Stratospheric Transparency: Perspectives on Internet Privacy

Rita M. Hauck, Associate Professor, Fort Hays State University

Abstract

As a parent of teenagers in the 1980s, I recall a concern of the intrusion by MTV into our home. After futile attempts to block the program, my spouse and I set out to convince our sons of its intrusion. Our challenge was miniscule when compared to the Internet privacy issues of today. This paper addresses such challenges and proposes some guidelines based on research and experience that may help Internet users to strike a balance between the advantages of social networking and virtually limitless information access, and possible calamities wrought by Internet intrusions and personal privacy breaches. The concept of "stratospheric transparency" touches the social responsibility of what to put in cyberspace, a cyberspace prophylactic that may encourage people who use the Internet to ask themselves questions such as, "Do I want to live in an Internet fishbowl?" "Would I want my most respected relative or friend to see my post?" "Am I using the same standards for behavior in Cyberspace that I use at home and at work?" and, "If I do not have any standards when I 'surf the Net' is this a time of my life when I should seriously avoid Cyberspace?"

This paper relates the "Karman line" (highest atmospheric altitudes of the earth) to the possibilities for innovation and wisdom in the future development of Cyberspace. Some people are traveling into Cyberspace without knowledge about how they are influenced by activity there, and without knowledge that they can influence its development and help keep it from litter and pollution. It is as if they are traveling into space, not realizing that to maintain altitude at that level, one must travel faster than the rotation of the earth.

Introduction

For purposes of this paper, although there are many possible historical and other differentiations among them, the Internet, E-mail, Text Messaging, the World Wide Web, and Cyberspace are lumped together as "Cyberspace." Cyberspace contrasts starkly to the "real world" for many of us. It is a "digital world" that involves interactivity much like the "real world" but a world that keeps records and databases that have the flavor of yesterday's science fiction fantasies. The word *cyborg* appears occasionally and refers to users of Cyberspace. The term was coined in 1960 and later used in a 1965 book about a "new frontier" bridging "inner space to outer space," between "mind and matter." It serendipitously coincides with the concept of stratospheric transparency and the preparation for travel in space. "Clynes and Kline created the cyborg technique as a means to alter the bodies of astronauts so they could survive the harsh environment of outer space, an alternative to providing an earthlike environment for space travel" (Kline 2009, 3). The word *cybernaut* fits with that concept. The word *cybersect* implies cyborgs or cybernauts with a collaborative agenda. There were 3,940 Google *hits* for the term on July 17, 2009, a relatively new term in comparison with cyborg that boasted 6,990,000 hits.

"Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations" (Clarke 2008b, 2). Clarke provides a reminder that there are different cultural perspectives about privacy. When a person puts content in Cyberspace, does he or she consider whether or not it may be offensive to another culture? Does the person consider how the content will impact boundaries, freedom, and privacy on the Internet? For example, do the people who participate in gambling and pornography in Cyberspace when it is illegal in their geographical location consider that their actions spawn increased government interest in regulation of Cyberspace as well as increased interest in surveillance?

Concern about the unknown possible calamities due to the gullibility and naiveté of typical cyborgs inspired this paper. People join social networks in Cyberspace daily, placing their pictures, their friends' pictures, videos, and other information about themselves, their families, their work, play, and their friends without much apparent regard to consequences or with a seeming blind trust in the owner of the space to protect them from the unknown. Perhaps they believe there is an invisible protection from anything and everything, even from the paparazzi, that might turn their individual experience into something less than pleasurable. Without caring to read the fine print to learn about who owns a particular website and to understand the site's privacy policies, purpose or history, cyborgs of various ages seem to leap to the conclusion that the site meets their own personal and basic expectations for security. There may be a brief consideration and decision that the convenience, services, or self-satisfaction provided by the site must exceed any possible breaches or loss of privacy.

Most people would be shocked to know how easy it is to trace where they go on the World Wide Web. The Internet Protocol (IP) address of our computer is a given to the server computer when we ask for information from a web site. Lessig (2006) described Single Sign-on (SSO) technology that allows the surfer to return without signing in each time, and Geoselect and Hostip.info, IP mapping services (Lessig 2006, 58). Clark described "PITs" and "PETs" PITs are privacy-invasive technologies, while PETs are privacy-enhancing technologies (Clarke 2008b, 2). Based on his pilot study of Business-to-Consumer (B2C) privacy policy statements, Clarke noted that it appeared that businesses, including not-for-profits, do not come close to meeting consumers' reasonable expectations for protection of personal data (Clarke 2008b, 8). If that's the case, and with the assumption that the majority of businesses have some inclination toward the improvement and greater good of society, consider what a criminal mind would do with personal data. Clarke concluded that there is a need for more studies about consumer understanding regarding "privacy-protectiveness" and the consumer decisions to continue with companies based on that understanding (Clarke 2008b, 8).

Concealment of evidence about "where we have been" is no longer the sole refuge of perverts. Most of us would say that it "is none of your business" to companies who want to track our searches on the web, no matter where we are searching. We don't want people stalking us as we run daily errands, but we seem to nonchalantly care when it's in Cyberspace. The browsers know that a majority of consumers care. Firefox is playing "catch-up" with other browsers as it

recently added several features designed to allow users to prevent others from discovering their web search.

Challenges

The possible calamities wrought by Internet intrusions and personal privacy breaches have led one person to list ten ways to improve security when using Facebook. O'Neill (2009) explained ten privacy settings for Facebook users such as how to use Facebook friend lists, how to avoid Facebook searches, and how to avoid unwanted photo and video tags. A tag involves Facebook *User1,* for example, putting Facebook *User2's* name with a picture on *User1's* page, automatically placing a link to the picture or video on *User2's* page. The ten privacy settings are followed by comments from Facebook subscribers and ex-subscribers. In response to the tips about how to use, remove, protect, prevent, make and keep private, and avoid embarrassment, one of the 268 responders as of April, 2009 commented, "[I] Don't use Facebook. Works wonders, everything stays nice and secure" (O'Neill, 2009). Abstinence remains the ultimate prophylactic to ensure Cyberspace privacy. Dummies.com has additional information about how to use Facebook, including information about privacy settings at http://www.dummies.com/how-to/internet/Blogging-Social-Networking/Facebook/Facebook-Photos-and-Video.html.

