

# Proposal for an Accessible Conception Of Cyberspace<sup>1</sup>

By David H. Gleason, Principal Consultant, [ITforProgress.com](http://ITforProgress.com)  
and Lawrence Friedman, Professor of Law, [New England Law|Boston](http://NewEnglandLawBoston.com)

Copyright © 2004

Rev. 11/13/2009

## Abstract

This paper addresses the knowledge required for individuals to evaluate Information and Communications Technologies (ICT) decisions that relate to the organization and management of cyberspace, and to hold accountable the parties responsible for those decisions, whether the responsible party is a government actor, market actor or private individual. The authors argue that the Open Systems Interconnection (OSI) model, with certain modifications, should serve as a primary educational tool in helping individuals to gain the understanding of ICT necessary to protect public interests related to cyberspace.

## 1. Introduction

Cyberspace is an artifact of the decisions and activities of many millions of actors – a reflection of the continuous subsumption of decisions that relate to the structure of cyberspace or to the norms that affect behavior in cyberspace. (Gleason, 2000) Those decisions occur at two levels: at the level of code, as the architecture of cyberspace is constructed on prior decisions made by programmers charged generally with maximizing the medium's various capabilities for private or public ends; and at the level of experience in cyberspace, as the actions of individual users contributes to the development of particular cyberspatial social norms.

Some actors have more of an impact on the construction of cyberspace than others: governments and market-leading corporations, for example, are establishing the structures – and the rules – of cyberspace within which users must operate. It is important, therefore, that, apart from programmers, a plurality of users have enough of an understanding of cyberspace that they can hold those influential actors accountable for their decisions about the ways in which cyberspace will or will not be constructed.

Though many human interactions that occur in cyberspace appear to mirror their physical world equivalents, individuals have varying levels of comfort with cyberspace: young people who grow up using computer technology appear intuitively to grasp how to negotiate their way through cyberspace, while to older users the experience of cyberspace may seem opaque and unnatural. (Gleason & Friedman, 2003) Both generations of users, however, suffer from a relatively limited understanding of how cyberspace actually works.

In this paper, we propose a framework for understanding cyberspace that is sufficiently accessible to allow a global citizenry to hold governments, market actors and other individuals accountable for the impact of decisions that relate to cyberspace. The goal is a framework for understanding cyberspace that is accessible across generational and cultural divides, so as to

---

<sup>1</sup> This paper was presented at ETHICOMP 2004 in Syros, Greece.

make possible some form of democratic participation in the management and organization of cyberspace. We suggest that the Open Systems Interconnection (OSI) model authored by the International Organization for Standards (ISO), the basis of interoperability of computers on the Internet, provides an appropriate initial framework for educating individuals about cyberspace.

The 7-layer OSI model, developed by and for engineers, explains how ICT can take information from an intelligible form down to electrical signals, and then back up to presentation. For our purposes, we suggest that three layers should be added to the model to elucidate the human side of the equation: user interface, interpretation and impact. With the addition of these layers, this model would provide a rubric against which most citizens could assess their understanding of cyberspace and, therefore, their potential to influence policy and make decisions about the structure and use of cyberspace. Should they desire more, it would also provide a framework for learning.

We first discuss the concepts of cyber-citizenship and accountability in a multi-cultural context. We then describe our proposed model in detail, concluding with suggestions about the use of the model in teaching and learning.

## **2. Cyber-citizens and the issue of accountability**

We are accustomed to thinking of citizenship as related to the legal condition of nationality – related, that is, to identification with, or at least residence within, the jurisdiction of a particular sovereign state. (Shklar, 1991) In the federalist governmental system of the United States, for example, the majority of individuals who claim to be Americans are citizens of both the United States, conceived as nation-state, as well as one of 50 political subdivisions, known within the U.S. as “states,” like Massachusetts and Texas. With increasing access to cyberspace via the Internet, Americans may also be cyber-citizens – that is, they are, while in cyberspace, members of a global community that includes citizens of other geo-political-legal sovereign entities. That community does not itself have sovereign status in the traditional sense – indeed, its legal status may be as indefinite as any attempt to pinpoint its physical location, for cyberspace transcends traditional geo-political-legal boundaries.

