Know Techn Pol
DOI 10.1007/s12130-010-9119-3

SPECIAL ISSUE

Responsibility of and Trust in ISPs

Raphael Cohen-Almagor

Received: 31 March 2010 / Accepted: 28 May 2010

Abstract This discussion is about the neglected concepts of trust and social responsibility on the Internet. I will discuss and explain the concepts and their implications to people and society. I then address the issue of moral and social responsibilities of ISPs and web-hosting companies. I argue that ISPs and web-hosting companies should aspire to take responsibility for content and that they should respect and abide by their own terms of conduct.

Keywords Trust · Responsibility · ISPs · Web-hosting companies · Rowdiness · VampireFreaks.com · Child pornography

1 Introduction

The Internet's design and *raison d'être* are complete freedom. The Internet provides cheap, virtually untraceable, instantaneous, anonymous, and uncensored distribution that can be easily downloaded and posted in multiple places. The transnational nature of the World-Wide-Web, its vast content, the fact that it has no central management or coordination, and that the routing computers do not retain copies of the packets they handle provide ample opportunities for people to exploit the Net's massive potential to enhance partisan interests, some of which are harmful and antisocial, thus undermining people's sense of trust in the Net. The Internet is not the problem. The problem is the relatively small number of people who abuse its massive potential to harm others.

In the focus of my discussion are the neglected concepts of trust and social responsibility, adopting them to the Internet realm. I will discuss and explain the

I thank Janet Spikes for her excellent research assistance. All websites were accessed on January 18–21, 2010.

R. Cohen-Almagor (✉)
Department of Politics and International Studies, The University of Hull, Hull, UK
e-mail: R.Cohen-Almagor@hull.ac.uk

concepts and their implications. To foster trust, there is a need to cultivate social responsibility on the Internet. The Concept of Social Responsibility should guide Net users,[1] Net readers, Internet Service Providers (ISPs), states, and the international community at large. Here, I focus attention on moral and social responsibilities of ISPs and web-host companies. Should they take effort to monitor their sites for such information or are they relieved of any responsibility? This is arguably the most intriguing and complex issue of Net responsibility. I argue that ISPs and web-hosting companies should aspire to take responsibility for content and that they should respect and abide by the laws of the countries in which they operate.

2 Trust

The Oxford Dictionary defines trust as "confidence, strong belief, in the goodness, strength, reliability of something or somebody."[2] Trust is a social phenomenon that requires acquaintance and some knowledge on part of the person who trusts and the person or thing that is trusted. It is about transparency and expectations from the trusted partner. The more transparent are the relationships, the more expectation a person possesses regarding the level of trust she can have in the relationships. When transparency is dubious, it is difficult to gain and maintain trust.

Although trust may require a meaningful relationship, it need not require good will or warm sentiments. I may trust the bank to keep my money safely, but I do not imagine for a moment that the bank is warmly disposed to me. It is clear that we have shared interests and that the relationships will continue only as long as we share the interests. Similarly, when I seek physician's advice, I may trust the physician's professional expertise and integrity even though the cold professional appears to be indifferent to me as a person (Kohn 2008).

There is considerable uncertainty about how trust in the offline world transfers into cyberspace and about the trustworthiness of the components of the cyberspace system. On the one hand, trust is closely connected with a greater level of certainty or confidence in the reliability and security of the Internet. Thus, it is likely that trust will be enhanced as a person learns more about the technology. As the technology becomes familiar, it becomes less intimidating. People who know more about the Internet may become more trusting of the medium. On the other hand, information can create uncertainty and contribute to an increased perception of risk.[3]

Helen Nissenbaum notes that there are specific features of the online world that bear on the formation and sustenance of trust, which conceal many of the aspects of character and personality, nature of relationship, and setting that normally function as triggers of trust or as reasons for deciding to trust. First, the medium allows agents to cloak or obscure identity. This reduces the number of mutual cues upon which trust may develop. It may further obscure the nature of mutual relations and suggest a diminished sense of responsibility to one another. Secondly, online, we are separated from others in time and space. Personal characteristics like gender, age,

[1] See Cohen-Almagor (2011a, 2011b)

[2] "Trust," *Oxford Advanced Learner's Dictionary of Current English.*

[3] Dutton and Shepherd (2005). See also (Dutton and Shepherd 2006).

race, socioeconomic status, or occupation can be hidden from us. Thus, we lack cues that may give evidence of similarity, familiarity, or shared value systems, cues which mediate in the construction of trust. One may be a 67-year-old man presenting himself as a 14-year-old girl. We all can assume the looks and characteristics of our role models when we try to attract the attention of those who we wish to attract. Thirdly, the settings of online environment are frequently inscrutable in ways that affect readiness or inclination to trust. Clear social and professional role definitions are often lacking; duties and responsibilities are less defined and understood. As a result, we cannot rely on traditional mechanisms for cultivating trust (Nissenbaum 2001: 113–114). In addition, as we often do not see other net users in person, we miss bodily clues that often help us to consolidate opinion about others: facial expressions, body movement, gestures, and our general impression of people. Tools like Skype may help in eliminating this difficulty.

These are obvious obstacles for developing personal relationships online. To secure some level of trust takes time and human investment. This is the optimistic view. Pessimists like De Laat argue that establishing trustworthiness is next to impossible and that any gesture of trust tends to be seen as an "opportunistic and ludicrous move which will only solicit ridicule instead of esteem."[4] The Internet is such an environment that we often find it difficult to know who is who and, as the famous cartoon "On the Internet nobody knows you're a dog,"[5] shape and form are in flux. Neil Barrett puts rhetorically: "ask yourself quite how much you trust the internet, a system built on invisible, unknown components, performing unknown functions in an unknown manner...still happy to shop, bank and flirt online? (Barrett 2005)."

