The Ethics of Cyberspace
by Cees J. Hamelink


How should democratic societies organize cyberspace? This question is at the heart of the argument presented by Dr. Cees J. Hamelink in his book Ethics in Cyberspace, published in the year 2000. Invoking the application, and abuse, of human rights in the rapidly evolving world of information and communication technologies (ICTs), Hamelink establishes his position as a proponent of normative and social standards at the international level which place freedom, justice, and human security at the top of the proverbial agenda. He eschews the profit-based motivation of individuals, corporations, and policy-makers involved in the economically and culturally discriminatory diffusion of ICTs across the globe. Citing the inadequacy of various moral rules, codes of conduct, and emerging “netiquettes”, Hamelink demonstrates the need for a new morality capable of addressing the dilemmas born from the rampant and largely despotic nature of ICT proliferation. In Ethics in Cyberspace he points to the inadequacies of current policies that govern the development, application, and access to ICTs emphasizing a return to the core respect of human rights as defined in the 1948 Universal Declaration on Human Rights.¹

In the preface of Ethics in Cyberspace, Hamelink points out that Cyberspace² forces societies to confront moral choices on a variety of levels: choices relative to the design of technology, choices relative to the application of technology as well as the responsibility for its introduction into social environments, choices relative to the distribution of technology, and, finally, choices that determine the control over technology and the impact that both this control and the technology itself may have on societies. He suggests that there are three main approaches to the governance of Cyberspace. The first is the “anarchistic position” that considers Cyberspace as an entirely independent territory where conventional rules do not apply. The second are those opposed to such cyber-anarchy in favor of a “strict regime” that protects all cyber citizens from subversive uses of the technology. Lastly, Hamelink identifies cyber citizens who prefer to police themselves and who propose various forms of self-regulation. This last group has generated a plethora of what are commonly termed “netiquettes”, or online codes of conduct, along with software programs and organizations such as Cyber Angels designed to discern appropriate cyber content and protect users from abuses (often illegal) of Cyberspace.

The first chapter outlines two categories into which conventional ethical theories are typically divided: duty-based (deontological) and effect-based (utilitarian-consequentialist). Hamelink discusses the problems inherent to each, ultimately concluding that a third “contextualist approach” is the ideal approach. He states, “The contextualist approach rejects the deductive model of moral problem-solving and prefers an inductive model of moral argument… [This] approach proposes a comparative case analysis through which resolutions to new choices

¹ The Universal Declaration on Human Rights of 1948 is the seminal text on human rights and is considered the first demonstration on behalf of the international community of its willingness to protect these rights in the widest possible measures.
² “Cyberspace is the virtual communicative space created by digital technologies. It is not limited to the operation of computer networks, but also encompasses all social activities in which digital information and communication technologies (ICTs) are deployed.” Hamelink, p.xi ; “Cyberspace is a geographically unlimited, non-physical space, in which – independent of time, distance, and location – transactions take place between people and computers…It is important to note that there is no single Cyberspace. There are ‘cyberspaces’.” Hamelink, p.9 ; “Science fiction author William Gibson invented the term Cyberspace in 1981 to describe a new, virtual world.” Hamelink, p.9
are sought by reasoning from solutions that were preferred in similar situations…[taking into account] the

institutional and cultural settings and the value orientations in which choice situations are located.” In other words, Hamelink aligns himself with this method of moral reasoning which he defines as the most comprehensive and sensitive when it comes to the weighing of cultural implications; implications apt to alter the givens in the course of a particular moral choice because of changes in social context and values. He further applauds this method for “the due process of moral argumentation” that it affords.

Hamelink goes on to discuss the fact that the complexity of modern technology has led to the delegation of responsibility for choices to experts who have an increasingly vested interest in the technology’s production and, therefore, its ultimate profitability. For the author, this rarified relationship between technology and humans poses a significant threat to the general access to and understanding of available ICTs. He points out that, historically, technological choice has been a highly undemocratic process that precludes all serious discussion of potentially negative social impacts. Hamelink denounces national and international policy-making on the topic, criticizing the emphasis on operational choices characterized by reactive measures and incremental adaptations. He cites the neglect of strategic choices as one of the primary causes for the undemocratic nature of ICT distribution and access.

