became the first human infected with a computer virus. Dr. Mark Gasson had an RFID chip implanted into his left hand in 2009 which allowed him to clear university security, be tracked, and use his cellular phone. However, Gaston infected his own implant:

> By infecting my own implant with a computer virus we have demonstrated how advanced these technologies are becoming and also had a glimpse at the problems of tomorrow. Much like people with medical implants, after a year of having the implant, I very much feel that it is part of my body. While it is exciting to be the first person to become infected by a computer virus in this way, I found it a surprisingly violating experience because the implant is so intimately connected to me but the situation is potentially out of my control. I believe it is necessary to acknowledge that our next evolutionary step may well mean that we all become part machine as we look to enhance ourselves. Indeed we may find that there are significant social pressures to have implantable technologies, either because it becomes as much of a social norm as say mobile phones, or because we'll be disadvantaged if we do not. However we must be mindful of the new threats this step brings.[94]

One could continue *ad nauseaum* with an inventory of developments ushered in by the changing face of the information society, from the banal to the apocalyptic. However, what all of these examples illustrate is the increasing destabilization of our notions of nature and the natural. The ethical question is whether such a destabilization also means rethinking the normative and "natural" frames that we have used to inform our values systems and beliefs about the world. Is the information society simply the next step in the long history of humanity and its relationship to techné? Or is it a radical break which renders uncertain all of the values and ethical structures that have guided modernity? Is the aftermath of the modern also an ethical threshold pushing us into a new world where we will need not only to reflect on how we behave with others but also with robots? Far from being the mere stuff of science fiction, Hollywood blockbuster, or "war games," these questions necessitate an interrogation into the ethical ramifications of the new "interface," with a view to thinking about how the information society alters well-being, but also being itself.

[93] See http://www.european-futurists.org/wEnglisch/aktuelles/2009_09_20_18296221_meldung.php
[94] See http://www.reading.ac.uk/sse/about/news/sse-newsarticle-2010-05-26.aspx

IV.1 From "Society" to "Network"

Classical social theorists, from Durkheim to Tönnies to Simmel, strained to apprehend the contours and necessary conditions for that taken for granted organism known as society. At the risk of oversimplification, this tradition not only assumed that there was something called the "social," but that it had a series of trans-historical characteristics which could be analyzed and strengthened in order to make society more robust. Among other things, it was defined by interpersonal interactions that had strict content and form. It was driven by a series of relatively stable political and symbolic institutions that functioned as its central loci (such as the state, the family, the church, and supra-individual forces). Individuals were formed by their dialectical relationship with the larger transcendent structure of the social order. Affinities were developed either within communitarian structures or mediated through symbolic political regimes. Societies evolved, but had a rather static character and constructed a series of conventional mechanisms for dealing with conflict and antagonism (such as juridico-legal processes, elections, and class struggle). Societies were anthropocentric constructions; their larger historical goal was the forging of greater solidarity and flourishing amongst their respective members.

The 20th century was important for many reasons. From a sociological perspective, it will be remembered as the epoch in which information and media eclipsed and perverted the classical understanding of the social, and where the forces of the global ushered in a post-national, destabilized, digital world dominated by information providers and purveyors. Information, not the individual, slowly became the central unit of the global (dis)order. At the same time, it bombarded and over-saturated the newly formed "masses", but also allowed the creation of new micro-communities whose affinities emerged from beyond the parameters of what was once called the social. Things appeared limitless, but also ominous. In response to the hegemony of information over society, as early as 1967, Guy Debord was theorizing about the degradation of society into information and "spectacle." For Debord, "images detached from every aspect of life merge into a common stream in which the unity of that life can no longer be recovered. Fragmented views of reality regroup themselves into a new unity as a separate pseudo-world that can only be looked at. The specialization of images of the world evolves into a world of autonomized images where even the deceivers are deceived. The spectacle is a concrete inversion of life, an autonomous movement of the nonliving."[95] As the 20th century came to a close, sociologist and media theorist Jean Baudrillard deemed the spectacle completed. He thus asked:

> Do modern societies correspond to a process of socialization or to one of progressive desocialization? … If the social is formed out of abstract instances which have laid down one after the other on the ruins of the symbolic and ceremonial edifice of former societies that these institutions (*which have sign-posted the advance of the social*) produce more and more of them … Media, *all* media, information, *all* information, act in two directions: outwardly they produce more of the social, inwardly they neutralize social relations and the social itself. But then, if the social is both destroyed by what produces it (the media, information) and reabsorbed by what it produces (the masses), it follows that its definition is empty, and that this term which serves as a universal alibi for every discourse, no longer analyses anything, no longer designates anything. Not only is it superfluous and useless – wherever it appears it conceals something else; defiance, death, seduction, ritual, repetition – it conceals that it is only abstraction and residue, or even simply an *effect* of the social, a simulation and illusion.[96]

[95] Debord, G., 1994, *The Society of the Spectacle*, (trans. Donald Nicholson-Smith), New York: Zone Books, p. 12

[96] Baudrillard, J., 2007, *In the Shadow of the Silent Majorities*, New York, Semiotext(e), pp. 65-66

However, as we entered the 21st century, and talk of the burgeoning "information society" slowly entered the public discourse, many theorists shed the dystopian visions of the previous generation of thinkers and writers. They assailed them for ever believing that there was such a thing called "society," let alone one that was static and not defined by dynamic transformations that were primarily technological or information based in essence. Moreover, there was no need to think that the classical vision of the "social" was any more ethical than new paradigms of aggregation that were mediated by technology and information. Perhaps, "society," was a stultifying concept. Perhaps it should be replaced by or merged with a more rhizomatic and fluid notion of "networks" which are non-hierarchical, ever expansive, nomadic, and creative in nature.

Of particular salience was Manuel Castell's thesis concerning the "network society", or world of flows, where social, political, and personal capital are not socially forged, but negotiated through the individual's implication in the global as a network and his or her own macro-networks and will to communicate. Castells reminds us, however, that it is not technology and information that have created the transformations of our society. Neither form the necessary conditions for new global and communal arrangements. For Castells, emerging technologies still remain bound to traditional modes of society which they enhance and shape. However, whereas networks were once previously "private," they now function as the shared substrate of the global world. The network society, for Castells, is not a rupture but rather is an overcoming of historical limits. It does, however, include a series of key transformations:

- *the transformation of sociability:* The network society is a hypersocial society, not a society of isolation. People, by and large, do not fake their identity in the Internet, except for some teenagers experimenting with their lives. People fold the technology into their lives, link up virtual reality and real virtuality; they live in various technological forms of communication, articulating them as they need it.