One study suggests that the social connections that people make on the Internet do not promote trust—indeed, there is some evidence that chat rooms may cause mistrust in people (Uslaner 2004). However, people exhibit on the Internet thick trust, thin trust, or no trust, depending on their knowledge, common sense, and experience. When people wish to obtain information about any phenomena on the universe, they often go first to the World-Wide-Web. For instance, I exhibit thick trust when I refer to *The Stanford Encyclopedia of Philosophy* as a major resource and refer my students to the Stanford site.[6] This trust was initially based on the reputation of Stanford University, substantiated by reading entries of this encyclopedia. In turn, thin trust is a qualified, circumscribed, cautious trust. People usually exhibit this kind of trust in financial affairs, typically when dealing with strangers. Companies and services try to convince us that it is possible to do business with them, or through them, fostering a sense of trust. They do this by building a certain reputation, upholding certain norms, and providing signals that may gain our assurance. For instance, ebay developed system of rated sellers with compliments that are designed to develop trust: the seller consistently receives highest buyers' ratings, ships items quickly, has earned a track record of excellent service, etc.[7]

[4] De Laat (2005: 170). See also (Pettit 2004).

[5] This problem has spawned a number of identity verification services. These services provide a verification-chain framework to both parties, while protecting sensitive information. See http://www.readwriteweb.com/archives/nobody_knows_youre_a_dog.php

[6] http://plato.stanford.edu/

[7] Ebay.com

Lastly, most of us do not trust strangers who notify us that out of the blue, we won a two million prize in a lottery in which we never took part.

Given the number of people posting information on the Net, it is reassuring that many of us exhibit thick trust when we obtain information from the Net, perceiving it as fairly reliable. A recent poll asked what is the most reliable source of information shows that the Internet came first with 37%, while television (17%), newspapers (16%), and radio (13%) lagging behind (Zogby 2009). While much of Net information is reliable and most users trust it, those who abuse the Net undermine users' confidence. Problems and perceived dangers may be seen as a failure either of the technical systems or of the system designers and users to take steps in order to prevent abuse or to reduce the vulnerabilities in the system.[8] However, technical measures alone would not suffice to foster trust in the cyberspace. Transparency and trust will not garner significant economic benefits for a corporation unless they are backed by a genuine concern for stakeholder interests (Elia 2009: 150). There is a growing urgency to foster a recognized known sense of social responsibility on the Net. This kind of transparency is likely to maintain trust over time. With the advancement of technology at large and specifically the Internet, responsibility for gaining and maintaining trust in the Net increasingly falls on those who operate the Net, namely on Internet Service Providers and web-hosting companies.

3 Social Responsibility

Responsibility is commonly associated with accountability and answerability. The Concept of Social Responsibility (CSR)[9] assumes the following: *first*, that autonomous agents have the understanding of the options before them, have access to evidence required for making judgments about the benefits and hazards of each option, and able to weigh the relative value of the consequences of their choice. *CSR further assumes* that people are not islands to themselves. We live within a community and have some responsibilities to it. The responsibilities are positive and negative. That is, we have a responsibility to better the society in which we live and a responsibility to refrain from acting in a way that knowingly might harm our community. The responsibility is ethical in nature. *CSR's third assumption* is that we are rewarded by the social framework in which we live, we care about society, would like to maintain it, and to contribute to it. The contribution is proactive. We take active steps to do good and to avoid harm (Kaliski 2001; Marshall 1994; Christians and Nordenstreng 2004; Bunton 1998; Rivers et al. 1980). We care for one another, communicate with respect, and do not stand idly by while seeing that others might be in danger. Both the private and the public sector are morally accountable. As Novak, Trevino, and Nelson argued, adopting social responsibility norms is the right

[8] Mansell and Collins (2005). Internet expert Brian Marcus argues that the Internet is based on trust. Most of its users act within the law. Therefore, in the USA, there are far more protections on free expression than restrictions on speech. We should not punish most users because of the small numbers who exploit the Internet to violate the law, and we should not allow a small number of abusers to dictate the rules of the game. Interview with Marcus, Washington DC (June 5, 2008).

[9] CSR as applied in this article, not to be confused with Corporate Social Responsibility.

way to behave (Novak 1996; Trevino and Nelson 1999). Later I will also argue that social responsibility is vital notwithstanding whether or not it contributes to an increased sense of trust in the Internet.

CSR carries a special meaning in the context of information and communication technologies (ICT). ICTs make humanity increasingly accountable, morally speaking, for the way the world is, will, and should be (Floridi and Sanders 2001). A member of these professions is trained to practice a core skill, requiring autonomous judgment as well as expertise. ICT professionals have an inviolable duty to serve the interest of their clients and often some wider social and public responsibility should be expected. Their work is governed by a set of appropriate ethics as well as being based on knowledge and skill. Certain standards and qualifications are expected to be maintained, following an accepted code of practice that observes wider responsibilities to clients and society.[10]

4 Responsibility of ISPs and Web Hosting Services

The issue of responsibility of ISPs and host companies is intriguing and complex. I will elaborate and explore this issue in detail from the ethical and social perspectives. In depth legal analysis has been provided by others.[11] An ISP is a company or other organization that provides gateway to the Internet, usually for a fee, enabling users to establish contact with the public network. Many ISPs also provide e-mail service, storage capacity, proprietary chat rooms, and information regarding news, weather, banking, or travel. Some offer games to their subscribers. An Internet hosting service is a service that runs various Internet servers. The host manages the communications protocols and houses the pages and the related software required to create a website on the Internet. The host machine often uses the Unix, Windows, Linux, or Macintosh operating systems, which have the TCP/IP protocols built in (Gralla 2007).

It is one thing to argue that *a moderator of a specific site* should be held liable for content on the sites s/he manages. This would seem a fair demand for small sites and arguably also for large sites. It is another thing to argue that *ISPs* should be held liable for content. Those who object the idea of holding ISPs responsible for content on their servers argue that the Internet is like a telephone carrier. Both provide communication service. You cannot hold a phone carrier, say Verizon, for using the

[10] Compare to the responsibilities of the press; see (McQuail 2003).