The concept of "stratospheric transparency" touches the social responsibility of what to put in Cyberspace, a Cyberspace prophylactic that may encourage people who use the Internet to ask themselves questions such as, "Do I want to live in an Internet fishbowl?" "Would I want my most respected relative or friend to see my post?" "Is my behavior transparent?" "Am I using the same standards for behavior in Cyberspace that I use at home and at work?" and, "If I don't have any standards when I 'surf the Net' is this a time of my life when I should avoid Cyberspace?" Lessig notes, "We should understand where we are going, and why, before we ask whether this is where, or who, we want to be" (Lessig 2006, 38).

Part of the reason that the MTV asymmetrical cultural intrusion of the early 1990s seems miniscule in 2009 is that it was not an interactive threat. Our sons weren't experimenting with interactive content, being invited to become actors to a world audience. They were watching actors and content that did not meet our own quality standards for good role models. In talking with a friend about how difficult it is for her to quit smoking, I was reminded again about the importance of role models and concerns about intrusions to privacy. Part of my friend's problem related to the role model that was ingrained in her. Her mother, a heavy smoker, was fifteen when Heather was born. Today, twenty-six years later, her sister tells her, "You look like Mother when you smoke." MTV and my friend's mother did not present the kind of "perpetrator" who sets out to steal identities and to surreptitiously invade privacy for criminal purposes or who invents "online scams defrauding the gullible" in Cyberspace (Jamieson 2008, 3-4) or models criminal behavior in Cyberspace.

Until recently, most users of the Internet did not seem concerned with the regulation of "web spiders, which gather data for web search engines; browsers, who are searching across the Net for stuff to see; [or] hackers…" (Lessig 2006, 170). In discussing recent, what I call, *cyber-outrage* at auto-warranty telemarketing scams and an attempt by cyborgs to take matters of

justice into their own hands, Fowler (2009) reported about a company that received the brunt of the outrage although the company was yet to be subjected to legislative and judicial scrutiny and action. Fowler quoted Silveira's description of the Internet: "It's as if we all live in one small town in an old Western movie, and once your picture goes up on the bulletin board as wanted for some deplorable crime, nobody forgets" (Fowler, 2009).

Awareness of the challenges has launched online resources for Internet consumers such as eConsumer.gov, available in several languages. With participation by consumer protection agencies in 24 countries and the International Consumer Protection Enforcement Network (ICPEN), eConsumer helps solve cross-border complaints. Jamieson (2008) noted that the International Criminal Police Organisation collaborates with its 186 member countries. He noted that the "Convention on Cybercrime of the Council of Europe is the only binding international instrument on the issue of cybercrime" (Jamieson 2008, 24-25). Svantesson (2009) discussed the pros and cons of geo-location technologies. A negative aspect of geo-location technologies is the attempted regulation of Internet content such as China's recent efforts, with "the potential to destroy the Internet's borderlessness" (Svantesson 2009, 3-5). An expressed concern was that more people would want the geographical regulation than not. The recent concern and opposition to China's regulation of its citizens' use of the Internet sends a vote of confidence for borderlessness. Part of the challenge is to retain the borderlessness while simultaneously preserving justice, fairness, and responsibility. For example, Patrick (2009) noted, "The anti-piracy provisions, which are only one part of the government's 'Digital Britain' report, are part of a broader clampdown across Europe, which U.S. entertainment companies have long complained isn't doing enough to stop."

Advantages of Social Networking

The advantages of social networking must seem obvious to both "good and bad" cybersects, cyborgs, you, me, us, and them. Alexander (2004) made reference to Arquilla's and Ronfeldt's book "Swarming and the Future of Conflict" and described the concept of swarming that dates back to pre-Napoleonic times. Like insects, cybersects organize into swarms. Cybersects develop social networks and gain momentum for a collaborative agenda. Reverting to "challenges" for a moment, there seem to be concerns about pollution of Cyberspace and the various swarms congregating there, and most certainly concerns about privacy issues and perspectives. All the while, we are able to communicate at a faster pace, in *real time* as never before. We are able to help or at least encourage people in countries such as Iran and assure them that they have support when they desire peace and freedom, for example.

Possible Calamities and Unpredictable Consequences

Research provides an example of an unpredictable consequence of providing too much personal information in Cyberspace. In describing the research of Acquisti and Gross at Carnegie Mellon University, Schaffhauser (2009) noted that "public information gleaned from governmental sources, commercial databases, and online social networks can be used to routinely predict

most—and sometimes all—of an individual's nine-digit Social Security number." The research made reference to "fraudsters" using "botnets." Jamieson provided a list of federated identity management solutions: Liberty Alliance (www.project liberty.org); Microsoft Passport (www.passport.com); WS-Federation (by IBM and Microsoft); Security Assertion Markup Language, SAML, and the Organisation for the Advancement of Structured Information Standards (OASIS). He noted that "The Convention on Cybercrime of the Council of Europe is the only binding international instrument on the issue of cybercrime" (Jamieson 2008, 14). The Federal Trade Commission in the United States offers a free brochure "Deter, Detect, Defend" and other materials to help better understand fraudulent activity on the Internet, and to help protect and defend oneself against identity theft. For more information, go to http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter-detect-defend.html.