Notwithstanding the lack of global, top-down regulation in cyberspace, the citizens of cyberspace who regularly access the medium for interpersonal and commercial interactions are all potential contributors to its construction. Through their contribution of content they participate in the development of social norms in cyberspace. In addition, through the user-demand-marketing-codification process, cyber-citizens also influence the development of the structure of cyberspace and the norms that structure will allow. Explicitly or implicitly, they make (or choose not to make) decisions in the physical world regarding how cyberspace is to be managed and organized; they vote by their activities.

Thus, every citizen of every nation-state with access to an Internet connection is potentially a cyber-citizen, and should be interested in a conception of cyberspace that will allow him or her to voice opinions and express views about cyberspace through appropriate national and international channels. For example, a plurality of voices should be involved in the development and adoption of formal regulation by governments or quasi-governmental bodies, the regulation

of market forces in cyberspace, and the otherwise unsupervised ability of code-makers to define the rules of cyberspace.

To hold a decision maker accountable is to hold him or her responsible for a decision in such a way that he or she must respond – perhaps to modify the decision, or at least to provide some explanation for it. Accountability thus requires, at a minimum, some knowledge or understanding sufficient to recognize and evaluate a decision, as well as the will to act on that knowledge or understanding. We focus here on the first requirement: the knowledge or understanding of cyberspace sufficient for cyber-citizens to hold those governmental, market or other actors accountable for such decisions.

### **3. An accessible model of cyberspace**

Aristotle believed that an important component of virtuous behavior is rational, deliberate decision-making, which assumes some basic knowledge. Without a basic framework for understanding, the higher-order process of decision-making becomes difficult – virtue can be threatened by that which we do not understand. The model of cyberspace presented here aims to help reasonably intelligent cyber-citizens to understand the context of decisions made about and in cyberspace, and how they may influence the proper functioning of cyberspace, both at the structural and experiential levels, by holding responsible parties appropriately accountable for decisions that affect cyberspace.

As an initial matter, we use the term “proper functioning” liberally. “Proper” is a value-laden term, and we assume that proper function may include, for some, display of pornography, while for others it means filtering such content. The point is that “proper” should be defined with the participation of users, and not despite them. Proper functioning is related to “proper use,” given that some individuals are positioned to be able to make determinations about how cyberspace *should* function – that is, what the structure and content of cyberspace will be.

It is in the context of proper use, then, that we propose a framework for teaching and learning about cyberspace that may give rise to more virtuous use of technology and social behavior. We believe that all actors ought to have a proportionate understanding of the technology at their hands. Like all tools (hammers, automobiles, knives), ICT can be dangerous if used improperly. ICT can be used to diagnose and treat cancer from a remote location; it can also be used to for hate mongering. If actors are going to promote good uses and discourage destructive ones at both the structural and experiential levels, they need to have a proportionate understanding of the tool and the uses to which it can be put – which uses, in the virtual realm, may be a great many indeed.

And we use the term “proportionate” advisedly. Automobile designers and regulators use an engineering framework in conjunction with driving knowledge to manage the technology as safely and effectively as possible. They must understand the entire process from combustion to air bags to air conditioning, and all within the context of the market; users need to understand less, but still know enough about cars and how they function to participate in discourse about how they ought to be regulated, not to mention the social activity of driving.

Though most computer users have a concept of virtual objects and tools, most likely would agree that their conceptual understanding of both the structure of cyberspace, as well as the experience of being in cyberspace, is opaque. These users, as cyber-citizens, need a framework within which to understand the impact of their actions in cyberspace. Not only must they have a sense of how to use the tool safely (to prevent, for example, carpal tunnel syndrome), they need to know what's behind the veil. Cyberspace at a minimum should be translucent, not opaque.

An appropriate model of cyberspace may go far in providing for the average cyber-citizen some grounding in the nature of cyberspace, the rules of the virtual domain, and how those rules affect traditional, physical world notions of cause and effect. The model proposed here serves several aims. First, it is multi-layered, and therefore reflects the reality of technological systems. Second, the model is comprehensive, internally coherent and maps cleanly onto actual practice, thus enhancing accessibility. Third, it can be extended at any layer and each layer can be explored in detail, to accommodate and enhance a wide array of existing knowledge bases.