[11] Web site hosting can give rise to liability for trademark infringement and copyright infringement but generally will not give rise to liability for defamation. The leading legal American precedents on Internet offensive speech are *Cubby, Inc. v. CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont, Inc. v. Prodigy Services Co*., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995); *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998); *Zeran v. AOL,* 129 F.3d 327 (4th Cir. 1997), cert. denied, U.S., 118 S. Ct. 2341 (1998); *Doe v. America Online* 25 Media Law Rep. (BNA) 2112; 1997 WL 374223 (Fla. Circ. Ct. June 26, 1997); Case No. 97-2587 (Fourth District Court of Appeal, Fla., October 14, 1998). At present, American courts tend to hold that ISPs are not liable for content posted on their servers, this under Section 230(1) of the Communications Decency Act (1996) which reads: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. 230. For analysis, see (Siderits 1996; Boehm 1998; Kane 1999; Goldstein 2000; Friedman and Buono 2000; Voelzke 2003).

phone line to plan a crime. Verizon provides a service, which can be abused. Same—so it can be argued—is true for Internet providers. On both the phone and the Internet, we find the basic components of communication: a sender, a message, a channel, and a receiver. Generally speaking, both also provide opportunity for feedback.

All this is true. But the Internet is different from the phone in some critical technological, organizational, and geographical ways that make the comparison unconvincing. Let me uncover some of the major differences. Firstly, the Internet is based on a technology that uses connectionless protocols for host to host resource sharing called packet switching. Packet switching represents a significantly different communications model. It is based on the ability to place content in digital form, which means that content can be coded into binary numbers or bits (1 or 0), which is how computers store information.[12] In packet switching, the content of communication is divided into small, well-defined groups of coded data, each with an identifying numerical address. Anything that can be digitized can be sent as a packet. It is possible to send an unlimited number of packets over the same circuit with different addresses. Diffused routers, rather than main switches, became the key to delivering the packets to the intended destination.[13]

Secondly, the volume, scope, and variety of data that the sender is able to transmit over the Internet are much larger than the phone. Over the phone, two or more people can speak. On the Internet, people can speak, chat, send email, buy merchandise, gamble, share and transfer files, and post various forms of data. The Internet presents information in textual, audible, graphical, and video formats, evoking the appearance and function of print mass media, radio, and television combined. The Internet is a global system of interconnected computer networks that interchange data. It is a "network of networks" that consists of millions of private and public, academic, business, military, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies.

Thirdly, the lack of centralized control means that it is difficult to prevent any agency determined to abuse the Internet for its own purposes. There is no phone line to cut.

Fourthly, unlike the telephone service, the Internet is borderless. The technology encompasses continents.

Lastly, the flexible, multipurpose nature of the Internet, with its potential to operate as a set of interpersonal, group, or mass media channels, is a unique communication system. The Internet provides many more avenues in comparison

[12] Floridi explains that the binary system of data encoding has noteworthy advantages. First, bits can equally well be represented semantically (meaning True/False), logico-mathematically (standing for 1/0) and physically (transistor=On/Off; switch=Open/Closed; electric circuit=High/Low voltage; disk or tape=Magnetized/Unmagnetized; CD=presence/absence of pits, etc.) and hence provide the common ground where semantics, mathematical logic, and the physics and engineering of circuits and information theory can converge. Second, this means that it is possible to construct machines that can recognize bits physically, behave logically on the basis of such recognition, and, therefore, manipulate data in ways which we find meaningful. Third, since digital data normally have only two states, such *discrete variation* means that a computer will hardly ever get confused about what needs to be processed, unlike an analog machine, which can often perform unsatisfactorily or imprecisely. See (Floridi 2010).

[13] Mathiason (2009). See also (Cohen-Almagor 2007).

with any other form of communication to preserve anonymity and privacy with little or no cost involved.

Better analogies than the Internet and a phone carrier are those between the Internet and a large first- and second-hand bookstore, or between the Internet and a large library. An owner of a bookstore cannot be held responsible for the content of each and every book in her store. She does not read and inspect all the books. Similarly, it can be argued, an Internet provider should not be held accountable for content on its server. But if a bookstore owner is informed that a specific book contains child pornography, some other illegal material, or material that violates copyright, and she does not take the book out of the shelves, then the owner may be held legally responsible for violation of the law. And she is also morally responsible. Similarly, it can be argued, is the case on the Internet.

Bookstore owners do have discretion about the books they offer for buyers. Many would like to maintain quiet and tranquil atmosphere in the store. The books, accordingly, will be for the general readership. Other book owners might opt for more a rowdy atmosphere. They will entertain books of socially problematic material. The likely result would be that the general readership would refrain from attending those bookstores. Those stores would become niche stores, for particular readers.

In both kinds of store, store owners would like to keep the business going. They will listen to alerts about the illegality of certain books. Same, it can be argued, with Internet providers and host companies: provide a notice first, allowing the provider to make a decision for the consequences to which she might be held liable. If the provider/host does not act upon the warning, then it will have to face the consequences. Indeed, on copyrights issues, ISPs are expected to assume responsibility. They should also assume moral and social responsibility when violent antisocial activities are taking place on their servers. Most ISPs and web-hosting companies would not like their servers to transform into forums in which people concoct criminal activities.