The present attempted regulation of Cyberspace access is focused mainly on providing layers of protection and boundaries rather than teaching "young people" and "not-so-young people" to make wise choices and to be prepared for travel across boundaries. Lessig noted that

> "…some of these choices involve values that are collective…We are at a stage in our history when we urgently need to make fundamental choices about values, but we should trust no institution of government to make such choices" (Lessig 2006, 8). He elaborated about his own choices…"I have choices in real life, but escaping the consequences of the choices I make is not one of them" (Lessig 2006, 11). "We should worry about a regime that makes invisible regulation easier…and makes it easier to regulate…invisibility makes it hard to resist bad regulation…we don't yet…have a sense of the values put at risk" (Lessig 2006, 136). Lessig presented a sense of optimism about our potential ability to control freedoms in Cyberspace while perpetuating a shared value system, "When we know what values we want to preserve, we need only be creative about how to preserve them" (Lessig 2006, 165).

For example, in a crowded carnival, most people are prepared to guard their pockets, in front and behind as they know there are likely to be pick-pockets in the vicinity. The risk of being naïve or careless will be loss of known valuables. One can only wonder if Lessig's observations are applicable to the next generation of Cyberspace users. Indeed, many of them may not even come to know how to make such choices.

Recent studies of "text messaging" seem to suggest that young people have a significant concern for privacy in this realm when it comes to parental viewing of messages. A study reported by cellular-news estimated that 33% of teens had received a "sext message," a message with sexual content. The company that sponsored the research has developed a "de-texter" (DTXTR) for parents and others at www.LGDTXTR.com (Cellular-news, 2009). Do the teens consider that once they send their messages, they are no longer private? The "sexting" phenomenon illustrates an extreme example of youngsters deliberately eschewing their personal privacy while hoping their parents don't notice or care.

Allen (2009) quoted an occupational health sciences professor Dr. Peter Johnson's recommendation about teen texting: "enjoy everything in moderation, including moderation." Breuner (2007) noted that this extension of social communication and relationships frequently

interrupts teens and their families in the middle of the night when the alert of a new message arrives, leaving all without enough sleep for the next day. She recommended that parents build trust by letting their teens know they can keep the device when they can be trusted not to turn it on during bedtime hours. Other researchers have expressed concerns about the generation of *texters* losing the subtleties of social intercourse that only come from physical presence during the communication with a wide spectrum of non-verbal communication tools such as facial and other visual cues for expression that people practice in "real life outside of Cyberspace." Allen noted that a linguistics and communications professor Crispin Thurlow is not alarmed about the teens' development as new literacies emerge.

What valuables do we have to lose in Cyberspace? What is our fitness level? Having lived in Los Angeles, New York City, Jersey City, and Miami, I recall our built in and practiced precautions such as "Avoid talk with strangers," "Blend in rather than stand out," "Don't look strangers on the sidewalk in the eyes, walk quickly, don't linger, and have an air of confidence." In Jersey City, on a public bus, I put my purse over my shoulder as new people arrived on the bus. I was asked by an approaching passenger, apparently offended by my conduct, "What's wrong? I'm not going to clip you." A purse snatcher on the subway in Barcelona was so surprised at my aggressive response to his crime that he handed back my property and one of his companions actually apologized. People enter Cyberspace daily without giving a thought to preparations and precautions, or not having heard "Safety in Cyberspace" instructions. We may not be aware of risks due to not understanding the schemes of a criminal mind or a "bottom-line mind." Frequently, they are similar to the pick-pocket, but much more subtle. Users in Cyberspace need to be aware of "cookies" and, as Lessig calls them, "mouse-droppings" (Lessig 2006, 203). He noted that fictitious names (of which I have a few) make a person "feel safe" (Lessig 2006, 46). Steele (2009) touched on efforts to develop what Lessig called authentication systems.

Our nephew and his fiancé financed much of their tuition at Stanford University with their Internet poker winnings. The recent flurry of legal responses to internet gambling have created significant invasions of bank customers' rights and privacies as the authorities now routinely monitor transactions to curb this activity. For more information, refer to the Testimony of the United States Federal Reserve's Louise L. Roseman, April 2, 2008 at http://www.federalreserve.gov/newsevents/testimony/roseman20080402a.htm. When asked how this has affected their poker playing, our nephew replied that the "savvy" gamblers have all figured ways around the restrictions and continue to play. They said that their main problem now is that the inexperienced players—from which most of their winnings had been drawn—have now disappeared from the action, and the remaining players are much harder to beat.

Clarke (1999) expressed his concern that his and other authors' warnings about "enormous impacts…these technologies can have on individuals and society, both for good, and for seriously ill …fell on deaf ears" (Clarke 1999, 3). In describing Cyberspace, he noted, "The Internet has created new kinds of 'space', within which human actors are disporting themselves …the participants indulge in a 'shared hallucination'" (Clarke 1999, 4). Perhaps my fear of the

unknown future dangers for the gullible or the naïve includes that they may subject themselves to harassment and electronic stalking, "impersonation, masquerade, identity fraud and identity theft" (Clarke 1999, 5; 2008a, 3). Stratospheric transparency embraces the need for preparation by means of social responsibility and guidance as we enter "thinner" zones with no endpoint except the imagination, regulation, and code. No longer falling on deaf ears and still good advice ten years later, "the ongoing explosion in cyberspace activity, and the wide variety of behaviours it exhibits, demand attention by both professional and theoretical ethicists" (Clarke 1999, 8).