- *the transformation of the realm of communications, including the media*: While interpersonal communication is a private relationship, shaped by the actors of the interaction, media communication systems sets the relationship between the institutions and organizations of society and people at large, not as individuals, but as a collective receiver of information, even if ultimately information is processed by each individual according to her personal characteristics.

- *self-directed mass communication:* The explosion of blogs, vlogs, podding, streaming, and other forms of interactive, computer to computer communication sets up a new system of global, horizontal communication networks that, for the first time in history, allow people to communicate with each other without going through the channels set up by the institutions of society for socialized communication.

- *politics is largely dependent on the public space of socialized communication, the political process is transformed under the conditions of the culture of real virtuality*: Political opinions, and political behavior, are formed in the space of communication. Not that whatever is said in this space determines what people think or do. In fact, the theory of the interactive audience, supported by research across cultures, has determined that receivers of messages process these messages in their own terns. Thus, we are not in an Orwellian universe, but in a world of diversified messages, recombining themselves in the electronic hypertext, and processed by minds with increasingly autonomous sources of information.

- *the rise of the network state*: It is not the result of technological change, but the response to the structural contradiction between a global system and a national state. However, globalization is the form that takes the diffusion of the network society in its planetary reach, and new communication and transportation technologies provide the necessary infrastructure for the process of globalization. The transition from the nation-state to the network state is an organizational and political process prompted by

the transformation of political management, representation and domination in the conditions of the network society.[97]

Castells remains convinced that, although power is also a network phenomenon, the advent of the network society is the next phase in the movement towards direct democracy. But this possibility of course depends on policy-makers who share the same fundamental vision about the network society.

Moving well beyond Castells are the proponents of Actor-Network Theory (ANT) who rally against the "social" in the name of the network. Most prominently represented by Bruno Latour, ANT theorizes a world of radical heterogeneity where information and the technological no longer compromise tools or material objects, but are ambient actors that interact with human actors in aggregate formations and compositions that affect decision-making, political agency, and the very durability of "social bonds." Human beings, as human agents, are nodes in a larger infinite structure of networks and networks within networks. Our respective agency is transformed depending on the nodal coordinate that we occupy at any given moment – the network, in other words, is that which informs, decides on, and distributes human activity. The network, moreover, is not simply a structural apparatus. On the contrary, it creates the grounds for new modes of inquiry, interaction, questioning, and knowledge. The network does not ask what the world should be, but rather how it works, how it evolves, and how its properties (whether natural or technological) increase or decrease. In other words, in a social, geographical, or mechanical network, the question is not one of integrity or identity, but rather of gradients of speed and slowness, abundance and entropy. Information societies operate more like networks than do "societies". For Latour, this is a welcome historical development:

> A network notion implies a deeply different social theory: it has no a priori order relation; it is not tied to the axiological myth of a top and of a bottom of society; it makes absolutely no assumption whether a specific locus is macro- or micro- and does not modify the tools to study the element "a" or the element "b"; thus, it has no difficulty in following the transformation of a poorly connected element into a highly connected one and back. A network notion is ideally suited to follow the change of scales since it does not require the analyst to partition her world with any priori scale. The scale, that is, the type, number and topography of connections is left to the actors themselves. The notion of network allows us to lift the tyranny of social theorists and to regain some margin of manoeuvers between the ingredients of society - its vertical space, its hierarchy, its layering, its macro scale, its wholeness, its overarching character - and how these features are achieved and which stuff they are made of. Instead of having to choose between the local and the global view, the notion of network allows us to think of a global entity - a highly connected one - which remains nevertheless continuously local ... Instead of opposing the individual level to the mass, or the agency to the structure, we simply follow how a given element becomes strategic through the number of connections it commands and how does it lose its importance when losing its connections.[98]

However, the fetishisation of the connection over the bond, network-freedom over social norm, and a scalar information topography over an intimate communicative geography, is not without its consequences. Indeed, for many social theorists, the supplanting of the "social" by the "network" that constitutes life in the information society can have potentially devastating effects on fundamental human needs and desires. Not all share the optimism of Castells and Latour, particularly in regards the hegemony of social media and personal networks to the detriment of social relations and personal ties.

---

[97] Castells, M., 2005, The Network Society: From Knowledge to Policy, in eds. M. Castells & G. Cardoso, *The Network Society: From Knowledge to Policy,* Washington: Center for TransAtlantic Relations, pp. 11-16

[98] Latour, B., 1990, On actor-network theory: a few clarifications plus more than a few complications, see http://www.bruno-latour.fr/sites/default/files/P-67%20ACTOR-NETWORK.pdf, p. 6

IV.2 Social Media: The End of Friendship

As a form of moral and philosophical inquiry, the central issue of ethics concerns how one should behave in relation to others. Thus, the field of ethical interrogation is inevitably bound to the examination of notions of love, friendship, solidarity, empathy, and reciprocity. While these modes of relating have never been stable, the information society has, undoubtedly, altered their structures, the values laden within them, and their value.. Networks and network societies fundamentally alter the way human beings relate to others. In human beings becoming "nodes" in a larger information grid, one must ask if something is sacrificed from the perspective of interpersonal life and interpersonal ethics. Suffice it to say, the rise of social media as the predominant means –at least in certain circles – of interpersonal communication (and a quasi-necessity in certain sectors) has produced, deep fears about the changing face of intimacy, friendship, and human relations. Unlike Castells and Latour, some theorists remain nostalgic for a simpler time where shared experience was perceived to be more tactile, visceral, and "real."
Two theses dominate in anti-social media scholarship: social media creates new modes of isolation and actually separates human beings while appearing to connect them; and social media is the ultimate reflection of a new culture of narcissism

According to media and technology theorist Sherry Turkle, society should remain enthusiastic about new technologies and social media, but simultaneously be wary of the mass info-techno-malasie that they have engendered over the past years. For Turkle, social media creates a domain in which human beings find themselves "alone together," unable to relate to others and to ourselves. We no longer relate, but we construct selves that are reduced to modes editing, linking, deleting, and changing profiles. Above all, for Turkle, social media is not a place where we engage in conversation, where we learn and learn to listen. Constant connectivity has destroyed an essential dimension of human growth: the capacity to be alone. Hence, whole "technology reshapes the landscapes of our emotional lives". Turkle exhorts us to ask, "is [technology] offering the lives we want to lead?"[99] Essential in such a reshaping is precisely how "we look to the network to defend us against loneliness even as we use it to control the intensity of our communications. Technology makes it easy to communicate when we want to and disengage at will …whether you are online or not, it easy for people to end up unsure if they are closer together or farther apart."[100] While human beings therefore connect to feel more full, the result is emptiness and the inability to interact with other people in any real way and inability to be alone. The creatures of the information society are fragile entities shot through by a solitude that they do not have the means to confront.