There are, of course, exceptions. In June 2009, the US Federal Trade Commission ordered to shut down Pricewert, described as a "rouge" or "black hat" ISP that acted as a hosting center for many hi-tech criminals. The FTC alleged that Pricewert was paid to host "child pornography, botnet command and control servers,[14] spyware, viruses, Trojans, phisihing-related sites, illegal online pharmacies, investment and other web-based scams (Messmer 2009)."[15] Pricewert evoked suspicion as its

[14] A botnet (also known as a Zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie—in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. See http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1030284,00.html

[15] *Federal Trade Commission v Pricewert LLC* (United States District Court Northern District of California San Jose Division) (June 2 2009); "FTC Shuts Down Notorious Rogue Internet Service Provider, 3FN Service Specializes in Hosting Spam-Spewing Botnets, Phishing Web sites, Child Pornography, and Other Illegal, Malicious Web Content," *Federal Trade Commission* (June 4, 2009), http://www.ftc.gov/opa/2009/06/3fn.shtm

domain has changed name servers three times over 5 years, and it was hosted on nine IP addresses over 5 years.[16]

5 ISPs and Web-Hosting Rules and Regulations

Most ISPs have rules and regulations by which they abide. Some ISPs offer guidelines regarding prohibited Internet content and usage, terms for service cancelation, and even user responsibilities. Obviously, ISPs and web-hosting companies have the right and the duty to report potentially criminal activities to the appropriate law enforcement agency. In addition, ISPs may prohibit posting legally seditious or offensive content. They have the right in their sole discretion to prescreen, refuse, or move any content that is available via their Service. ISPs and web-hosting companies reserve the right to terminate service if in their discretion a client has violated the terms and conditions of the service. The terms and conditions specify what they perceive to be antisocial activity, not covered by law (child pornography, terrorism). What this realm includes may vary from one ISP to another. Some ISPs abhor having racist organizations on board. Others are tolerant and even supportive of this activity.

America On Line Terms say:

> Online conduct should be guided by common sense and basic etiquette. You will be considered in violation of the Terms of Service if you (or others using your account) do any of the following: […] Transmit or facilitate distribution of content that is harmful, abusive, racially or ethnically offensive, vulgar, sexually explicit, or in a reasonable person's view, objectionable. Community standards may vary, but there is no place on the service where hate speech is tolerated.[17]

However, if such content is not removed by the ISP, neither it nor its partners assume any liability. Yahoo! has terms of service that prohibit to "upload, post, email or otherwise transmit any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable."[18] Yet, another American ISP, DataPipe, declares that:

> DataPipe will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 concerning child pornography. Customers are ultimately responsible for the actions of their clients over the DataPipe network, and will be liable for illegal material posted by their clients. According to the Child Protection Act, child pornography includes photographs, films, video or any other type of visual presentation that shows a person who is or is depicted as being under the age of 18 years and is engaged in or is depicted as engaged in explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ

[16] http://whois.domaintools.com/pricewert.com

[17] http://legal.web.aol.com/aol/aolpol/comguide.html.

[18] http://uk.docs.yahoo.com/info/terms.html.

> or the anal region of a person under the age of 18 years any written material or visual representation that advocates or counsels sexual activity with a person under the age of 18 years.[19]

DataPipe has a Social Responsibility section in which it names their favorite charities and their commitment to preserve the environment.[20] Several ISP associations have developed different codes concerning, among other things, the protection of minors.[21]

Now, the question begs whether ISPs and host companies should be proactive, i.e. not only cooperate upon receipt of information from various sources but in order to promote trust among their subscribers, scrutinize their sphere for problematic, antisocial, and potentially harmful material. They are obviously reluctant for very practical reason—the costs involved in employing professional staff who will scrutinize the information. Cynically, they might argue, morality is one thing, but here, we are talking about money.

In the UK, ISPs have rejected a call by children's charities to implement the government's approved blocklist for images of child sexual abuse, because the list does not stop anyone who wants to access such material. Warning was raised that 700,000 homes could access websites hosting images of abuse because small ISPs do not filter their networks. The charities aimed to put pressure on the government to force them to implement the Internet Watch Foundation's blocklist, pointing out that in 2006 ministers said all providers should do so by the end of 2007. But small ISPs have resisted filtering their networks for several years on economic and principle grounds. For them, it would mean spending a lot of money on something that they do not deem absolutely necessary. It should be noted that pedophiles with minimal technical knowledge are able to circumvent the blocklist. The policy, therefore, has no impact on their ability to access websites distributing child abuse images. Rather, the blocklist protects average web users with no interest in such material from accidental exposure (Williams 2009).

6 Rowdiness

The Red Light District in Amsterdam is one of the most notoriously known pornographic centers in the world. In it, there are dozens of sex shops offering merchandise for all human preferences, tastes, and perversions. I went to a few of them and asked for child pornography. The shop keepers all said that they did not hold such material. They have thousands of magazines and videos, how did they know, with such unshaken confidence, that no such material had found its way into the store? When I stubbornly asked: Are you sure? The response was a suspicious stare and angry conviction that no child pornography existed in their stores. They had taken measures to ascertain that such illegal material will not be available to the general public.

[19] http://www.datapipe.com/Acceptable_Use_Policy.aspx.

[20] http://www.datapipe.com/Social_Responsibility.aspx

[21] http://www.biac.org/members/iccp/mtg/2008-06-seoul-min/DSTI-ICCP-IE(2005)3-FINAL.pdf; see also (Price and Verhulst 2000).

Likewise, there are rowdy websites entertained by rowdy ISPs. Would it be an exaggerated expectation of them to scrutinize their sites so as to avoid certain illegal material? At present, the widespread answer in the USA is positive. The issue of trust seems secondary as the thought is that people who wish to visit rowdy sites do this. The concern that others might stumble accidently to those sites deems insignificant. The further question is whether this objection is principled or practical. Is it because of constitutional First Amendment right, or because of consideration of cost and traffic volumes? It is possible to find solutions to practical issues. It is far difficult to convince ardent principled opposition to change their view.