Friendly Fire

Some of the less serious intrusions to our privacy but nevertheless time-consuming and time-disrupting come as e-mail messages are forwarded "in bulk" by friends or acquaintances who less-frequently send us something we may actually want to read. Many threaten a superstitious outcome such as, "if you don't forward this to eight friends, you will be financially *broke* in eight days." Some Netiquette Guidelines state, "Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your local system administrator if your ever receive one" (Hambridge 1995). Do you know anyone reading Netiquette Guidelines? Should we send guidelines to the acquaintances in response to each intrusion? It seems obvious to many people, that only humans make the code used in Cyberspace, yet it does not seem so obvious to the people who elevate some of the activity there to supernatural levels of power. A virtual place! That's all Cyberspace is – figments of imagination and interactive figments limited by code. Some users have a little too much enthusiasm on the uptake. Many people put everything "out there," on their websites and postings without consideration of consequences, even violating obviously apparent intellectual property rights by stealing information or images from other websites without giving credit or asking for permissions. Rather than write a personal message to a friend, some choose to "stay in touch" by "bulk forwarding." It seems like a quick way for them to say "Hello" to all their friends and acquaintances in one easy click. Their bulk forwarding may be a hoax; One can easily verify or debunk suspect material at http://www.snopes.com/info/whatsnew.asp.

Guidelines based on research and experience

Whether traveling in public spaces around the world or stratospheric places in space or Cyberspace, there is clearly a need for regrouping, knowing what tools to take, knowing the "must takes," and the related costs. Steele (2009) reported that advertisers and others will announce guidelines to help consumers to be better informed about data being collected and how it will be used. Efforts are underway to allow consumers to request that their data not be used. It will come as news to many consumers that their web searches are being recorded by some companies. The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. that works with Privacy International (PI) to provide guidelines at privacy.org. PI is a human rights group based in London with an office in Washington D.C. One of the resources from privacy.org is http://www.privacyrights.org/links.htm with extensive links

and blog resources including links to "Privacy Sources in Academia." In the United States, the Consumer Product Safety Commission and the American Academy of Pediatrics puts a seal of approval on books such as *Online Family: Your Guide to Fun and Discovery in* Cyberspace by Preston Gralla.

A Google search for "netiquette" revealed 6,140,000 "hits." One of them located at http://www.stanton.dtcc.edu/stanton/cs/rfc1855.html can be used and revised by any individual or organization. It has guidelines for "One-to-one communication, which includes mail and talk; One-to-many communications, which includes mailing lists and NetNews; and Information Services, which includes ftp, WWW, Wais, Gopher, MUDs and MOOs" (Hambridge 1995). One can only wonder what effect this interest by our generation in such subjects will have on the upcoming generation of *texters* and *sexters*.

At http://www.albion.com/netiquette/corerules.html one can learn about the "Ten Core Rules of Netiquette" excerpted from *Netiquette* by Virginia Shea: 1) Remember the Human, 2) Adhere to the same standards of behavior online that you follow in real life, 3) Know where you are in cyberspace, 4) Respect other people's time and bandwidth, 5) Make yourself look good online, 6) Share expert knowledge, 7) Help keep flame wars under control, 8) Respect other people's privacy, 9) Don't abuse your power, and 10) Be forgiving of other people's mistakes. There are also "Ten General Security Rules" from *Unix System Security Tools* by Seth T. Ross, published by McGraw-Hill posted at http://www.albion.com/security/intro-8.html#pgfId-446947: 1) Security Through Obscurity Doesn't Work, 2) Full Disclosure of Bugs and Holes Benefits Security, 3) System Security Degrades in Direct Proportion to Use, 4) Do It Right Before Someone Does It Wrong For You, 5) The Fear of Getting Caught is the Beginning of Wisdom, 6) There's Always Someone Out There Smarter, More Knowledgeable, or Better-Equipped Than You, 7) There Are No Turnkey Security Solutions, 8) Good and Evil Blend into Gray, 9) Think Like the Enemy, and 10) Trust is a Relative Concept.

Gateway to Censorship and Regulation

Most people seem to live under some type of government authority and regulation except perhaps lawless places such as Somalia. It shouldn't come as any surprise that governments want to apply authority and regulation to the Internet. According to Lessig, "Governments are necessary to protect liberty, even if they are also able to destroy it. But neither does the answer lie in a return to Roosevelt's New Deal. Statism has failed. Liberty is not to be found in some new D.C. alphabet soup (WPA, FCC, FDA…) of bureaucracy…ask questions that avoid dead-ends" (Lessig 2006, xv).

Lessig presented the question, "Which sovereign should govern" in Second Life, for example? In discussing "a world drowning in spam, computer viruses, identity theft, copyright piracy, and the sexual exploitation of children," he noted, "if some government could really deliver on the promise to erase all the bads of this space, most of us would gladly sign up" (Lessig 2006, 27). He presented "a single normative plea: that all of us must learn at least enough to see that technology is plastic. It can be remade …to reflect any set of values that we think

important. The burden should be on the technologists to show us why that demand can't be met …under the architecture that I believe will emerge, cyberspace will be the most regulable space humans have ever known" (Lessig 2006, 32). Lessig described *The Generative Internet*, an article by Zittrain. This would be the stratospheric level, "an extraordinarily innovative ('generative') platform for invention …But we …don't pay enough attention to the bad" (Lessig 2006, 74). Lessig described various cyber-places, one of them being AOL where AOL makes the decisions about control of "rules, norms, prices, or architecture" for over 27 million subscribers (Lessig 2006, 88-94). Among the open code described are PGP (pretty good privacy) made available by Zimmermann and the Free Software Foundation over 15 years ago.

Contrast our concerns with the intrusion of "MTV actors" into our living room via television in the 1990s with the concern of the Chinese government in 2009 about certain web sites that may be harmful to young people. The Chinese government attempted to require all personal computers sold in China after July 1, 2009, to be packaged along with software called Green Dam – Youth Escort. When installed on the PC, the filtering software blocks certain web pages deemed violent, pornographic, or otherwise inappropriate for young people. Appropriate pages are called "green" pages in China. According to Bodeen (2009), the software is topic-oriented and "users who have tried it say it prevents access to a wide range of topics, from discussions of homosexuality to images of comic book characters such as Garfield the cat" (Bodeen 2009, 1). Chao noted that some computer companies were concerned that by choosing the Chinese market they might be accused of "abetting censorship" (Chao 2009, 1). China is also the second largest market for computers.