Philosopher Roger Scruton is more acerbic in his critique of the information society. For him, the decline of contemporary societies co-exists with the new habit of "hiding behind the screen." Facebook, texting, skyping, and the like have, furthermore, according to Scruton, destroyed the possibility of real friendship which was always about "action" and "affection". Instead, these applications have created a new breed of citizens who are not *attentive* to one another, who do not *know themselves,* and who find themselves addicted to screen-relating yet are lost in the world of affect, body, gesture, and intimacy. Social networks and network society are nothing short of "parasitic on the real relationships they foster, and which they alter in large part by encouraging people to put themselves on display, and in turn to become voyeurs of the displays of others."[101] The ethical, social and bodily implications of the information society can be

[99] Turkle, S., 2012, *Alone Together: Why We Expect More from Technology and less from Each Other*, New York: Basic Books, p. xlix
[100] Ibid., 14
[101] Scruton, R., 2010, Hiding Behind the Screen, *The New Atlantis,* Summer 2010, p. 48

potentially devastating to the emotional core of what will perhaps one day be looked back on as the "human." According to Scruton, one day there may not be any "real human children" left:

> Perhaps we can survive in a world of virtual relations; but it is not a world into which children can easily enter, except as intruders. Avatars may reproduce on the screen: but they will not fill the world with real human children. And the cyber-parents of these avatar-children, deprived of all that makes people grow as moral beings – of risk, embarrassment, suffering, and love – will shrink to mere points of view, on a world in which they do not really occur.[102]

While it may be tempting for some to dismiss Turkle and Scruton as conservative reactionaries who simply need to get hip with the times, it is interesting to note that the cognitive and social neuroscience communities more or less confirm their findings. Social neuroscientist and psychologist, John Cacioppo, argues that loneliness is among the greatest emotional scourges of hyper-modern civilization. Human beings find themselves experiencing an epidemic of solitude where the fundamental human need to connect with others has been perverted, let alone, effaced, and results in a new acute forms of social isolation in a radically "social" world. As for social media, he also notes that it does little to help -- when others use online connections to substitute for face-to-face relations, they become lonelier and more depressed. Lonely people are likely to use the Internet as a crutch, the nonlonely as a type of leverage. So, according to Cacioppo, "the rich get richer and the poor get poorer."[103] Years of empirical study further offer evidence for Cacioppo's arguments. In a 2010 study, he and a group of Harvard and University of San Diego researchers found that not only is loneliness more prevalent, but it is also contagious. "Using data from a longitudinal study in small-town Framingham, Massachusetts, they charted a social network of more than 12,000 ties among 5,124 people, determining that having one lonely friend raised one's chance of loneliness by 40 to 65 percent. A lonely friend-of-a-friend raised the chance by 14 to 36 percent. By the third degree of separation, the increased likelihood was slighter still, and beyond that the effect disappeared."[104] More recently, in his study on loneliness, Cacioppo also observed that "Given the importance of social connection to our species, then, it is all the more troubling that, at any given time, roughly 20% of individuals – that would be 60 million people in the US alone – feel sufficiently isolated for it to be a major source of unhappiness in their lives."[105] What Cacioppo's findings demonstrate is how social media, the information society, and the replacement of real social connection with networks creates heightened forms of social exclusion and exacerbates already existing social dividing lines. He too concludes that Facebook makes people lonelier than they already are. While social media provides something of a "safe haven" for those who feel unwanted, it does little to battle the real causes of isolation; it is "a little bit like being hungry and eating celery, in that it feels good for a moment, but it's not actually nutritious, it's not satisfying the underlying need."[106] In short, the information society is not necessarily good for people's psychological and physical health. The ethics of the information society must find a means of counterbalancing social media's capacity to further divide people from others and themselves. It is also not clear that, in light of these potentially destructive trends, we can still claim that the technology is neutral.

Heightened narcissism has historically functioned as one means of coping with loneliness. For all its strengthened social connectivity, the information society has also given rise to new forms

---

[102] Ibid., p. 60
[103] See http://magazine.uchicago.edu/1012/features/the-nature-of-loneliness.shtml
[104] Ibid.,
[105] Cacioppo, J. 2009, *Loneliness: Human Nature and the Need for Social Connection*, New York: Norton (2009), p. 6
[106] See http://www.prweb.com/releases/loneliness/help/prweb4088414.htm

of narcissism, personal branding, network capital, and consumption of the self and "status." With the new loneliness, this new narcissism has also been identified as an ever growing pathology among young people between the ages of 16 and 35. According to Jean Twenge and W. Keith Campbell, in the US, the information society effectively moves people from the "Me Generation" to the "Look at Me Generation". This has serious ethical consequences:

> People strive to create a "personal brand" (also called "self-branding") Not only are there more narcissists than ever packaging themselves like products to be sold. Ads for financial services proclaim that retirement helps you return to your childhood and pursue your dreams. High School students pummel classmates and then seek attention for their violence by posting YouTube videos of the beating. Although these seem like a random collection of trends, all are rooted in a single underlying shift in American psychology: the relentless rise of narcissism in our culture. Not only are there more narcissists than ever, but non-narcissistic people are seduced by the increasing emphasis on material wealth, physical appearance, celebrity worship, and attention seeking.[107]

For Twenge and Campbell not only will the epidemic grow outside of the borders of America, but will do so through the empire of the information society. Moreover, from an ethics of science and technology perspective they concur that, while beating up fellow students or pupils may not be new, the culture of narcissism coupled with the culture of YouTube (where you can "broadcast yourself") turns this bullying into a wholly different affair.