I have said that the Internet may also liken to a large library. In many research libraries, books known to be problematic for their content are kept in designated area, under the open eye of an experienced librarian. If someone wishes to read a book from that section, she has to sign for it and read it in the same room where the book is kept. This way, the library is balancing between the right to free expression and flow of information, and societal interests in maintaining peace and order. People who have library cards can still have access to the information, but they might be asked questions about their purpose for reading the book, and a record is kept that they read the book in question. Similar arrangement can be made on the Net. Some problematic material will have restricted access, and people will have to sign up for reading it, providing some details about their identity and why they wish to read this particular piece of information. Thus, certain forms of speech that are presently shielded under the First Amendment should be in restricted Net areas to which people should register. If you wish to read a manual as to how to kill your wife without leaving a trace, you will need to leave verifiable details.[22] Similarly, people interested in recipes for rape drugs, recipes for bombs, and manuals as how to kill people like *Hit Man: A Technical Manual for Independent Contractors* (*Rice v. Paladin* 1997). I fully realize that the principle of Net neutrality would oppose registering problematic sites. However, the issue is not the neutrality of the Net but whether we should be neutral regarding this kind of content. Morally speaking, CSR speaking, we cannot be neutral regarding such alarming speech (Cohen-Almagor 2011a, 2011b). At the very least, this speech requires some precaution. This precaution would certainly promote the level of trust in the technology.

7 VampireFreaks.com

Some websites have gained notoriety for serving as hubs and meeting place for criminals. One of them is VampireFreaks.com, founded in 1999 by a Brooklyn resident, Jethro Berelson, who names himself “Jet.” The site claims to have 600,000–700,000 members and millions of entrances (Pona 2006; Mandel 2006). On this site, Jeremy Allan Steinke had met his minor girlfriend. Both were charged with the triple murder of Marc Richardson, 42, his wife Debra, 48, and their son Jacob, 8 (Robertson 2006). On this site, Eric Fischer, a 23-year-old man, was arrested after showing up at a cemetery expecting to have sex with a 13-year-old girl he met on VampireFreaks. It was the second alleged incident in which Fischer used the site to

[22] http://powerballplace.blogspot.com/2005/03/how-to-kill-your-wife-and-get-away.html

lure young girls. Fischer had been arrested on rape charges after meeting a 16-year-old girl he had met on the website (Agrell 2006a, b). On this site, three young men were sentenced for a deliberate fire that destroyed the 105-year-old Minnedosa United Church, in Minnedosa, Manitoba. One had posted his profile on VampireFreaks (MacLeod 2006). On this site, a troubled young man, Kimveer Gill, vented his hostilities before he embarked on a shooting spree in Dowson College, Montreal that resulted in one dead student and some 20 others injured (Cohen-Almagor and Haleva-Amir 2008).

VampireFreaks site rules do not allow people under the age of 13 to use the site. It prohibits posting of nude photos and "excessively gory/offensive pictures."[23] It does not allow the exploitation of anyone in a sexual or violent manner; uploading pornographic or obscene material to the site; engaging in, promoting, or condoning any type of harmful or illegal activity; spamming and sending sexual messages to minors.[24] Jet said that in the past, he had alerted the police a few times of users whose profiles were suspicious (Agrell and Cherry 2006). But despite the abovementioned incidents, Jet does not take any measures to monitor his site. He is aware of what is going on the site, he has capacity for decision, and yet he chooses to allow complete freedom. Jet is not acting from ignorance. He fails to take moral and social responsibility because of whatever reason: overconfidence, unshaken belief in the First Amendment, laziness, dogmatism, or simply because he wishes to save money. Trust is not an issue. His assumption is that VampireFreaks subscribers are oblivious to the dangers. They do not care. Neither does Jet. But social responsibility is important notwithstanding whether or not it contributes to an increased sense of trust in the medium.

VampireFreaks.com is a busy site with hundreds of thousands of postings. Some effort is needed for moderators of such large sites to monitor the heavy traffic. There are two practical questions: one related to cost; the other related to ability. As for costs, there is a need to hire services of web experts to devise a research algorithm for identifying what is regarded as problematic material. The costs can be shared between the website's members. This consideration alone is insufficient to relieve ISPs from their moral and social responsibilities. As for ability, among laypersons, it is a contested issue whether it is technologically possible to monitor websites, especially very large and voluminous websites with heavy traffic. The issue is far less contested among experts. A web expert who worked for Yahoo! in monitoring Yahoo! groups told me that a small number of experts who specialize in social networking could devise batches of programs to look for illegal material and remove it. This expert did this for Yahoo! in its struggle against child pornography.[25] Similarly, Marc Rotenberg, President of the Electronic Privacy Information Center, said that the capability to monitor the Internet is greater than what most people assume. It is a question of will, not of ability.[26] National security organizations have developed mechanisms to scrutinize large parts of the Internet susceptible to criminal

[23] http://vampirefreaks.com/termsofservice.php. See also (Agrell and Cherry 2006)

[24] http://vampirefreaks.com/termsofservice.php

[25] Discussion with a research specialist, George Washington University, Washington DC (June 12, 2008). See (Silberman 2002).

[26] Interview with Marc Rotenberg, President of the Electronic Privacy Information Center, Washington DC (May 2, 2008).

activity. The University of Florida has created a software tool called ICARUS that monitors traffic over its network, identifies traffic that appears to be characteristic of peer-to-peer file sharing, and then suspends network service to the computer generating the traffic for 30 min. Users may regain network access only if they complete a 10-min interactive presentation on copyright law (Evans 2004: 498). Companies like Check Point Enterprise[27] and Symantec Gateway Security[28] provide traffic management features with highly developed security-management tools. Allot Communications provides facilities to manage traffic and produces a fully integrated, carrier-class platform capable of identifying the traffic flows of individual subscribers.[29] Packeteer tracks link and provides statistics per application—including peak and average utilization rates (down to one minute), bytes, availability, utilization, top talkers and listeners, network efficiency, and frames. It monitors use and performance through proactive alarming and exception reporting or through comprehensive central reporting tools.[30]

Thus, it is possible to monitor traffic on large websites. It is a question of will and of priorities in allocating resources for monitoring. At present, VampireFreaks is not exceptional in its reluctance to monitor sites and relieve itself of responsibility. Most ISPs and hosting companies shy away from assuming such responsibility as it is the easiest and profitable path to pursue. But this attitude may change. It is already changing in the sphere of child pornography.