### 3.1. The 7-layer OSI model

We begin with the 7-layer OSI model. The International Organization for Standards (ISO), initially developed the 7-layer OSI model to explain the way in which ICT can take information from an intelligible form down to electrical signals, and then back up to presentation. It is important to note that the TCP/IP protocol of the Internet, was developed concurrently with the OSI model, and therefore does not conform precisely to it. Specifically, TCP/IP does not have a physical layer, and it combines the session, presentation and applications layers. We base our proposal on the OSI model because it is more comprehensive (Martin, 1994).

The OSI model is structured as follows:

<b>The Seven-layer OSI model</b>	
<b>Layer</b>	<b>Description</b>
1. Physical	Mechanical and electrical structure of the system
2. Data Link	Blocks of data (frames); error and flow control
3. Network	Making and managing connections between network nodes
4. Transport	Transfer of complete data sets between end-points
5. Session	Communications between applications
6. Presentation	The interface between software applications and communication data
7. Application	User-access to the network environment

Each layer may be explored in at least four domains: in respect to technology, regulation, innovation and ethical considerations. Both high-level and specific understanding is possible, depending on the knowledge base and interest of the actor.

#### **The physical layer**

The physical layer connects devices to one another. It consists of wires, fiber-optics, satellites, transmitters, receivers and so-on. This is the one and only layer of hardware. The science of the

physical layer involves everything from radio transmission to microprocessor engineering and manufacturing to geo-synchronous satellite orbit.

Beyond basic operational requirements, regulation of the physical layer revolves around safety and keeping signals contained. Thus governmental regulations require that a computer chassis be grounded, reducing the risk of electrical shock and minimizing radio-frequency interference.

In 1965, Gordon Moore proposed that transistor density would double every 18 months. The Intel 8008 processor, introduced in 1972 had 2,500 transistors. The Pentium 4, introduced in 2000, has 42,000,000 (Intel, 2004). Moreover bit strength and memory have increased concurrently. The original Apple computer was an 8-bit machine; now 64-bit chips are starting to appear in personal computers.

The physical layer has an ethical dimension. Hardware has direct environmental impacts. Systems emit low-level radiation, and keyboards can cause wrist injuries. The manufacture of devices produces toxic waste, and safe disposal of used ICT equipment is posing an increasing problem.

### **The data link layer**

At the data link layer, information is broken down into packets (“frames” or “datagrams”), transmitted to a remote receiver, and then reassembled. Packets contain addresses for the sender and the receiver, encryption and error control. An e-mail transmission may be sent as many frames. On the Internet, these packets may be sent by different routes, and may even arrive out of sequence. The receiver will sort out the data, strip off control data, and re-assemble the e-mail as it was sent. The science of the data link layer includes Internet addressing, encryption and datagram error correction.

Regulation at the data link layer is largely dictated by technical constraints: if the protocol is not built and followed correctly, it won’t work. New protocols are difficult to develop because existing protocols are deeply subsumed into systems. Subsumption ethics suggests that regulators and innovators should perform extensive stakeholder impact analysis should be performed before any changes are made to operational specifications at subsumed layers.

### **The network layer**

The network layer manages connections between computers, including the routing of data packets through the network. The science of the network layer includes network structure, maintaining routing tables, the “uniform resource locator” (URL) system and Internet domains.

Regardless of the form regulation of the network layer takes, regulators should understand that the open nature of the Internet occurs here. It is possible to browse the Internet because computers without prior authorization can find each other. Regulators could, for example, restrict domain names to only certain users, effectively censoring the Internet. Decisions about universal connectivity, domain name management, availability of domain name services (DNS) all have ethical dimensions.

### **The transport layer**

The transport layer ensures that data received matches data sent. Once packets have been re-combined into complete data sets, such as a long e-mail message, the transport layer ensures that the e-mail is complete – that a section has not been left out of the middle. The transport layer requires mathematical algorithms for error checking and correction.

Like the data link layer, regulation at the transport layer is largely dictated by technical constraints. Nonetheless, innovation and concomitant ethics issues arise as corporations and individuals vie for position as authors of protocols.

## **The session layer**

At the session layer, programs share a protocol to structure and send information to each other. For example, the two computers may have different e-mail programs, but both use a common protocol to encode the recipient, sender, cc, subject and body of the message. That way the recipient sees what would otherwise be gibberish with a message buried somewhere inside it. HTML, the basic language of the World Wide Web, is another such protocol.