The motor of the information society is not simply "information," but the cult of narcissism and its derivatives. Social media and networks, for Twenge and Campbell, remain the main drivers of the epidemic. Pastiching Candice Kelly's study, *Generation MySpace: Helping Your Teen Survive Online Adolescence* (2007), they conclude that social media's "ethical" message is: "I must be entertained all the time. If you've got it, flaunt it. Success means being a consumer. Happiness is a Glamorous Adult (with adulthood primarily defined in terms of sexuality)."[108] Twenge, Campbell, and Elise Freedman have also recently conducted an exhaustive empirical study on life-goals and values between generations. They sadly concluded that:

> …the popular view of Millennials as more caring, community oriented, and politically engaged than previous generations is largely incorrect. However, the rate of volunteering – an important community behavior – has increased in today's young people, though likely due to outside forces. Saving the environment, an area purported to be of particular concern to young Millennials, instead showed one of the largest declines. How these attitudes and behaviors will shape the young generation and the country as more Millennials enter adult life remains to be seen.[109]

The narcissism of the network society, however, does not to appear to be in decline. Each new cyber-platform becomes yet another platform for me-directed behaviour. While one could argue that narcissism, as a personality disorder, can exist independent of Facebook or be tamed by strong family and institutional foundations, the more that these foundations become absorbed into the information society the more their critical and corrective capacities are undermined (particularly when each member of the family returns "behind the screen" after having eaten a quick dinner together or separately). Christine Rosen characterizes the shift as epochal in scope: "The Delphic oracle's guidance was *know thyself*. Today, in the world of online social networks,

---

[107] Twenge, J., and Campbell, W.K., 2009, *The Narcissism Epidemic; Living in the Age of Entitlement*, New York: Simon and Schuster, p. 1

[108] Ibid., 108

[109] Twenge, J., Campbell, W.K., and Freeman, E., 2012, Generational Differences in Young Adults' Life Goals, Concern for Others and Civic Orientation: 1966 –2009, *Journal of Personality and Social Psychology*, Vol. 102, No. 5, see http://www.apa.org/pubs/journals/releases/psp-102-5-1045.pdf, p. 1061

the oracle's advice might be *show thyself*."[110] If knowing has given way to showing, and showing does not present itself as a type of knowledge at all, it is important to reflect seriously on the internal contradictions embedded in glorifying the information society as a knowledge society.

IV.3 Attention Economies

Attention is the most prized commodity of the information society wherein to be hailed by the image is indeed to work for it. The spectacle, in other words, reproduces itself through the soliciting our attention and transforming our respective gazes into a site ocular and subjective labor. Simultaneously, the information society allows a person to do many things at one time and demands more of your attention in more places and in more ways. While technology has seemingly enhanced people's capacity to complete a multitude of daily tasks more efficiently, in the process it also reconfigures capacities for sustained reflection, critical thinking, aesthetic appreciation, and "slowness." Multitasking, as it has come to be called, is an obligatory skill in the workplace, in the university, and in the kitchen. "Productivity," the byword of hyper-modern societies, demands that people are able to respond to email, write a report, respond to calls on the cellphone, phone, write the other report, check one's bank account, update one's Facebook status, read all that is necessary for whatever project, and think about dinner, all at once. The irony of the imperative of multitasking, which has become such an imperative because of the technological potential of social media, is that only "2% of people can multitask effectively. As for the remaining 98%?, they're actually lessening their productivity without even realizing it."[111] Of course, worker productivity is not necessarily an "ethical" concern, but one can argue that the assumption of transparency between the Google application and human activity as deep ethical stakes, particularly in terms of the problem of ontologically identifying human capacity with the extensions available in current software. More interesting is the fact that multitasking creates a culture of distraction which has deep implications on brain functions, social relations, and "culture." Multitasking crosses over into our "private" lives as well. It not only has an impact on work productivity, but on people's capacity to be with each other in unmediated and sustained manner. Interpersonal relationships are now also threatened by the spectre of distraction and new forms of irritation are seen in those common scenes when friends or lovers attempt to talk to one another while texting other people or checking their email over dinner. The information society has implications for common courtesy and politeness which, from Aristotle and Confucius to the present, have been the central hallmarks to the ethical life.

The information society is noisy. It thrives on economies of attention where indeed consumers "work" when they give their attention to an array of advertisements, images, and spam. Looking, in this context, is a type of labor. Podcasts streams, beeps and blips form the aural ambience, screens interpolate, and everyone blares on their cell phones on the crowded bus in what can only be called an information society cacophony.[112] Talking loudly via cell phone on public transportation was deemed an incivility by the French transit authorities in 2012. It counts as one of the many infractions to the "civil" studied by the newly formed Incivility Observatory.[113] The lesson is clear: the information society creates new forms of digital nuisance. The air and

[110] Rosen, C., 2007, "Virtual Friendship and the New Narcissism," *The New Atlantis*, Summer 2007, p. 16
[111] See http://mashable.com/2012/08/13/multitasking-infographic/
[112] The degree of relative cacophony in any given public space is certainly culturally sensitive and dependent upon contingent social customs and taboos. Quiet Spaces are also being readily introduced on public trains and tramways.
[113] See http://www.mobilicites.com/fr_actualites_la-ratp-installe-un-observatoire-des-incivilites_0_77_1941.html

environment, however, are fully “digital,” demanding if there is such thing as an outside to the information society. Christine Rosen characterizes the information society as the great electronic din, which is not simply impolite, but is also detrimental to the life of the mind:

> For the younger generation of multitaskers, the great electronic din is an expected part of everyday life. And given what neuroscience and anecdotal evidence have shown us, this state of constant intentional self-distraction could well be of profound detriment to individual and cultural well-being. When people do their work only in the “interstices of their mind-wandering,” with crumbs of attention rationed out among many competing tasks, their culture may gain in information, but it will surely weaken in wisdom.

Information societies are none the more wiser, according to Rosen. In the midst of the din of “access,” created by the prospect of more democratized information, people are blind to the simple fact that the human brain and psyche could be potentially adversely effected by the information society (in the simple sense of how human beings learn and communicate). Rosen cites, for instance, neurologist Jordan Grafman who remains convinced that “Kids that are instant messaging while doing homework, playing games online and watching TV, I predict, aren’t going to do well in the long run.”[114] She also cites education psychologist, James Healy, who suggests that “this generation of kids is guinea pigs,” who will demonstrate only the capacity for “very quick but very shallow thinking.”[115] The information society thus appears to favor book reviews to books, PowerPoints to philosophical meditation, instrumental and quickly usable knowledge to wisdom, quick web searches to research, and distraction to careful deliberation. It appears to mystify the possibility of information mastery in order to mask the reality of confusion. From a neurological perspective, it perhaps assumes that the hardwiring of the brain and the emotions are more malleable than they actually may be. This implicitly begs the question of what the responsibilities of the information society are to both current and future generations.