The Chinese government's attempt to only allow a "green" Internet in China was put on hold, apparently from the efforts of companies who stated they couldn't make the deadline and from efforts of Chinese citizens, and representatives from the United States, the European Union, and Japan. Chao noted that Hong Kong Journalism Professor MacKinnon reported an enormous increase in searches for *fan qiang* or how to circumvent China's "Great Firewall" after news about the regulation attempts became public. Chao also noted that the Information Technology Industry Council had participated in a joint letter sent to Chinese Premier Wen Jiabao expressing interest that any measures adopted by the Chinese government "are considered in a transparent way and are consistent with global norms and encourage user choice" (Chao, 2009b). This outcome illustrates the potential impact of citizens, governments, and other organizations on preventing or "long-term postponing" governmental regulation of the Internet. Governments, businesses, and individuals find themselves in a transparent, global fishbowl.

Governments, and other groups and individuals will notice and openly express concern about how actions impact the greater good of society such as freedom of expression. Awareness about future controls wanted or desired by governments because of poor choices by individuals or groups such as those putting trash on the Internet brings responsibility closer to home for every user of Cyberspace. It is an awareness to learn the transparency that constitutes good transparency such as preparing children and adults to live responsibly in a world that will always

harbor people and groups who have evil intentions or intentions that vastly differ from individuals or governments who strive to protect individual freedom of expression.

Teaching about stratospheric transparency at an early age means teaching people to accept the consequences of their choices, to respect others' rights to make their own choices, to not infringe on others' rights to privacy and respect, to make all choices, such as how to use the Internet, in socially responsible ways. I rarely run across offensive websites or pages. When I do, I leave them immediately. Rousseau (1762) described that he took his student at an early age to bars to see people who abused alcohol, to consider and learn why he would want to learn to live responsibly and avoid certain pitfalls. Today, Rousseau might have taken his student and friend to see people coming and going from an Internet Café. Although there isn't anything wrong with the cafes, some people entering or exiting may appear to be in a similar fog as people who abused alcohol in Rousseau's lifetime. Perhaps we can consider ways to get the criminal minds turned around to realize they are littering the Internet highway and Cyberspace game rooms, and that they could instead, help make it a better place. For a humorous creation from the American Civil Liberties Union that may spur interest in molding privacy and the future of the Internet, go to http://aclu.org/pizza/images/screen.swf.

Stratospheric Wisdom Pyramid

Trying to regulate access to Cyberspace can be compared to attempts to regulate access to Space. The cost for some people to go to either "space" may be too great. In any event, when people choose to go to any "space," they need to be prepared. Anyone trying to regulate access will also pay a cost. It may be that the cost is in vain. The term "stratospheric" deals with the boundary of the atmosphere, i.e. where the mesosphere and space meet. Apparently to stay aloft ("afloat!") at the highest atmospheric altitudes, at a theoretical 100 km., the "Karman line" named after Theodore von Karman, you have to be traveling faster than the earth's rotation (See Figure 1). Some people are traveling into Cyberspace but not traveling faster than developments in spyware, spam, and other malicious technologies. They are only traveling as fast as "data and information," not as fast as knowledge development and wisdom. The decision to enter the stratosphere has to be deliberate rather than glib satisfaction of curiosity. It is about assessing needs for publishing to a world audience while simultaneously gathering data and knowledge from a world of unknown intellectuals, entrepreneurs, actors as well as criminals.

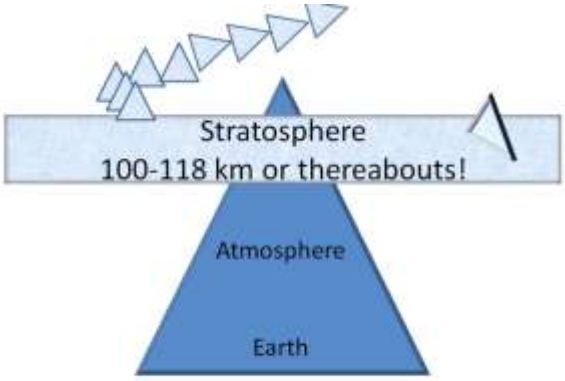

Figure 1. The highest atmospheric altitudes, at a theoretical 100 to 118 km

The "Stratospheric Wisdom Pyramid" serves to illustrate some of the issues and concerns about privacy as the Internet goes into its next and future stages (See Figure 2 presented and discussed in more detail below). The pyramid is based on the commonly-cited "wisdom pyramid" and the comparison to the Karman line (not a clear cut boundary line or "end point" but approximately where the air gets thinner). The bottom level of the pyramid has abundant data and information. It includes pictures of millions of smiling and not-smiling people, their animals, their homes, descriptions of their aspirations, artwork, unfinished and botched up web pages as well as award-winning pages, and countless other precious data and junk data – the earth data layer of the World Wide Web and the Internet. Next is the Earth Information layer where information starts to grow and blossom and vulnerability grows. Advertisers begin to build their e-mail targets and databases of information on this layer. Then there's the knowledge layer of the pyramid – in reality "organized information." As much as some want to deny it, there lies Wikipedia. On the knowledge layer, as one might expect, there are libraries, learned societies, museums, recipes, videos such as how things work or how to succeed in life, and more knowledge than one can use in a day. The final stratum—wisdom—is simply applied knowledge.

Figure 2 "Stratospheric Wisdom Pyramid" illustrating the layers of data, information, knowledge, and wisdom related to the "Karman line"

The foundation for the "wisdom model" includes data, information, and knowledge. According to Lessig, "Foundations get laid, they don't magically appear." Do we want people to be explorers and discoverers, or limit their understanding of both real and imaginary worlds, good and evil worlds? What a person does or becomes "there" whether in the real, imagined, or digital worlds, is part of their "innermost being" with the potential to ultimately influence the future and perhaps their own destiny and that of others. Like any other space, Cyberspace is a place to learn about ourselves, our existence, our destiny…It is a place that is architected by humans. For example, how many ways can we get family pictures accessible to others and how can we access others' pictures? What is the easiest, most flexible, safest and wisest platform?