8 Child Pornography

In 2008, the USA enacted the Protect Our Children Act, which requires providers of electronic communications services and remote computing services (“service providers”) to submit reports of online child pornography to the National Center for Missing and Exploited Children (“NCMEC”).[31] On June 10, 2008, three of the American major Internet service providers have agreed to block customer access to newsgroups and websites that offer child pornography. Under the agreement with Sprint Nextel, Verizon Communications, and Time Warner Cable, which are expected to hold nationwide, the companies agreed to shut off access to newsgroups believed to traffic in child pornography and to remove from their servers any websites offering such images. The targeted sites will be based on a list compiled by the National Center for Missing and Exploited Children (Whoriskey 2008). The list comprises only the “most egregious” types of child pornography, especially those involving young children. Internet providers are required by law (42 USC 13032)[32] to report apparent child pornography. Moreover, child pornography is bad for their business. They do not wish to serve child pornographers or to have the reputation of

[27] http://www.checkpoint.com/products/enterprise/

[28] http://www.symantec.com/avcenter/security/Content/Product/Product_SGS.html; http://www.symantec.com/business/products/allproducts.jsp

[29] http://www.allot.com/index.php?option=com_content&task=view&id=2&Itemid=4

[30] http://www.packeteer.com/solutions/visibility.cfm

[31] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s1738enr.txt.pdf

[32] Reporting of child pornography by electronic communication service providers, 42 USC 13032, http://vlex.com/vid/19244635

helping spread child pornography. One day earlier, French Interior Minister Michele Alliot-Marie announced that she plans to use the help of Internet Service Providers to block websites, which disseminate child pornography. From September 2008 onwards, Internet users are able to flag sites that carry child pornography, incitement to terrorism and racial hatred, or attempted fraud. This real-time information would help France to draw up a blacklist of sites that disseminated child pornography and other illegal material, which it would transmit to Internet service providers that have agreed to block such sites.[33] It should be noted that AFA—the French ISP's association (Association de Fournisseurs d'Acces et de Services Internet), established in 1997, has been collaborating with the French law authorities since 1998, on a regular basis.[34]

More recently, a new service in the aid of fighting child pornography over the web was launched. This free service enables operators and ISPs to deny their users access to websites that contain material depicting children's sexual abuse (TeliaSonera 2008). And in February 2009, Facebook removed more than 5,500 accounts of convicted sex offenders. This came after MySpace announcement that it removed more than 90,000 accounts of sex offenders.[35]

Both MySpace and Facebook, as well as many other online social communities, have drastically changed their policies to deal with trust and CSR concerns. MySpace is contributing to about 150 police investigations a month and has initiated education programs and reporting criteria for its users. In 2006, Facebook has changed its format to protect sensitive information about its users (Agrell 2006a). Following Megan Meier's tragic suicide (Cohen-Almagor 2011b), MySpace issued a statement saying it "does not tolerate cyberbullying" and was cooperating fully with the US attorney (Deutsch 2008). This attitude manifests social and moral responsibility to be encouraged and become commonplace among all Internet companies.

In January 2008, MySpace and American Attorneys General in the Multi-State Working Group on Social Networking representing 49 states and the District of Columbia unveiled a Joint Statement on Key Principles of Social Networking Sites Safety designed for industry-wide adoption. This common set of Principles relates to online safety tools, technology, education, and law-enforcement cooperation. The Joint Statement recognizes that an ongoing industry effort is required to keep up with the latest technological developments and to find additional ways to protect teens. The Attorneys General called on other social networking sites and Internet providers with community features to adopt the Principles and bring their sites up to par with MySpace in terms of safety. On behalf of MySpace, Chief Security Officer Hemanshu Nigam, said, "We thank the Attorneys General for a thoughtful and constructive conversation on Internet safety. This is an industry-wide challenge and we must all work together to create a safer Internet. The Principles we have adopted set forth what the industry needs to strive towards to provide a safer online

[33] Reuters, "France to block child pornography websites" (June 10, 2008).

[34] See an English communiqué—http://www.afa-france.com/p_20040113.anglais.html

[35] http://www.philstar.com/Article.aspx?articleId=441984&publicationSubCategoryId=200; http://www.computerweekly.com/Articles/2009/02/20/234945/facebook-removes-5500-sex-offenders.htm; News agencies, "Facebook blocked some 5,500 sex criminals," *Haaretz* (February 20, 2009) (Hebrew).

experience for teens and we look forward to sharing our ongoing safety innovations with other companies."[36] The Principles of Social Networking fall into four categories:

- Site Design and Functionality. The Principles incorporate various safety initiatives. Examples of safety features MySpace has in place include reviewing every image and video uploaded to the site, reviewing the content of Groups, making the profiles of 14 and 15-year-old users automatically private and protecting them from being contacted by adults that they do not already know in the physical world, and deleting registered sex offenders from MySpace. MySpace is said to strive to implement further improvements, including defaulting 16- and 17-year-old users' profiles to private and strengthening the technology that enforces the site's minimum age of 14.
- Education and Tools for Parents, Educators, and Children. The Principles acknowledge that MySpace has already been devoting meaningful resources to Internet safety education including a new online safety public service announcement targeted at parents and free parental software that is under development. MySpace is said to explore the establishment of a children's email registry that will empower parents to prevent their children from having access to MySpace or any other social networking site. In addition, under the Principles MySpace increases its communications with consumers who report a complaint about inappropriate content or activity on the site.
- Law Enforcement Cooperation. The Attorneys General view MySpace's cooperation with law enforcement, which includes a 24-h hotline, to be a model for the industry. The parties continue to work together to enhance the ability of law enforcement officials to investigate and prosecute Internet crimes.
- Online Safety Task Force. As part of the Principles, MySpace organized, with the support of the Attorneys General, an industry-wide Internet Safety Technical Task Force to develop online safety tools, including a review of identity authentication tools. While existing age verification and identity products are not an effective safety tool for social networking sites, the Task Force explored all new technologies that can help make users safe and secure including age verification. The Task Force included Internet businesses, identity authentication experts, nonprofit organizations, academics, and technology companies. The Task Force submitted its Final Report to the Attorneys General in December 2008 (Berkman Center for Internet and Society 2008).