IV.4 This is Your Brain on Google

The empire known as Google has slowly emerged as being at the “core” of the information society. Not simply a search engine or algorithm, Google seemingly contains "magical" properties that transform every internaut into a sorcerer of information, imagery, data, and goods and objects. Card catalogues in musty libraries are a thing of the past as research is increasingly done on line. The petty problems of daily life, from common colds to leaky faucets, can be resolved with a quick Google search. Google can be used to “screen” others. With the rise of Google, reputation, achievement, and personality are no longer limited to curriculum vitae and presentations, but are equally effected by the development of one’s “online profile” (which one can attempt to deliberately construct or can be pieced together through the dissemination of one’s activities). In both cases, however, people no longer necessarily control completely the representations of themselves. Many people wake up to Google. Googling is also a verb which means to Google or to search the internet. It is also rumored that Google will become its own island nation somewhere in the Pacific.

There is indeed something “unnatural” about Google, something “unnatural” about being able to tap into those flows of information with such ease. Yet, for all its “non-nature,” Google is slowly becoming another nature, a type of collective intelligence or global brain, and a new collective panoptician that permits everyone to see everything through Google street views and Google

[114] Ibid.,
[115] Ibid.,

Earth. Bernard Girard likens the Google effect to a type of “Cognitive Capitalism,” a site of “information exploitation” where data is not only mined but is responded to in customized ways that seem to give Google the semblance of agency.[116] Moreover, Google invents new means of controlling knowledge and intellectual production – its epistemological parameters and choices largely circumscribe the flow of knowledge and the limits of the social field. It is not simply the purveyor of “state thought,” but “world thought” against which a counter-movement of knowledge(s) need to struggle. The terms of emerging post-Fordist “Google economies” and “Google hegemonies” are used, where the platform controls and mediates all economic production and consumption while also absorbing into its folds both the immaterial and material conditions of the market. Ariel Kyrou and Yann Moulier Boutang, unnerved and anguished by Google’s status as the centre of global information, economy, and imagination, have pleaded for a world “Beyond Google”. This other world would involve ceasing to think of Google as that "all too nice friend": people should, in other words, respond to the demiurge of the Google imaginary with another imaginary that refuses to be appropriated by its function as a mechanism of domination.[117] Such domination is psychic, social, economic, and information-based, but also physical and cognitive.

As Google does so much for human beings, they do less and less. Betsy Sparrow, Jenny Liu, and Daniel M. Wegner’s much touted study on “Google memory” and Google’s effects on human memory has concluded that human beings no longer remember in the same way, nor do they need to, as Google functions as the frontier of what the three authors refer to as “external and transactive memory.”[118] In other words, people no longer recall, but know where to look to remember. In a more general sense, people no longer need to struggle in the same ways to learn, to attain, or to get what they want. Brains and gratification patterns have therefore been thoroughly recalibrated. Memories and knowledge processes are now intrinsically Google dependent. In short, Google has replaced memory and has become the key memory-entrepreneur in the construction of global memory. Google knows. Thus human beings no longer need to know. The relationship between people's brains and Google is less one of symbiosis than a kind of captivity. While the impacts of Google on human cognition have yet to be fully explored, it is clear that the Google Brain is doing much of what the human brain once did. Knowledge, moreover, is no longer “honed”. People can “fake” knowledge by simply rehashing a Wikipedia page.

The ethical question, of course, if whether this represents another stage of human adaptation to technology or a fundamental transformation in what it means to be a human, to remember, to “know,” and to flourish. Following from this development, it can be easily argued that, from both a knowledge-based and personal perspective, human beings are the sum of their memories which allow people to engage with others and to share their experience of the universe. The mutation of this knowledge will have repercussions on the fullness of human engagement and experience. The original theorist of the end of history, Alexandre Kojève, held a dreary image of technological progress which he deemed to be the paroxysm of man’s slackening into comfort or an animalistic state of sloth. Without cognitive and spiritual “labor,” human glory and its evolution would end insofar as there would no longer be any need for resistance or matter to negate. Were he alive today, Kojève might argue that the end of history was not global liberal democracy, but perhaps Google.

[116] Girard, B., 2009, Google en parfait modèle du capitalisme cognitif, *Multitudes* 36 (Summer 2009), p. 81
[117] Kyrou, A., and Boutang, Y.M., Beyond Google, in Ibid., p. 43
[118] See http://www.sciencemag.org/content/333/6043/776.full

IV.5 NBIC and the Ethics of Convergence

The ethics of convergence and NBIC should not be dismissed as external to the ethics of the information society or simply relegated to the domains of nano and bioethics. In other words, the "I" (for information) in NBIC needs to be taken seriously. The prospect of human enhancement leading to new computational organisms and post-human computer cyborgs poses a new set of ethical challenges for the information society to come in which the human being risks to be wholly digitalized. Convergence will thus also be telecommuncational and information-based. The array of ICTs detailed in this report will come together in new hardware and software paradigms. When contextualized in the discourse of trans-humanism, they will be embedded into the human body or reconstructed as the human body's natural extension. Cyber-agency and human agency will converge in more resolute ways that recast humans not necessarily as actors in networks, but as networks themselves. Among the information-related visions of the post-human imagined by the 2002 Rocco and Bainbridge report, one finds:

- Fast, broadband interfaces directly between the human brain and machines will transform work in factories, control automobiles, ensure military superiority, and enable new sports, art forms and modes of interaction between people.
- Comfortable, wearable sensors and computers will enhance every person's awareness of his or her health condition, environment, chemical pollutants, potential hazards, and information of interest about local businesses, natural resources, and the like.
- Robots and software agents will be far more useful for human beings, because they will operate on principles compatible with human goals, awareness, and personality.
-People from all backgrounds and of all ranges of ability will learn valuable new knowledge and skills more reliably and quickly, whether in school, on the job, or at home.
-Individuals and teams will be able to communicate and cooperate profitably across traditional barriers of culture, language, distance, and professional specialization, thus greatly increasing the effectiveness of groups, organizations, and multinational partnerships.
-National security will be greatly strengthened by lightweight, information-rich war fighting systems, capable uninhabited combat vehicles, adaptable smart materials, invulnerable data networks, superior intelligence-gathering systems, and effective measures against biological, chemical, radiological, and nuclear attacks.
-Anywhere in the world, an individual will have instantaneous access to needed information, whether practical or scientific in nature, in a form tailored for most effective use by the particular individual.
-Engineers, artists, architects, and designers will experience tremendously expanded creative abilities, both with a variety of new tools and through improved understanding of the wellsprings of human creativity.[119]

The brave new world promised by Rocco and Bainbridge does sound promising.