Another of Hamelink’s key arguments is that “social relations that are obtained in the physical world do not disappear in the virtual world.” The exaggeration of the openness and equality to be gained in Cyberspace is problematic because it ignores ongoing injustices and their continued proliferation through this new medium. Hamelink reminds the reader that virtual transactions do, in fact, affect the physical world, often reinforcing existing practices and realities. In his explanation of this connectivity and interactivity, he highlights three important characteristics of ICTs: their pervasiveness, digitization, and convergence. “Technical convergence,” he argues, “leads to institutional convergence and to the consolidation of national and international provision of information (and culture) to the hands of a few mega-providers.”

Furthermore, digitization has changed and continues to impact economic, political, and cultural landscapes. The production and distribution of information has evolved into the most important economic activity in a society, one in which “information technology begins to function as the key infrastructure for all industrial production and service provision, and in which information itself becomes a commodity tradable on a global scale.” One of the problems Hamelink identifies with this economic model is the difficulty that information-based products encounter in export markets. They are faced with linguistic and other cultural barriers, but more importantly often have a “high service content” which requires a strong local component in order to establish direct interaction with end-users. On the political front, Hamelink rejects utopian scenarios that suggest that ICTs will bridge the gap between governors and the governed and points out that ICTs may be just as readily harnessed by anti-democratic factions and used nefariously. Ultimately, he remains uncertain as to whether or not more access to information leads to social improvement or the creation of a more egalitarian society. For Hamelink, the most pronounced cultural impact of ICT pervasiveness, digitization, and convergence can be summarized by what he dubs “the Disneyfication scenario” whereby “a specific brand of Western modernity becomes the dominant ‘way of life’ around the globe and local cultures are assimilated by it” to varying degrees. He maintains, however, that such an impact may well be limited to those cultures’ peripheral layers. On a more optimistic note, he points out that local cultures “may also define their own specific responses to culture globalization” using ICTs in a process he calls “the dual-track scenario.” Nevertheless Hamelink conjures a second scenario, “the hostility scenario”, involving “aggressive forms of rejection of the imposed modernity.”
The social transformation brought about by the so-called technological revolution, according to the author, has given rise to a new elite despite claims that capital in the new “Information Society” will not be restricted because information will be the new capital and “everyone can own information.” Hamelink enumerates several factors that disprove this claim and bolster his notion that a new elite is emerging, the most convincing of which points out that with the increasing complexity and specialized nature of information “more people know less” despite the greater volume and availability of this information. Other points include the difficulty in exploiting information, the prohibitive cost of such exploitation preventing societies at a relative economic disadvantage from participation in this new market, the need for the necessary infrastructure to support information capital, and the uneven control and distribution of ICTs throughout the world.3

This flagrant inequality is owed to hasty and biased policy-making at the national and international level. The author points to the fact that the GATT Uruguay Round of Trade Negotiations shaped the world’s current institutional arrangements for ICT exploitation more than developments made within the telecommunications industry itself. He goes on to explain that as long as ICTs are deployed in outdated institutional frameworks the full benefits of the technology may not be harnessed, leading to a tendency on behalf of such institutions to experience a technology lag as newer, more powerful systems emerge demanding even newer and more powerful infrastructures. This is especially true for developing nations where the technology lag represents a daunting obstacle to durable economic development. Forever steps behind the latest ICT advancements, there is little hope of creating and maintaining a competitive profile in emerging technological industries where there exists exponential room for growth in the present-day global economy. The secondary impacts of this market exclusion are, perhaps, even more distressing. Hamelink rightly identifies the threat to linguistic diversity as ICT standards tend toward the dominant language of international trade between institutions which is, more often than not, English.4