9 Conclusion

The Internet is a vast ocean of knowledge, data, ideologies, and propaganda. It is ubiquitous, interactive, fast, and decentralized. The ease of access to the Internet, its low cost and speed, its chaotic structure (or lack of structure), the anonymity

[36] http://socialmediaportal.com/PressReleases/2008/01/-MySpace-and-Attorneys-General-Announce-Joint-Effo.aspx

which individuals and groups may enjoy, and the international character of the world-wide-web furnish all kinds of individuals and organizations an easy and effective arena for their partisan interests. The Internet contains some of the best products of humanity, and some of the worst ones. It serves the positive and negative elements in society.

The Internet's short history provides us a crash course in understanding why a balanced approach is needed to address and resolve conflicting freedoms. Here, I would like to invoke Aristotle's Rule of the Golden Mean that for every polarity, there is a mean which when practiced are good benchmarks for a life of moderation. The more we see the golden mean in each polarity, the better we find the true benchmarks of a life of wellness.[37] People have the freedom to express themselves, within reason. Two underpinning principles, in the heart of liberal democracy, are respect for others and not harming others. We should strive to uphold them also on the Internet.

In this essay, I stressed the concepts of trust and social responsibility. As more public information, commerce, and social life involve online interactions, the Internet has become an indispensible part of our lives. Behaving in a trustworthy way and trusting others as a way to express respect for others as moral beings constitute ethical behavior (Myskja 2008: 219). So does acting responsibly. Luciano Floridi envisages a steady increase in agents' responsibilities (Floridi 2007). I hope he is correct in his observation. We can reasonably expect people to know the difference between good and evil and then to act accordingly. ISPs should continue to develop and embrace initiatives designed to protect users, especially children. These include technological tools as well as educational campaigns. They should carefully balance reasonable expectations of customer privacy with the need to ensure a safe and secure online environment. Industry should give due weight to societal considerations that may be essential to promote trust of people in it and to prevent abuse. There is a need to assure a certain security level on the Internet, like in any other industry. A senior security officer suggested that Internet providers should have integrity teams, instructing providers to take off inappropriate content.[38] Technical solutions can be engineered if all involved parties recognize the problem and cooperate to overcome it. With them, awareness of and adherence to basic CSR with its vital ethical implications will assure a certain security level on the Internet, like in any other industry.

I suggest publishing overviews and reports on a regular basis; exchanging information to enhance the effectiveness of ISPs-State cooperation; lobbying for international awareness about the harms and abuse of technology; helping support groups and institutions that want to set up tip-lines, and advancing our knowledge of social networking and the psychology of people who use the Internet for various purposes. Clearly, there is a lot to learn about Net human behavior and what can be done to increase trust and social responsibility of all parties concerned.

[37] Aristotle (2008). See also Adkins (1984); Kraut (2002).

[38] Interview with a senior security officer, Washington DC (March 25, 2008).

References

Adkins, A. W. H. (1984). The connection between Aristotle's *Ethics* and *Politics*. *Political Theory, 12*, 29–49.

Agrell, S. (2006a). Troubled kids 'gravitating' to vampire site: several violent crimes in Canada tied to network. *National Post* (September 15), *A6*.

Agrell, S. (2006b). 'Vampire' meets 'teen' in graveyard. *UPI* (April 28).

Agrell, S., & Cherry, P. (2006). Blogs reveal a deteriorating mind, police say. *National Post* (September 16), *A9*.

Aristotle (2008). *Works* (MobileReference, 2008), at http://www.mobilereference.com/BS_Philosophy/index.htm#ari.

Barrett, N. (2005). Criminal IT: Should you trust the internet? *Silicon.com* (January 27, 2005), http://www.silicon.com/technology/security/2005/01/27/criminal-it-should-you-trust-the-internet-39127375/.

Berkman Center for Internet and Society. (2008). Final Report of the Internet Safety Technical Task Force, *Enhancing Child Safety and Online Technologies*. Boston: Berkman Center for Internet and Society, at http://cyber.law.harvard.edu/research/isttf#.

Boehm, S. B. (1998). Note, a brave new world of free speech: should interactive computer service providers be held liable for the material they disseminate? *Richmond Journal of Law & Technology*, *5*, 7, Winter, at http://jolt.richmond.edu/v5i2/boehm.html.

Bunton, K. (1998). Social responsibility in covering community: a narrative case study. *Journal of Mass Media Ethics, 13*(4), 232–246.

Christians, C., & Nordenstreng, K. (2004). Social responsibility worldwide. *Journal of Mass Media Ethics, 19*(1), 3–28.

Cohen-Almagor, R. (2007). *The scope of tolerance*. London: Routledge.

Cohen-Almagor, R. (2011a). Content net neutrality—a critic (forthcoming).

Cohen-Almagor, R. (2011b). Responsibility of net users. In M. Fackler & R. S. Fortner (Eds.), *Global communication and media ethics*. Oxford: Wiley-Blackwell.

Cohen-Almagor, R., & Haleva-Amir, S. (2008). Bloody wednesday in Dawson College—the story of Kimveer Gill, or why should we monitor certain websites to prevent murder. *Studies in Ethics*, *Law and Technology*, *2*(3), Article 1.

De Laat, P. B. (2005). Trusting virtual trust. *Ethics and Information Technology, 7*, 167–180.

Deutsch, L. (2008). Woman indicted in Missouri MySpace suicide case. *Associated Press Online*.

Dutton, W. H., & Shepherd, A. (2005). Confidence and risk on the internet. In R. Mansell & B. S. Collins (Eds.), *Trust and crime in information societies*. Cheltenham: Edward Elgar.