Regulation of session layer protocols is both difficult and important. The session layer can facilitate sharing information, or complicate it. Protocols like HTML, XML and SMTP work because they are standardized across platforms. While these protocols have been developed by the private sector, they have now become subsumed, and are difficult to change. At the same time, corporations and consortia can gain significant leverage by coming to own intellectual property rights to a given protocol. Thus the ethics of the market and government regulation play a significant role at the session layer.

## **The presentation layer**

The presentation layer converts data from the format of one system to another. This is the lowest layer that addresses the *meaning* of data. For example, one system may encode dates as mm/dd/yy, where another uses yyyyymmdd. For MS-Word for Macintosh and Word for Windows to exchange data files, data must be converted at the presentation layer. There is less science than logistics at the presentation layer, where programmers must understand the differences between systems.

Regulation at the presentation layer has been driven by market interests – protocols are compatible when it is in the interests of companies to make them so. Compatibility may be blocked to improve competitive advantage. Innovation encompasses a vast array of meaningful data. Because of the diverse impacts of presentation, ethics issues tend to revolve around those with an interest but no voice.

## **The application layer**

At the top of the OSI model, the application layer provides user access to information on the network. For example, the application layer enables a user to retrieve a file list and open a file from a remote location. It invokes the lower layers to actually obtain the list and content, and it is unconcerned with how the request is transmitted.

The application layer determines what resources will be available to users. Regulators at this layer must negotiate with corporate motives to publish or withhold their resources. For example, Microsoft offers clip-art as part of its Office suite, and extended clip art through the web. On-line clip art is available within the general clip art interface. This is an added-value service that makes Office more desirable. Other services provide clip art for a fee, but it is usually not available from inside the Office user-interface. Thus it becomes less attractive.

There is room for significant innovation at the application layer – more and more information can be made available to users, and made increasingly accessible. Internet portals, for example, have been evolving for years, and continue to increase the availability of content.

### 3.2. Three new layers

The traditional OSI model was developed by and for engineers. Its domain ends before taking humanistic issues into account. In order to generalize the model, we suggest adding three layers to the OSI model to address the human side of cyberspace: user interface, interpretation and impact. These 10 layers provide a seamless model that allows users to understand both the effects of ICT and the underlying technology, to the extent that they need to in order to make rational, informed decisions, depending upon their particular responsibilities.

8. User Interface	The immediate connection between the user and cyberspace; access to content
9. Interpretation	User understanding of system content
10. Impact	The effects that systems and content have on stakeholders (including society)

#### User Interface

The user interface (UI) is immediately visible; and is comprised of output and input, such as the graphic images, text and sound that appear on a user’s video and audio devices, like a computer, personal digital assistant or cell phone, and keyboards, mice and other input devices. Through the interface, the user interacts with content and people in cyberspace. It connects users to subsumed artifacts that have accumulated over time, like magazine archives, as well as content that is instantly updated, like the weather or live chat. User interfaces in this way serve to mediate the individual users’ excursions into cyberspace and the purposes for which they enter, whether the purpose is to check e-mail, shop or engage other users in on-line gaming.

The images, text, sounds, keystrokes and clicks of the interface allow individuals to communicate with each other in cyberspace; these are the language through which cyberspatial norms are being constructed by cyber-citizens, whether intentionally or not. Indeed, the interface is itself an artifact, one that deliberately masks (in order to mediate) the way in which cyberspace operates at a technical level.

Most user interfaces are developed to achieve a particular end. The results vary considerably, from clear and accessible websites to convoluted quagmires of disparate material. By nature of creativity and the market, regulators have little control over the UI. And yet, a mediocre user interface can lead to unforeseen consequences (see, for example, the Therac 25 case). Accessibility by the variously-abled also becomes an issue at this layer.

The user interface may be the single most malleable aspect of cyberspace. Graphic artists and programmers come together here. Musicians ply their wares through the UI, and the possibilities of “A/V footage” are as broad as the medium itself.

The ethics of the user interface are complex. Ethical analysis of the UI must be both broad and pointed, accounting for widely distributed software that is nonetheless used by specific people for specific purposes. Much of the public discourse about good and bad software occurs at this layer.