In chapter two, Hamelink addresses some challenging issues confronted by parties involved in the establishment of a morality in Cyberspace ranging from virtual sex and hacking to questions of anonymity and the creation of online personas. His objective in this section is to call the reader’s attention to existing policies of self-regulation relative to such issues as well as corporate comportment in ICT settings. He cites policies, user contracts, and codes of ethics and professional standards of the University of Southern California, CompuServe, AOL, the Computer Ethics Institute, the Australian, British, and South African Computer Societies, the Japanese Information Service Industry, and Nintendo among others. Hamelink highlights the critical link between business ethics and ethical reflection relative to ICTs, arguing that the “ethical enterprise” in its current form is more likely a response to industry pressures and pre-

---

3 Taking the Internet as an example: as of December 31, 2005 the continent of Africa, with a population count of 915,210,928, reports a mere 22,737,500 Internet users (2.5% of the population), while Europe, with a relatively comparable population of 807,289,020, boasts 290,121,957 Internet users (35.9% of the population), a difference of 267,384,457 users. This is only one of several telling comparisons which reflect the unequal distribution of access to the Internet. “Internet Usage Statistics”, [www.internetworldstats.com]

4 “The danger that the internet thus presents to linguistic diversity is in fact one of the mainsprings of the digital divide, and it represents a serious threat for the diversity of contents in cyberspace. Indeed, four essential conditions pre-exist to the contents themselves: the existence of a language acting as a vehicle of these contents, the possibility to write in this language, the existence of a code allowing the transcription of this written language in cyberspace and eventually the compatibility of such a transcription with existing softwares...Several thousand languages are practically not used in cyberspace, thus automatically marginalizing those cultures of which they are the vehicle. Among the many factors that account for this state of affairs, one basic determinant in the case of unwritten languages is the fact that, as such, they simply have no chance of being used as a language of communication on the internet. And around 6,000 of the world’s languages are not written but spoken.” UNESCO, Towards Knowledge Societies, Paris: UNESCO Publishing, 2005.
emptive measures taken to avoid legal censure and political run-ins. On this topic, the author concludes that even if ethical codes are designed with honest intentions they do not contribute in any significant manner to the solution of pressing moral dilemmas. Such solutions, he maintains, “can only be found in the dialogue between those concerned and not by prescriptions and rules.”

Chapters three through seven of Ethics in Cyberspace place human rights at the forefront of their respective dialogues, forging connections between ethical concerns raised by Cyberspace and ICTs and principles outlined in specific articles of the 1948 Universal Declaration of Human Rights. Chapter three focuses on the realization of rights and freedoms within the framework of Cyberspace’s governance (corresponding to Article 28 of the Universal Declaration of Human Rights). Chapter four broaches the issue of equal entitlement to education about and access to ICTs (corresponding to Article 2 of the Universal Declaration of Human Rights). Chapter five discusses the right to security and personal protection in ICT applications and ICT-human interactions (corresponding to Article 3 of the Universal Declaration of Human Rights). Chapter six addresses issues of free speech and knowledge in Cyberspace (corresponding to Article 19 of the Universal Declaration of Human Rights). Finally, chapter seven concludes with Dr. Hamelink’s call for the democratization of technological choice (corresponding to Article 21 of the Universal Declaration of Human Rights).