Dutton, W. H., & Shepherd, A. (2006). Trust in the internet as an experience technology. *Information, Communication & Society, 9*, 433–451.

Elia, J. (2009). Transparency rights, technology and trust. *Ethics and Information Technology, 11*(2), 145–153.

Evans, E. (2004). From the cluetrain to the panopticon: ISP activity characterization and control of internet communications. *Michigan Telecommunications and Technology Law Review, 10*, 445–499.

Federal Trade Commission (2009). FTC Shuts Down Notorious Rogue Internet Service Provider: 3FN service specializes in hosting spam-spewing botnets, phishing web sites, child pornography, and other illegal, malicious web content. *Federal Trade Commission*, http://www.ftc.gov/opa/2009/06/3fn.shtm.

Floridi, L. (2007). A look into the future impact of ICT on our lives. *The Information Society, 23*(1), 59–64.

Floridi, L. (2010). *Information—a very short introduction*. Oxford: Oxford University.

Floridi, L., & Sanders, J. W. (2001). Artificial evil and the foundation of computer ethics. *Ethics and Information Technology, 3*(1), 55–66.

Friedman, J. A., & Buono, F. M. (2000). Limiting tort liability for online third-party content under section 230 of the communications act. *Federal Communication Law Journal.*

Goldstein, M. P. (2000). Service provider liability for acts committed by users: what you don't know can hurt you. *Marshall Journal Computer and Infomation Law, 18*, 591. Spring.

Gralla, P. (2007). *How the internet works* (8th ed.). Indianapolis: Que.

Kaliski, B. S. (Ed.). (2001). *Encyclopedia of business and finance*. New York: Macmillan.

Kane, M. J. (1999). Internet service provider liability: Blumenthal v. Drudge. *Berkeley Technology Law Journal, 14*, 483.

Kohn, M. (2008). *Self-interest and the common good*. New York: Oxford University.

Kraut, R. (2002). *Aristotle political philosophy*. New York: Oxford University.

MacLeod, I. (2006). Vampire culture gets another black mark after shooting: website linked to Medicine Hat slayings. *The Calgary Herald* (September 15), *A3*.

Mandel, M. (2006). Out for blood. *The Toronto Sun* (September 24), *5*.

Mansell, R., & Collins, B. S. (Eds.) (2005). *Trust and crime in information societies*. Cheltenham: Edward Elgar.

Marshall, M. L. (1994). Ensuring social responsibility. *Thrust for Educational Leadership*, *23*(4).

Mathiason, J. (2009). *Internet governance* (p. 7). Abingdon: Routledge.

McQuail, D. (2003). *Media accountability and freedom of publication* (p. 191). New York: Oxford University.

Messmer, E. (2009). ISP pricewert protests shutdown. *PCWorld.com* (June 6).

Myskja, B. K. (2008). The categorical imperative and the ethics of trust. *Ethics and Information Technology, 10*(4), 213–220.

News agencies (2009). Facebook blocked some 5,500 sex criminals. *Haaretz*, (Hebrew) (February 20).

Nissenbaum, H. (2001). Securing trust online: wisdom or oxymoron. *Boston University Law Review, 81* (3), 107–131.

Novak, M. (1996). *Business as a calling: Work and the examined life*. New York: Free Press.

Pettit, P. (2004). Trust, reliance and the internet. *Analyse & Kritik, 26*, 108–121.

Pona, N. (2006). Net violence unchecked. *Toronto Sun* (September 15), *4*.

Price, M. E., & Verhulst, S. G. (2000). The concept of self-regulation and the internet. In J. Waltermann & M. Machill (Eds.), *Protecting our children on the internet: Towards a new culture of responsibility.* Gütersloh: Bertelsmann Foundation.

Reporting of child pornography by electronic communication service providers, 42 USC 13032, http://vlex.com/vid/19244635.

Reuters (2008). *France to block child pornography websites* (June 10).

Rivers, W. L., Schramm, W., & Christian, C. G. (1980). *Responsibility in mass communication*. New York: Harper and Row.

Robertson, L. (2006). Web links to shooting. *CTV Television* (September 14).

Siderits, M. C. (1996). Comment: defamation in cyberspace: reconciling Cubby, Inc. v. Compuserve, Inc. and Stratton Oakmont v. Prodigy Services Co. *Marquette Law Review, 79*, 1065–1081.

Silberman, S. (2002). The United States of America v. Adam Vaughn. *Wired*, http://www.wired.com/wired/archive/10.10/kidporn.html.

TeliaSonera (2008). *Launches service that prevents distribution of material depicting child sexual abuse.* A press release (September 4).

Trevino, L. K., & Nelson, K. A. (1999). *Managing business ethics: Straight talk about how to do it right.* New York: Wiley.

Uslaner, E. M. (2004). Trust, civic engagement, and the internet. *Political Communication, 21*(2), 223–242.

Voelzke, J. (2003). Don't shoot: i'm just the web site host! *The Computer & Internet Lawyer, 20*(5), 4.

Whoriskey, P. (2008). Internet providers agree to block child pornography. *Washington Post* (June 11), *A01*.

Williams, C. (2009). "Small ISPs reject call to filter out child abuse sites," *The Register* (February 25, 2009), at http://www.theregister.co.uk/2009/02/25/iwf_small_isps/.

Zogby, J. (2009). Why do people trust the internet more? *Forbes.com* (June 18).

Court Judgments

Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998)

Cubby, Inc. v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991).

Doe v. America Online 25 Media Law Rep. (BNA) 2112; 1997 WL 374223 (Fla. Circ. Ct. June 26, 1997), Case No. 97-2587 (Fourth District Court of Appeal, Fla., October 14, 1998)

Federal Trade Commission v Pricewert LLC (United States District Court Northern District of California San Jose Division) (June 2, 2009)

Rice v. Paladin Enterprises Inc., No. 96-2412, 128 F.3d 233 (November 10, 1997).

Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)

Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997), cert. denied, U.S., 118 S. Ct. 2341 (1998).