## **Interpretation**

As an artifact which engages human interaction, the UI and, by extension, all of cyberspace, requires some interpretation by the user: the user must locate within his or her own knowledge and experience what he or she is seeing on the screen and give it some meaning. This effort at interpretation is frustrating without some relation back to the more technical layers of the framework: a basic literacy is required. Some understanding of the way in which the rules that govern action and behavior in cyberspace are programmed, at the technological level, and socially constructed, at the level of interactions among individuals in cyberspace, is essential to user interpretation (and hence the value) of information, as knowledge of language is required in order to read. Moreover, the rules of cyberspace at the programming level are mutable, unlike the mechanical rules of the physical universe, and that fact necessarily influences efforts at interpretation.

Interpretation will depend on the content a user is accessing, and the context in which that content is viewed. Indeed, context is crucial: unlike a printed book or film, the sequence of cyberspatial content is not pre-determined. Thus the interpretation of cyberspatial content can be significantly more varied than with traditional media, and the varieties of possible interpretation pose a challenge to regulators. The problem is amplified by the fact that cyberspace transcends state and national borders, so accounts of interpretive possibilities related to particular content must be multi-cultural.

As a result of efforts to draw attention, sell products or push boundaries, cyberspace hosts continuous innovation designed to evoke ever more intense, complex or subtle interpretations from users. Web sites are updated constantly, since stagnant sites will tend to draw less attention, while chat rooms become experimentation labs for young people seeking self-knowledge. The desire to be evocative drives innovation that bends and breaks social barriers, pressing individuals to become more self-aware at the same time that they may be increasingly confused about what is expected of them.

And yet, cyberspace is an intensely social medium: many cyber-citizens enjoy multithreaded chat sessions running all day long with other users, while others maintain continuous information gathering from the web and communication by e-mail and voice-over-IP telephony. In all these interactive processes, interpretation of information is continuously required; in the mature user's experience, cyberspace-mediated content may be tightly integrated into all daily activities, useful to the degree that it is intelligible.

## **Impact**

Using any tool in the physical world, we are expected to have some knowledge about its potential impact on others. From cars to kitchen knives to weaponry, tools misused lead to suffering and death. No less so ICT and cyberspace: a programming change that creates a more

efficient way to store users' purchasing information may also lead to the greater possibilities of privacy loss or identity theft if security issues are not properly addressed.

Actions taken in cyberspace, through user interfaces and as the result of interpretation, directly and indirectly affect stakeholders – cyber-citizens, and also the government and corporate market actors that occupy and rely upon cyberspace as a medium of communication and commerce. The effects of decision-making within cyberspace, as well as the effects of decision-making about cyberspace, may be unknown to stakeholders. And those stakeholders may be difficult to identify, given the intentional and accidental anonymizing capacity of digital communication.

This layer of the model, again with reference as necessary to the lower layers, presents an opportunity for discourse about the ethical implications of decisions about and in cyberspace. Agents have an ethical responsibility to think through the potential impacts of their cyberspatial activities in advance, and cyber-citizens should also feel obliged to question the ethics of decision-making that affects the structure of cyberspace or the development of social norms therein.

#### **4. A model for teaching and learning**

To draw all 10 layers of the extended OSI model together: Stakeholders can be affected by cyberspace in myriad ways, but they can also attempt to predict the impacts of their own activities on others. These impacts are subject to interpretation, and so impact analysis immediately requires the interpretation layer. Interpretation depends on the user interface to be meaningful. And the user interface will not operate without the smooth functioning of the seven traditional layers of the OSI model. And all of this must be understood as requiring some interplay with daily life in the physical world.

Thus traditional ethics, cyber-ethics and Internet technology must be interactively coherent. The ethics of particular activity in one space must align with the ethics of the equivalent activity in the other, while at the same time acknowledging the important differences between the ways in which cyberspace and the physical world operate. Individuals seeking to develop character must exercise virtuous behavior in cyberspace just as they would in the physical world. To do so with informed deliberateness, they must understand not only the impact of their cyberspatial activities, they also must have some sense of various layers of cyberspace as featured in the extended OSI model we propose.