Like MTV, the science fiction book, "Marooned in Realtime," does not provide interactivity or social intercourse in the sense of the Internet. Cyberspace "real time" seems more like "real life." In the sci-fi book, databases on individuals were available dating back 10,000 years. Ironically, the first paragraph of the book's preface, setting the scene, noted that "Billions of tones of ash and rock were pumped into the stratosphere" (Vince 1986). Throughout the book, people travel back and forth through time and are heavily reliant on technology. I gleaned a few choice quotations that could describe many travelers in Cyberspace:

> "As usual, the low-techs had little choice but to tag along" (Vince 1986, 11),"The species insulated itself from physical stress for so long that what few individuals survived the destruction of technology would have been totally unable to live on their own" (Vince 1986, 70), "You'd have to live like a hermit or have lots of money to go forty years and not get on a junk-mail list or have a published credit rating" (Vince 1986, 79), "And those new models are beyond our intelligence" (Vince 1986, 111), "Besides, I wanted more to build things than to protect folks. At the beginning of the twenty-third, the world was changing faster than you can imagine. I'll wager there was more technical change in the first decade of the

> twenty-third than in all the centuries to the twenty-second. Have you noticed the differences among the advanced travelers?" (Vince 1986, 146).

Lessig reported about someone who "slithered away to cyberspace, and only there did his deviancy flourish" (Lessig 2006, 19). Deviancy in virtual worlds inevitably influences behavior in the real world. Lessig described the case of a certain Jake Baker who acted completely different in his dorm room in Ann Arbor, Michigan based on "the norms of civility and decency" there that were non-existent in his cyberspace. Actor Heath Ledger, who played "The Joker" in the latest "Batman" movie and then virtually became "The Joker" in real life, killing himself as an apparent consequence of his conversion, provides another example of the potential danger of getting too absorbed in a role, and the value of keeping balance and equilibrium as we proceed into stratospheric Cyberspace.

Swisher and Mossberg (2009) noted, "…we think that the digital sector is now moving full bore into an entirely new cycle of profound change." Hauck (2008) referred to the profound changes as the "Springtime of E-learning." It is a time when individuals can focus on their own interests and "knowledge gaps" rather than having to regurgitate, cram, and compete with other students as in many "traditional" classes. It is approaching a time when we can better understand that how we control, use and interface with *the medium is the message*.

Hauck (1997) discussed transparency as it relates to being able to teach or learn without due regard to the instructional technology being used. An example of this type of transparency is the ability to become immersed in another language and culture through the Internet. "Although there are resources for immersion in another language and culture that can be purchased, including translation services, there are also resources available 'for the searching.' There are newspapers and dictionaries from around the world available for free online. For example, a search for 'Puerto Rican newspaper' resulted in 895 'hits'" (Hauck 2009a, 2). When I read the notice, "Search and preview millions of books from libraries and publishers worldwide using Google Book Search" at http://books.google.com, I could not resist looking up one of my favorite books, "Understanding media: the extensions of man" by Marshall McLuhan:

> "In a culture like ours, long accustomed to splitting and dividing all things as a means of control, it is sometimes a bit of a shock to be reminded that, in operational and practical fact, the medium is the message. This is merely to say that the personal and social consequences of any medium—that is, of any extension of ourselves – result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology" (McLuhan 1964, 7).

At its core, is this expansion of our supposed or intended audience actually an assault on an author's privacy, or a welcome expansion of the audience?

An example of an extension of oneself in Cyberspace is the Massively Multiple Online Game (MMOG) environment. Lessig noted that the typical MMOG user spends "20-30 hours per week inside the fantasy…The things people do there are highly varied…They appear (in a form they select, with qualities they choose and biographies they have written) in a virtual room and type messages to each other. Or they walk around (again, the ambiguity is not a slight one) and talk to people. My friend Rick does this as a cat—a male cat, he insists. As a male cat, Rick

parades around this space and talks to anyone who's interested. He aims to flush out the cat-loving sorts. The rest, he reports, he punishes" (Lessig 2006, 12). It may well be that introduction of one's *real self* into the Cyberspace stratosphere is so tempting yet challenging that MMOG participation may be a way of participating by avatar without allowing the invasion of one's "private" self. In reality, the *real self* (one's innermost being) and *Cyberspace self* become blurred without providing particulars such as physical location or personal identity information to other MMOG participants.

Conclusion

Lessig's book had a significant impact on my own views of the Internet. He talked about the "fallacy of 'is-ism'" when people just think the Internet "is what it is" and is part of a theory of evolution out of their control or zone of influence (Lessig 2006, 32). Along with him, I recommend the acquisition of the book or otherwise gaining honest access to it. It provides a solid foundation for understanding why it is vastly important to follow the issues and perspectives of privacy in cyberspace. Since his students and others from his wiki helped him with the content, the royalties from his book go to the nonprofit Creative Commons.

In part, this paper has been a study of "Good Citizen versus Bad Citizen," "Good versus Evil," "Criminal Mind versus Socially Responsible Mind." My travels are about to take me to Salamanca where I have heard briefly about the irony portrayed in a book called Lazarillo de Tormes by Diego Hurtado de Mendoza, AnÓnimo - 1883. Apparently, it reveals the difficulty at times of determining "Right versus Wrong." Of course, there are no simple answers. One of my typical responses to questions is, "It is complicated" because you will not argue that "all things are simple." For example, "What is the difference between a *good insect* and a *bad insect*?" Some will say they are all bad, some that they are all good. Since we really don't know, let's tolerate them. I can recommend at least four remedies for insect bites if you are tolerating them. It's like Rousseau taking his student Emile to a bar in order for Emile to observe first-hand the effect on the bar's customers. We learn from the good and the bad.