However, the ethical challenges of reducing humanity to "a single, distributed and interconnected "brain" based in new core pathways of society"[120] does give occasion for pause. Ethics will, of course, have to rethink itself. Already, a foundational problem concerning the moral parameters of the trans-human and the non-human emerges. Simply stated, one cannot necessarily argue that NBIC creatures have the same ontology as humans. Thus, it becomes increasingly difficult to identify the "moral ground" of the NBIC world. In addition, there is no guarantee that convergence will improve our lives and point the way to greater freedom and

[119] Eds. Bainbridge, W.S., and Rocco, M., 2002, Converging technologies for improving human performance: nanotechnology, biotechnology, information technology, and cognitive science, NSF-DOC Sponsored Report, see http://www.wtec.org/ConvergingTechnologies/1/NBIC_report.pdf, p. 14
[120] Ibid., p. 16

autonomy. Are we thus to speak of ethics of the information society or ethics for the information society?

Convergence and enhancement have the potential to transform human beings into very different creatures. Thus, they pose not only ethical questions about the risks and moral implications of transformation, but also the ethics of this different creature. Those opposed to enhancement argue that NBIC intervention into the "natural" order of human life is morally wrong precisely because it is "unnatural." They worry that enhancement may create a race of super beings who will be able to subjugate the vulnerable and non-enhanced. Such a technology could be easily be misused in the name of techno-colonialism or techno-totalitarianism Pro-enhancement advocates, however, claim that freedom and liberty should also include the autonomy to make the choice to be enhanced. Such techno-libertarianism also claims that any regulation of nano-enhancements would be an affront to a person's right to choose how to live and what one can do to one's own body. Moreover, if enhancement does not necessarily harm anyone else, can it be intrinsically demonized.

As a prospect that remains on the horizon of the possible, and yet is, nonetheless, a firm future reality, there exists a vacuum in terms of ethical and policy-based reflection on NBIC enhancement. However, the issues that enhancement poses stand to be reflected on from an ethical perspective in the present. As James H. Moor argues, "society needs to formulate and justify new policies (such as laws, rules, and customs) for acting in these new kinds of situations. Sometimes it can be anticipated that the use of the technology will have consequences that are clearly undesirable. As much as possible, these need to be anticipated, and policies established that will minimize the deleterious effects of the new technology. At other times the subtleties of the situation may escape discussion, at least initially, and we will find ourselves in a situation of assessing the matter as consequences unfold…the situation may have analogies with different and competing traditional situations."[121]

A processual or dynamic ethics is needed which does not simply address enhancement from a cost-benefit analysis framework, but rather enables people to think about enhancement from the nexus of value, knowledge, and "nature." Even if cyborgs never materialise, such an exercise will prove invaluable to thinking about and rethinking what it means to be "human" in the 21st century.

IV.6 Friendly Robots?

While NBIC convergence and the becoming-cyborg of the human race are not such distant possibilities, in the short term, another set of ethical quandaries appear in the interface between the human and the robotic. Cross-cultural sociologies of the human-robot interface illustrate the gamut of ethical attitudes towards the lives of human beings with sentient machines. As José Cordeiro has observed, in Japan robots are considered the friends of human beings, mysterious mechanical spirits (whose presence is beneficial and) which entertain, aid, console, and guide. On the contrary, the American imaginary remains transfixed by robots of war, robo-cops, and terminators. The great conflict of this dystopia is one that pins man against machine.[122]

[121] Moor, J.H., 2005, Why we need better ethics for emerging technologies*, Ethics and Information Technology* 7:1, see http://commonsenseatheism.com/wp-content/uploads/2011/03/Moor-Why-We-Need-Better-Ethics-for-Emerging-Technologies.pdf

[122] Cordeiro, J. 2011, Humanism to transhumanism, Paper given at the First World Humanities Forum, Busan, Korea, November 25, 2011.

Relations with robots thus mirror the political unconscious of national landscapes. This also begs the question of how one should behave with virtual artificial agents and, of course, how they should behave with human beings. Whether incarnated in the form of Astro Boy, the singularity, android mutants, telerobots, military drones, or new technologies for people with disabilities, the popular imaginary is ambivalent about whether such man-made robots are really created to help human beings or will articulate their own autonomy and will so as to shatter humanity itself. Already in 1942, Isaac Asimov reflected on such concerns. He pinned down what can be arguably considered the first set of ethical principles on human/robot relations. In his famous three laws, he argued that:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.[123]

Asimov's laws resonate with an explicit paranoia of robot-human harm. They affirm simultaneously the robot's capacity to have an identity, integrity, and a survival instinct. Yet, Asimov's three laws were simply narrative devices employed to advance and frame the diegesis of his science fiction; they were not ethical rules in their own right. However, as fiction become reality, robot ethics has emerged as an important discipline in science and technology studies. It not only assesses the real challenges of living with robots, but also asks about the moral consequence of humans harming machines. In other words, it is not simply human beings who may potentially have rights but also robots. It is not only robots who must be "made" to act ethically towards human beings, but we who must act ethically towards our robots. It is not only we who must use robots to protect a nation, but the nation that must protect a robot.

Patrick Lin, Keith Abeney and George A. Bekey have framed the robot ethics discussion in terms of questions of harm, rights, and liability.[124] Among their primary objectives is to destabilize the biological supremacist position that refuses rights to robots by arguing that the pain of humans is obviously a much more important issue than that of the machines which which they connect. Indeed, they ask whether machines can even feel pain. However, in order to benefit from the advances of robotic technology, and enter into the brave new world of different forms of comfort and equity, requires that these kins of, often elliptical and improbable, ethical questions need to be asked. The three authors' larger fear is that, as is often the case, policy will again be too slow to address the robotics revolution which is taking place. This could lead to an abyss of missing regulation where artificially intelligent forms of labor, security, entertainment, warfare, and health could have potentially devastating consequences. As they remark, we need hence to ask:

Are some jobs too dangerous, or too important, for machines to take over? What do we do with workers displaced by robots? How do we mitigate disruption to a society dependent upon robots, if those robots become inoperable or corrupted e.g. through an electromagnetic pulse or network virus? Is there a danger with emotional attachment towards robots? Are we engaging in deception by creating anthropomorphized machines that may lead to such an attachment and is that bad? Is there anything essential in human

[123] Asimov, I., 2004, *I, Robot,* New York: Bantam Dell pp. 44-45. It should also be noted that in certain developing regions, the leap from our current reality to future possibilities must be carefully managed on both a rhetorical and infrastructural level. The lack of "futures management" is precisely what plunges many populations into anxiety or transforms the robotic into the stuff of Hollywood entertainment.
[124] Lin, P, Abeney, K., and Bekey, G.A., 2012, *Robot Ethics: The Ethical and Social Implications of Robotics*, Cambridge: MIT Press.

companionship that robots cannot replace?...This points to the need to attend to robot ethics now, particularly as ethics is usually slow to catch up with technology which can lead to a "policy vacuum."[125]

The ethical and policy implications of the robotics revolution are cross-cutting, interdisciplinary, and "total" in many regards. Robots are poised to affect the economy by forming a highly trained workforce which can perhaps do jobs better than human beings. Viruses could also easily create an army of rogue robots that turn against human beings. The question again becomes whether such entities should be granted any rights at all. What if robots replace friends, pets, and lovers, and potentially offer more fulfilling emotional, social, and sexual relations? When envisaged on a mass scale, robots would be the organizing hub of our society and the information society. They would be creatures who could not only facilitate human development, but also control its pathway.