The establishment of a “decent society” in Cyberspace, taking into account the full set of rights and freedoms guaranteed to all individuals under the Universal Declaration of Human Rights, preoccupies the author throughout chapter three. Hamelink promotes the “relativist approach” to ethical quandaries concerning Cyberspace, one that defends the notion that all morality is relative to culture. His persuasive, if not sometimes idealistic, discourse affirms the “universal validity of human rights” and the moral obligation to protect and enforce them in evolving technological terrains. For Hamelink, the recognition of this universal validity can take on a variety of admissible forms according to local/cultural interpretation. The critique that stands out in this chapter is that of the inadequate enforcement of human rights standards around the world. The author details procedures currently in place such as the those based on the Optional Protocol (OP) to the International Covenant on Civil and Political Rights (ICCPR) of 1966. Hamelink notes, “The Protocol authorizes the UN Human Rights Committee to receive and consider communications from individuals subject to its jurisdiction who claim to be victims of a violation by that State Party of any of the rights set forth in the Covenant.” He goes on to explain, however, that despite the existence of such enforcement bodies their power to enforce human rights standards is severely limited. A second major problem for human rights enforcement, in “the real world” and Cyberspace alike, is the convention state-citizen relation which precludes the need for “a horizontal effect” of these basic rights. In other words, abuses that occur in citizen-citizen contexts between private parties are even less punishable. In Cyberspace, such citizen-citizen violations are that much more difficult to detect and persecute. In order to achieve the good governance of Cyberspace, Hamelink insists that the democratic organization of societies (and by this he means to imply the complete adherence to human rights standards) must be coupled with the public accountability of both institutions and individuals.

Chapter four of Ethics in Cyberspace demonstrates that the social inequalities, disadvantages, and injustices with which “the real world” is familiar are reproducible, and observable, in Cyberspace. The author evokes “the global digital divide” citing information issuing from the United Nations Development Program (UNDP) : “The network society is creating parallel communication systems: one for those with income, education, and – literally – connections, giving plentiful information at low cost and high speed; the other for those without connections, blocked by high barriers of time, cost and uncertainty and dependent on outdated
He likewise mentions the skewed distribution of ICT resources, education, and knowledge between men and women throughout the globe, pointing to illiteracy rates that reflect a strikingly similar gender gap. Alongside such questions of entitlement and access, Hamelink raises the debate over what information should be accessible, calling into question the concentration of power held by a small number of decision-makers in increasingly privatized spheres with purely economic agendas.

Chapter five is devoted to the author’s premise that “the pervasive application of digital technologies creates new forms of social vulnerability.” He makes reference to the highly unpredictable nature of software failures which pose real threats to contemporary societies where such programs are fully integrated into critical functions and services, the failure and/or malfunction of which could be potentially devastating. Key to Hamelink’s argument is the exposure of concrete examples of digital sabotage and “cyberwar.” He lists numerous examples of such attacks involving important organizations affiliated with the American government as well as international banks and e-mail services. Alongside this list of abuses, however, Hamelink points out that some digital sabotage and hacking is productive in the sense that it exposes systems’/codes’ weaknesses often spurring innovation in the field of data encryption and cryptography which have taken on new importance. He returns, however, to a negative argumentation underlining the fact that while encryption technology is an important tool for the protection of the confidentiality of communications, it also facilitates secret communication among criminal organizations making security harder to ensure both “offline” and in Cyberspace. Various multi-partisan legal measures are already in place in an effort to regulate the design, application, and the sharing of encryption techniques, but these measures are subject to constant criticism because of the parties (private and public) they tend to favor. Hamelink’s ultimate point in this chapter is that with the globalization of electronic surveillance and other digital technological security interventions, the human rights claim to security in Cyberspace is under threat. He states that “against the erosion of confidential communications, national governments and the international community [must continue to be] engaged in providing forms of legal protection for security in the private sphere.”