In this paper, I touched on the "innermost being" concept. Based on ten years of experience as a volunteer in prison ministry, I assert that those who truly want and choose to be socially responsible cannot fathom activities of the criminal mind although we try. The criminal mind must have similar challenges figuring out why the socially responsible act the way they do. For example, we met Terry when he was in prison. After a year of his failed attempt at re-entry into society, he was told by his parole officer one day, "That's criminal thinking!" That was an enormous awakening for Terry (he said), and it seemed to be so. The people thinking that way have learned that way of thinking to be "true" and "valid" in their realm of belief and perspective. It may be the responsibility of the "non-criminal thinkers" to teach them social responsibility and a respect for their own privacy as well as the privacy of others.

There is a delicate balance in the United States allowing freedom of expression, thought, and social change. Integrating Blacks into society in the distant past could have been seditious. For example, the Fairness Doctrine required licensed radio broadcasters to provide equitable

content, giving equal time for someone to express the other side of a controversial issue. Liberal talk shows failed. People don't want to listen to them. As a result, several representatives in Congress want to bring back the Fairness Doctrine or something similar to it.

When one enters Cyberspace, one should stay focused on the integrity of one's posts: good advice for checking e-mail, searching the web, uploading, downloading, and otherwise traveling, walking, talking, pretending, or imagining in Cyberspace. Personal responsibility and influence should be carefully considered, as should the abstract concept of desensitization. Careful focus on the integrity of posts will enhance sensitivity to everything one encounters in Cyberspace and enhance overall values, morality, and standards. In discussing the topic of Privacy Perspectives in Cyberspace, a friend asked, "Why do smart people use their intelligence for bad? They could do so much good!" Her comment was in reference to someone who broke into a school network to change his grade! Our responsibility is to let the smart, yet deviant, cybersects know they have a bigger and better purpose by leading the Internet and Society through a process of learning rather than through a process of going from ignorance to arrogance and back again. Let anger, ignorance, arrogance, and such debacles be a thing of the past.

Part of our dilemma or challenge seems to be the conflict between privacy and trust. I trusted Dell's employees in India to access my computer and my lifestyle when I was so frustrated with a problem with my cursor and mouse pad, that I was desperate to get the problem resolved. So far, while I am writing this paragraph of my reflection, the problem has not occurred. When I asked the tech support person (TSP) whether or not there had been other consumers of a Dell Inspiron 1525 with a similar problem, he said that he recalled a woman who, after 2 ½ hours on the telephone with him, came to the conclusion that her thumb was inadvertently hitting the mouse pad while she was using the keyboard. The TSP seemed surprised that I take my laptop—designed for portability—with me. He asked if I use it "as a desktop computer" or if I use it other places! He said something like, "Hmmmm, so you take it back and forth?" I said, "I take it everywhere. I use it while traveling, while in a car, while sitting on a couch…so my thumbs are not always in the same position…I have tried the staccato method I learned in piano lessons…Nothing has worked. When he tried to get me interested in purchasing insurance for about $80 that would be good through 2014, I said the warranty until 2011 was sufficient, as I would probably have so much duct tape on the mouse pad, that I would no longer have a use for the computer. Soon after talking with the TSG (technology support gentleperson who shared with me when asked that he was located in a town in the northern part of India), I received a survey from Dell via e-mail, asking if the problem was fixed. In the comment area, I noted that I had not had a chance to test it out, but I was optimistic that it was going to work. I received a telephone call the next day inquiring about the situation. Again, I had not been using the laptop for "keying in a great number of words" but I was still optimistic. Now, after this paragraph, I am more than optimistic. So, the problem seems to have been solved by the installation of an updated device driver. Perhaps it's the "device driver for people who use their laptops for the *old-fashioned laptop purpose – mobile computing*!" When I called the TSG, he said he was going to run a diagnostic. I said I had already run the automatic diagnostics and

that the report said the keyboard and mouse pad were operating properly! Another "Hmmm, you may need an updated driver." The call only took about half an hour. I hope that lady who is still blaming her thumbs reads this. I also hope that our concern with privacy doesn't completely invade our right to trustworthy and efficient, yet seemingly perplexed at times, TSGs.

What was that cleaner that we couldn't live with and couldn't live without? It was trisodium phosphate (TSP), a terrific remedy for tough stains, but apparently not acceptable to the environment. If we cry too loudly about the invasion of tech support, we will lose it. My touchpad is working for the remainder of this paper. If we perfectly execute a comprehensive Internet privacy strategy, do we face depriving ourselves of developing and maintaining robust non-verbal communication skills? That was key with my TSG and also with someone we met from a remote tribe in Nigeria whose culture was very much against eye contact. What was comprehensible in one culture was not in another. As we learn about privacy strategies, we are also learning about cultures and applications of our learning that are not necessarily evidenced in the foreseeable future. As people, businesses, and governments attempt to control the Internet to provide an "atmosphere of privacy," it is each cybernaut's responsibility to learn more and become more prepared for travel and the stratospheric use and development of Cyberspace.