Therefore, while meta-ethicists reflect on whether robot subjectivities and their capacity to experience pain and enjoy "robot rights," legal and ethical reflection needs to engage with robot crime, robot transgression, and robot etiquette. For instance, while in Japan robots might be humans' friends, these friends are precisely those machines which will are mining people's personal data as they cuddle with their plastic torsos.

For cyberlaw theorist, Ryan Calo, the frontier of robot ethics is ultimately an issue of regulation. The over-arching problem is precisely that "As robots leave the factory and battlefield and enter our homes, hospitals, and skies, it is not clear who will come to regulate them … Eventually we could imagine an agency devoted specifically to robotics. (It may not be named as such, just as there is no major agency specifically dedicated to computers or cars.) Until then, it makes sense to watch agency claims of authority over robots of all kinds, as well as agency disavowals of such authority. Each hold their dangers."[126] The crux of the matter is that these uncomfortable questions can no longer be avoided. They are in fact central to the evolution of the information society.

The scientific community is already engaged in research concerning the teaching of ethics to machines.[127] Such processes create a new image of "moral agency" out of simple plastic, wires, and microchips. Hence, while robots can easily become corrupted and wreak unimaginable havoc, they may also turn out to be ethical actors that are superior to human beings, who were the founders of so-called ethics.

IV.7 Cyber-War

A hacker can potentially release a virus that disables the entire power grid of a nation. The repercussions would be manifold: electrical outages, communications blocks, logistical confusion, eventual resource scarcity, military disablement, panic, disorder, and infighting. In the Art of War, Sun Tzu argued that, because warfare was an inevitable part of political life, the least that could be done was to attempt to conduct it ethically. For the Chinese strategist, this meant, among other things, allowing the enemy to implode with little loss of energy or men on the part of the aggressor. One thus wonders what Sun Tzu would think about the ethical ramifications of the new mode of bloodless, non-frontal combat: cyber-warfare. The once silent virtual arms race

[125] Ibid., pp. 11-12
[126] Calo, R., 2012, Who will regulate the robots?, see http://cyberlaw.stanford.edu/blog/2012/01/who-will-regulate-robots
[127] Zyga, L., 2012, How to make ethical robots, see http://phys.org/news/2012-03-ethical-robots.html

has become less covert. Nations have begun to reconstruct their geopolitical influence and strategies towards friends and enemies through the building of operational frameworks for cyber-warfare. Government agencies, intelligence agencies, military complexes, "terrorists", "rogue states", and international organizations such as NATO, among others, are all attempting urgently to advance their own cyber-weapons and cyber-security and develop their cyber-offenses and cyber-defenses.

In October 2012, US Secretary of Defense, Leon E. Panetta, broke his silence on this virtual arms race, by voicing the need to develop terms of engagement in cyber-warfare while, at the same time, warning potential enemies of the advances the Americans have made in terms of deterring and defending against potential cyber-attacks. Panetta described a possible scenario, whereby a nation is attacked on both the cyber and physical fronts, thereby paralyzing its ability to function: "The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."[128] However, such paralysis would not only be rendered easier to orchestrate, but would also be more devastating in terms of new forms of cyber-empire and cyber-imperialism when implemented against developing nations whose networks and security protocol remain relatively unadvanced. Panetta may have been worrying about the repercussions of such an action inside America. However, it is also important to think seriously about the uses of cyber-warfare by the mighty in attempts to subjugate the technologically weak. Far from being simply another example of a digital divide, such scenarios prove how new forms of global hegemony and sovereignty will be tied to the strength and deployment of cyber-tactics and cyber-weapons. In the new frontier of cyberspace, the potential for cyber-warfare or the "fifth domain of warfare" is vast, limitless, and can take on many different dimensions, including physical. Cyber-terrorism, cyber-espionage, virtual attacks on critical infrastructure, control of physical warfare, the capability to launch weapons, cyber-worms and viruses, and so on can all fall under the umbrella of cyber-warfare.

The inherent challenges and difficulties of regulating this "fifth domain" are already visible. A cyber-warfare game changer came in the form of a computer worm, known as Stuxnet, which attacked Iranian nuclear centrifuges in 2010. The even more powerful Flame malware was discovered in 2012, attacking computers throughout the Middle East. Most recently, attacks on several US banking institutions disrupted services and the Internet operations of these companies. Modern warfare on the ground has also been enhanced with the use of cyber-weapons, most commonly drones.

The US has setup Cyber Command. It has been relatively forthcoming about public information when it comes to the future of cyber-warfare and the nation's desire and resolve to defend its citizens at all costs. Having an advantage when it comes to cyber technology, the US' relative increase in transparency with regards to cyber-warfare can be translated into the nation's desire to set the boundaries of international cyber-warfare, its discourse, and parameters. Some of these initiatives, including the Cyber Intelligence Sharing and Protection Act (CIPSA), are a cause for concern for privacy advocates alike, as they would make intelligence-sharing between different parties lawful and simple. The secretive nature of cyber-warfare and intelligence make government oversight difficult, and provide little to no transparency when it comes to the nation's cyber-offense and defense. The US' heightened cyber rhetoric, however, may in effect push other nations into advancing their own cyber-attack capabilities. As Luciano Floridi suggests, will this cause become a "new arms race, given the very high rate at which cyberweapons

[128] See http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262

'decay'"?[129] Close monitoring of potential cyber-aggressors, such as Iran and Russia, have already been underway for sometime. NATO has also taken steps to advance its own cyber-defenses and usher in greater cooperation and information-sharing among allied nations. In fact, NATO is conducting exercises as this report is being drafted, that are known as the "Cyber Coalition 12" in order "to test Alliance technical and operational cyber defense capabilities."[130]

Mirroring the ethical impasses of public versus private that plague the information society, cyber-warfare and its entrenchment in national security intrinsically gives rise to the ethical nexus of what is lawful versus what is lawless. It is complicated by the fact that reconnaissance and espionage not only need to be secret, but are often lawless for the good of the given state and its interests. Returning to the writings of Sun Tzu, it would not only be naïve to conduct war in an "honest" manner, but potentially dangerous for those beautiful souls who advocate such transparency. Deception is not only the rule, but it is precisely that which allows cyber-warfare to operate under various states of exception when and where the law is suspended in the name of the common good. The ethics of the emerging technology of cyber-warfare are therefore tied to larger discourses of just war, ethical warfare, and the rules of engagement.