This model has both breadth and depth. A user could enter the model at whatever layer fit his or her aptitude and training. This would encourage engineers toward better understanding of the impact of their activities, and it would encourage young “gamers” to dig into the technology behind their play. For most citizens, it would provide a rubric against which to measure their understanding and, therefore, their potential to influence policy by holding decision-makers appropriately accountable. Using this model, cyberspace can be approached from multiple perspectives, at whatever degree of detail is needed by a given individual, and accounting for generational and cultural differences.

#### 4.1. The model along generational lines

Both older and younger generations may benefit from the extended model, though additional study must be undertaken to determine the level of understanding of the model by various age groups. For many users born before 1965, a theoretical approach will likely prove more accessible. By habit, many such users will want to *understand* first and *do* second. Many users born after the 1960s may be comfortable with experimenting; for them, it may be better to explain the OSI model in terms of their experience, through examples and explanations of technology they have either seen or can experiment with. Obviously, there will be exceptions to these generalizations; the point here is that the model we propose should provide entrée across generational lines.

#### 4.2. The model in a multicultural context

The extended OSI model has cross-cultural and multi-lingual application. The traditional 7-layer model, concerns universal technical requirement and is, by its nature, reasonably culture-independent. Use of the upper three layers, interestingly, should reveal varying interpretations from different cultural perspectives. Those varying cultural interpretation will affect the impact of ICT decision-making and should influence regulatory preferences across traditional geo-political-legal boundaries – a diversity of views on the management and organization of cyberspace that might not be seen absent cyber-citizens who possess some knowledge and understanding of the nature and structure of cyberspace.

#### 4.3. Thoughts on where the model could be introduced

The following table suggests potential points of entry for introducing the 10-layer model in various educational environments. From the entry point, the model can be explained in a naturally accessible way, up or down through the layers, to allow students both basic understanding and the possibility for more extensive learning.

Forum	Extended OSI layer:									
	Phys	Data	Netw	Trans	Sess	Pres	Appli	UI	Interp	Impct
High School	✓						✓	✓		✓
Vocational	✓	✓	✓	✓	✓	✓	✓	✓		✓
Corporate User							✓	✓	✓	✓
Adult General							✓	✓	✓	✓
Adult Professional	✓		✓				✓	✓	✓	✓
University										
- Comp. Science	✓	✓	✓	✓	✓	✓	✓	✓		✓
- Mathematics		✓	✓	✓						
- Physics	✓	✓								
- Philosophy								✓	✓	✓
- Ethics	✓		✓				✓	✓	✓	✓
- Graphic Arts							✓	✓	✓	
- Government			✓		✓			✓		✓
- Business					✓		✓	✓	✓	✓
- Law								✓	✓	✓

## 5. Conclusion: An Accessible Conception of Cyberspace?

In our paper *Toward an accessible conception of cyberspace*, we argued that a baseline understanding of cyberspace is required by a plurality of users in order to hold actors who make decisions about or in cyberspace accountable. We believe that the extended OSI model we propose could serve as a core model in teaching people about cyberspace and the way in which it operates, to the end of moving cyber-citizens toward a practical understanding – one that lends itself to rigor and depth of analysis, where the learning of non-technical people dovetails with the knowledge being used by designers, engineers, marketers and regulators.

### Acknowledgments

For their feedback on “Towards and Accessible Conception of Cyberspace,” our thanks to Deborah Johnson, Lucas Introna and Kari Gwen Coleman; for suggesting the OSI model as a teaching tool, Keith Miller; and for their ongoing support and encouragement, Don Gotterbarn and Simon Rogerson.

### Bibliography

Gleason, David H. “Subsumption Ethics.” *Cyberethics: Social and Moral Issues in the Computer Age*. Amherst, New York: Prometheus Books, 2000: 56.

Gleason, David H. and Friedman, Lawrence. “Toward an Accessible Conception of Cyberspace.” *Vermont Law Review* 26 (2003): 1.

Martin, James: *TCP/IP Networking: Architecture, Administration and Programming*. Englewood Cliffs, NJ: Prentice Hall, 1994.

Intel, “Moore’s Law” - see <http://www.intel.com/research/silicon/mooreslaw.htm>. accessed 1/14/04.

Shklar, Judith N. *American Citizenship: The Quest for Inclusion*. Cambridge: Harvard University Press, 1991.

Stallings, William: *Data and computer Communications*. New York: Macmillan Publishing, 1988.