References

Ross, S. (1990-2005). "Netiquette. The Core Rules of Netiquette." Retrieved July 1, 2009 from http://www.albion.com/netiquette/corerules.html

Allen, A. (2009). "Texting Teens: Bad for their Health? Experts Weigh in on Potential Problems Surrounding the Surge in Text Messages." Fox News. Retrieved July 16, 2009 from http://www.q13fox.com/news/kcpq-052609-textingteens,0,19495.story

Alexander, B. (2004). "Going Nomadic: Mobile Learning in Higher Education." EDUCAUSE Review, vol. 39, no. 5 (September/October 2004): 28-35. Retrieved July 17, 2009 from http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume39/GoingNomadicMobileLearninginHi/157921

Bodeen, C. "China defends net filtering software amid outcry." *Associated Press*, Retrieved June 11, 2009 from http://tech.yahoo.com/news/ap/20090611/ap_on_re_as/as_china_internet

Breuner, C. (2007). "Teens and Text Messaging." Video interview. Seattle Children's Hospital, Research, and Foundation. Retrieved July 16, 2009 from http://www.seattlechildrens.org/child_health_safety/resources/videos/2007/05/002218.asp

Cellular-news. (2009). "2,000+ Unknown Words Used by Teens in More Than 1.2 Million Text Messages Every Minute." Retrieved July 16, 2009 from http://www.cellular-news.com/story/37717.php

Chao, L. (2009). "China Squeezes PC Makers." *The Wall Street Journal*, Retrieved June 8, 2009 from http://online.wsj.com/article/SB124440211524192081.html#mod=testMod

Chao, L., Dean J. (2009). "Chinese Delay Plan for Censor Software." *Associated Press*, Retrieved July 1, 2009 from http://online.wsj.com/article/SB124636491863372821.html#mod=djemalertNEWS

Clarke, R. (1999). "Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations." Paper prepared to support a keynote presentation to the Sixth Annual

Conference of the Australian Association for Professional and Applied Ethics, Old Parliament House, Canberra, 2 October 1999. Retrieved May 25, 2009 from www.rogerclarke.com/II/IEthics99.html

Clarke, R. (2008a). "Terminology Relevant to 'Identity in the Information Society.'" Retrieved May 25, 2009 from http://www.rogerclarke.com/DV/IdTerm.html

Clarke, R. (2008b)."The Effectiveness of Privacy Policy Statements

A Pilot Study Against a Normative Template." Retrieved May 25, 2009 from http://www.rogerclarke.com/EC/PPSE0812.html

Fowler, G. A. (2009). "Peeved at Auto-Warranty Calls, a Web Posse Strikes Back." *The Wall Street Journal*, Retrieved May 15, 2009 from http://online.wsj.com/article/SB124234497033421649.html

Hambridge, S. (1995). RFC 1855. "Netiquette Guidelines." Retrieved July 1, 2009 from http://www.stanton.dtcc.edu/stanton/cs/rfc1855.html

Hauck, R. M. R. (1997). Media Integration in University Classrooms. (Doctoral dissertation, University of Kansas, 1996).

Hauck, R. (2008). "Good Practices for E-learning in Higher Education Courses." In G. Richards (Ed.), *Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2008* (pp. 870-875). Chesapeake, VA: AACE.

Hauck, R. (2009). "Immersion in Language and Culture through Multimedia and Web Resources." *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications*. Ed-Media 2009. Chesapeake, VA: AACE.

Hauck, R. M. (2009). "Individuality, Innovation, and Accountability for Learning in Online Multimedia/Hypermedia Applications Courses." *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications*. Ed-Media 2009. Chesapeake, VA: AACE.

Jamieson, R., L and, L., Stephens, G., & Winchester, D. (2008). "Identity Crime: The Need for an Appropriate Government Strategy." Forum on Public Policy, Oxford, England.

Kline, R. "Where are the Cyborgs in Cybernetics?" Social Studies of Science 39/3 (June 2009) 331–362, Retrieved August 27, 2009 from http://sss.sagepub.com/cgi/content/refs/39/3/331

Lessig, L. (2006). *Code 2.0*. New York, N.Y. Basic Books.

McLuhan, M., Lapham, L. (1964). *Understanding Media: The Extensions of Man*. London. The Mit Press.

O'Neill, N. (2009). "Ten Privacy Settings Every Facebook User Should Know." Retrieved April 9, 2009 from http://www.allfacebook.com/2009/02/facebook-privacy/

Patrick, A. (2009). "U.K. Government Unveils Digital Policy With Anti-Pirating Provisions." *The Wall Street Journal*, Retrieved June 16, 2009 from http://online.wsj.com/article/SB124516964471519431.html

Rousseau, J. (1762). *Emile or On Education*. Translation by Basic Books, Inc. (1979)

Schaffhauser, D. (2009). "Carnegie Mellon Researchers Find SSNs Can Be Predicted." Campus Technology. 1105 Media, Inc. Retrieved July 14, 2009 from http://campustechnology.com/Articles/2009/07/13/Carnegie-Mellon-Researchers-Find-SSNs-Can-Be-Predicted.aspx?Page=1

Shanker T. , Sanger D. (2009). "Privacy may be a victim in cyberdefense plan." *The New York Times.* Retrieved June 15, 2009 from http://www.msnbc.msn.com/id/31338666/ns/politics-the_new_york_times/

Steele, Emily. (2009). "Web Privacy Efforts Targeted. Facing Rules, Ad Firms to Give Consumers More Control." *The Wall Street Journal*, Retrieved June 25, 2009 from http://online.wsj.com/article/SB124588328571950163.html

Svantesson, D.J. B. (2009). "The times they are a-changin' (every six months)–The challenges of regulating developing technologies." Forum on Public Policy, Oxford, England.

Swisher K. & Mossberg W. (2009). "All Things Digital." *The Wall Street Journal*, Retrieved June 8, 2009 from http://online.wsj.com/article/SB10001424052970203431004574197842436069268.html

The AVweb Editorial Staff (2009). "Edge Of Space Defined." *AVwebFlash Complete Issue: Volume 15, Number 15a.* Aviation Publishing Group. Retrieved April 13, 2009 from http://www.avweb.com/eletter/archives/avflash/1350-full.html#200126

Vince, V. (1986). *Marooned in Realtime*. Tom Doherty Associates, LLC, New York.

Worthen, Ben. (2009). "U.S. China in Talks Over Web Filters." *The Wall Street Journal*, Retrieved June 22, 2009 from http://online.wsj.com/article/SB124569653149438053.html

Published by the Forum on Public Policy