Nonetheless, Jody Westby, CEO of Global Cyber Risk suggests that "The current framework of international law and treaties does not adequately address cyber-conflict … customary international law should be extended into the cyber domain and define a certain amount of a nation's critical infrastructure that should be 'declared sacred and off limits for attack'."[131] In 2012, the United Nations also entered the debate, arguing for the need to create an ethical framework from with which to address the cyber-war world. Highlighting the interconnectedness of freedom and security, Dr. Hamadoun Toure, head of the UN's telecommunications agency acknowledged that, "There is a fine line between security and freedom," while explicitly stating that one cannot exist without the other.[132]

Just like the need to develop a cyber civil society to reduce incidents of malice, nation states must also develop codes of ethical conduct for the much dreaded but probable scourge of cyber-warfare. In essence, a virtual just war theory must be developed. Luciano Floridi has emerged as the most vocal proponent of such a theory. In his upcoming *Just Cyberwar Theory,* Luciano Floridi explains how extensive time, discussion, and evolution of thought brought forth just war theory. The inhuman pace of advancing technology leaves thinkers of this generation with no time to understand fully the debate about the social boundaries and contracts of cyber-society. The information society functions as an obstacle to the molding of a more ethical information society. It is a haphazard cyber-world where, at the moment, anything goes. Floridi goes on to ask, "how can virtue and ethics be applied to phenomena that are actually reshaping the conditions of the possibility of virtue ethics itself?"[133] He concludes, that, if this is indeed the case, then ultimately "information warfare calls for an information ethics."[134]

---

[129] Floridi, L., 2011, Just cyberwar theory. *The Philosophers' Magazine* 55. pp. 17-18, see <http://secure.pdcnet.org/tpm/content/tpm_2011_0055_0017_0018>.
[130] See http://www.nato.int/cps/en/SID-F42C9D1D-E4CB5A56/natolive/news_91115.htm?blnSublanguage=true&selectedLocale=&submit=select
[131] Heichler, E. 2012, Cyberwar evolves faster than the rules of engagement, see http://www.computerworld.com/s/article/9233524/Cyberwarfare_evolves_faster_than_rules_of_engagement
[132] Lee, D., 2012, Flame: UN urges cooperation to avert global cyber-war, see http://www.bbc.co.uk/news/technology-18351995
[133] Floridi, L., 2011, pp. 17-18
[134] Ibid.,

V. POTENTIAL RECOMMENDATIONS FOR UNESCO AND ITS PARTNERS

(a) UNESCO should encourage international and interdisciplinary reflection and debate on the ethical challenges of emerging technologies and the information society, in particular through the Information for All Programme (IFAP) and the work of the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST). Such reflection and debate should have a multi-tiered dimension that connects to policy and advisory bodies, with particular attention to participation of developing countries and sensitivity to their needs. Among themes of particular relevance in examining the interface between information technologies, social transformation and governance are the relation between human rights and ethical principles for the information society; the challenges of interculturality in information ethics; the possible tensions between freedom of expression and moral harm; issues of privacy and security; and the fundamental question of personal and collective identities in a digital world.

(b) In order to support equitable participation of all stakeholders, efforts should be made, including through UNESCO programmes where appropriate, to build or strengthen regional and national capacity in to analyse, discuss and respond to the ethical challenges of the information society.

(c) Awareness should be raised of the ethical implications of the information society, particularly among young people, along with life-long education initiatives to equip all citizens with the skills and competence to participate actively and knowledgeably in the information society. New info-ethical and info-civic pedagogical paradigms, including but not limited to e-learning, could be envisaged in this regard to support new modes of global citizenship fully integrating digital media and virtual political spaces.

(d) Freedom of expression should be affirmed as a fundamental right and as the basis for reflection on its responsible use in the context of broader consideration of the right to communication in a framework of cultural sensitivity, tolerance, and dialogue. Consideration should be given to the ethical principles that bear on technological and social issues in the information society and underlie specific regulatory frameworks, whether or not such principles are enshrined in existing normative instruments or codes of conduct. Of particular importance in this regard is analysis of gaps and lags that hamper policy in the face of the ethical challenges of the information society, with a view to supporting policy-makers and stakeholders in moving in synchrony with technological advance rather than reacting after the fact.

VI. APPENDIX: EXISTING NORMATIVE FRAMEWORKS

- **The Universal Declaration of Human Rights**
  http://donegallpass.org/UNIVERSAL_DECLARATION_OF_HUMAN_RIGHTS.pdf
- **Declaration on Science and the Use of Scientific Knowledge**
  http://www.unesco.org/science/wcs/eng/declaration_e.htm
- **Recommendation concerning the promotion and the use of multilingualism and universal access to cyberspace**
  http://portal.unesco.org/en/ev.php-URL_ID=17717&URL_DO=DO_TOPIC&URL_SECTION=201.html
- **Santo Domingo Declaration on Bioethics and Human Rights**
  http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/declaration_santo_domingo.pdf
- **Hanoi Statement on the Ethical Dimensions of the Information Society**
  http://portal.unesco.org/ci/fr/ev.php-URL_ID=26324&URL_DO=DO_TOPIC&URL_SECTION=201.html
- **Fez Declaration on Media and Information Literacy**
  http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/Fez%20Declaration.pdf
- **Tshwane Declaration on Information Ethics in Africa**
  http://www.africainfoethics.org/tshwanedeclaration.html
- **The Internet Rights and Principles Charter**
  http://irpcharter.org/wpcharter/
- **Code of Ethics for the Information Society proposed by the Intergovernmental Council of the Information for All Programme (IFAP)**
  http://unesdoc.unesco.org/images/0021/002126/212696e.pdf
  http://unesdoc.unesco.org/images/0021/002126/212696f.pdf
- **APC Internet Rights Charter**
  http://www.apc.org/en/system/files/APC_charter_EN_0.pdf
- **APC Code of Good Practice on Information, Participation and Transparency in Internet Governance**
  http://www.apc.org/en/system/files/COGP_IG_Version_1.1_June2010_EN.pdf
  http://www.apc.org/en/system/files/COGP_IG_Version_1.1_June2010_FR.pdf