Chapter six deals with Hamelink’s take on free speech and knowledge in Cyberspace. He brings up issues of censorship, citing examples where the publication and diffusion of information and opinions (particularly in journalistic contexts) in Cyberspace has given way to controversial public discourse. The author identifies extreme pressures exercised by governments against national network providers and Internet Service Providers (ISPs) in countries such as Singapore, China, Vietnam, and Burma. He alludes to the “global online marketplace” and the unpopular business-to-business exchange of personal information for marketing purposes. He notes that the “commercial variant” of censorship is generally supported through the widespread belief that the provision of information between actors “guarantees a creative and competitive marketplace with a diversity of contents” when in actuality there is increasing evidence to the contrary: no such effect took place in the mass media sector where the trend toward concentration and consolidation “tends to produce a limited package of commercially viable content.” Hamelink proposes that virtual marketplaces will behave similarly and that there is no valid reason to believe otherwise. Intellectual property rights and the problem of piracy in Cyberspace is addressed: a problem essentially governed by the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO). Worthy of note is the increasing emphasis on the commercial facets of copyright protection, a tendency reinforced by the progressive shift of forums of negotiation from the WIPO to the WTO. Hamelink’s concluding argument in this chapter is that “the realization of an international human rights to

---

knowledge would need a balance between a set of rival claims”: the claim to the rightful protection of human property against the claims to global welfare.

The seventh and final chapter of *Ethics in Cyberspace* discusses the democratization of technological choice. It reinforces arguments that appear in previous sections of the book such as the pre-requisite of democratic participation in order to ensure the respect of human rights in Cyberspace and the need for public accountability particularly in large and complex societies. A third recommendation set forth by Hamelink calls for the acknowledgment and amelioration of the reduced space afforded national governments for independent policy-making relative to ICTs. He points to the technology boom of the last few decades that decisively internationalized (and complicated) the governance of such technology as a cause of ad-hoc supra-national policies. Yet another obstacle to the democratization of technological choice, as identified by the author, is the increasing influence of trade and market standards over world communication politics and the diminishing role of political considerations, including human rights considerations. Not only have the private actors in the arena of ICT-governance become more influential, they have become increasingly invisible to the extent that government and private business policies have become nearly undistinguishable. Thus, as Hamelink concludes, the global governance of Cyberspace has become largely committed to “minimizing public intervention and maximizing freedom for market forces.” This “globalization-from-above” scenario places industrial elites in a position of near-absolute control of such governance with minimal public accountability.

All of this places our global society in a very precarious situation. As Dr. Hamelink reasons:

“The enemies of the egalitarian democratic ideal are those forces that actively shape the ‘new world order’ that currently emerges largely in response to the collapse of Communism. The new world order poses a serious threat to the project of an egalitarian democracy since it exacerbates existing inequalities and results in a deep erosion of people’s liberty to achieve self-empowerment. Since the new world order is not welcome everywhere, it also provokes a fierce opposition in forms of national ethnic and religious fundamentalism that – ironically – equally threaten the prospect of an egalitarian democratic arrangement of world communication.”

What, then, are the solutions to these urgent crises? For the author, society’s only recourse is civic education and intervention through international, inclusive forums such as the World Summit on the Information Society (WSIS) and through the active participation of non-governmental organizations (NGOs) in this inter-cultural dialogue.

---

6 The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005. The objective of the first phase was to 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. The objective of the second phase was to put Geneva's Plan of Action into motion as well as to find solutions and reach agreements in the fields of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents. [http://www.itu.int/wsis/index.html]
ABOUT THE AUTHOR

Dr. Cees J. Hamelink studied philosophy and psychology in Amsterdam. He is Professor of International Communication at the University of Amsterdam, and Professor of Media, Religion and Culture at the Free University in Amsterdam. Professor Hamelink has also worked as a journalist as well as a consultant on media and communication policy for several international organizations and national governments. He is honorary president of the *International Journal for Communication Studies: Gazette*, past president of the International Association for Media and Communication Research, president of the Dutch Federation for Human Rights, founder of the People's Communication Charter, and board member of the International Communication Association and the international news agency Inter Press Service. Professor Hamelink has guest-lectured in over 40 countries and is currently special adviser to the United Nations for the forthcoming World Summit on the Information Society.


In 2004 he received the Lifetime Achievement Award from the International Communication Association. Professor Hamelink is also a regular commentator on radio and television in the Netherlands.

[ http://www.com.umontreal.ca/spry/spry-ch-e.html ]