Teaching IS to the Information Society using an "Informing Science" Perspective

Ramesh Subramanian and Bruce White
Quinnipiac University, Hamden, CT, USA

Ramesh.Subramanian@quinnipiac.edu; Bruce.White@quinnipiac.edu

Abstract

Information systems permeate every aspect of society, requiring IS professionals to acquire a wide perspective on how information systems shape society and *vice versa*. This notion has ramifications for IS curricula in universities everywhere. We believe that collegiate IS curricula would enhance currency and relevance by broadening their coverage to include more *Information Society* concepts. We take the view that "information systems" are not restricted to organizational systems alone, but are really trans-disciplinary, socio-technical systems that are enmeshed with the cultural, legal, and political environment in which they exist. Therefore all students of IS will benefit and become better informed by learning about the current and emerging issues that closely couple IT and society. We review the concepts and issues of today's *Information Society* with case-studies and examples separated into various topic areas, so as to provide direction for incorporating these concepts into information systems academic curricula.

Keywords: Information Systems Education, Information Systems Curriculum, MIS discipline, Informing Science, Information Society, Intellectual Property, Piracy, Open Source Software, Antitrust, Access to Knowledge, Public Policy

Introduction

In a 2003 article, Nicholas Carr argued that, as the availability of information technology (IT) continued to increase and its costs continued to decrease, IT's ability to provide competitive advantage to organizations would diminish and eventually cease to matter (Carr, 2003). Many counter-arguments notwithstanding, it is clear that certain aspects of IT in organizations will indeed change in focus due to commoditization, on the one hand, and disruptive developments such as peer-to-peer computing, cloud and social computing on the other. These developments have already dramatically changed the ways by which IT affects individuals, organizations, and societies, and *vice versa.*

What do these developments mean to the information systems (IS) field? The IS field is no longer just about the effective use of information systems in organizations. Instead, all IS professionals require a deeper level of understanding and proficiency on how to be effective in this complex, networked, information-rich global cyber society facilitated by IT - that some have referred to as the *Information Society.* (We use the term "IT" interchangeably with "ICT" or Information and Communications Technologies. Today's IT cannot be separated from the communications tech-

nologies that enable even the most basic IT implementation).

We examine the concept of the *Information Society* in greater detail in the next section, but argue that the notion of the Information Society – one which permeates all aspects of society – has, in turn, important ramifications for IS education. To be successful in today's *Information Society* IS graduates must not only know how to design, develop, and maintain information systems; they must also be keenly aware of the societal realities wrought and perpetuated by information technologies. They must be proficient not only with the "mechanics" of their profession, but also on all new developments and related trans-disciplinary aspects. It is critical for IS educators and students alike to recognize the "trans-disciplinary" nature of information systems.

We therefore submit that IS education, regardless of geographic location, should take on more of an "informing science" approach as elucidated by Cohen (2009) – that the purpose of IS education is not to focus narrowly on managing information systems within organizations, or on specific topics such as systems analysis or data management, but instead to take a larger, socio-technical perspective that seeks to inform managers, employees, and individuals about the *Information Society* in which they are all participants. There is another critical reason for taking this approach to IS education: it has been noted for several years now that the MIS academic discipline is failing in its role as informer to its external clients. This is noted by Gill and Battacherjee (2007), who comprehensively analyzed the impact of MIS academic publication outlets among practitioners. They noted that "observations strongly suggest that the MIS disciplinary informing system supports very limited pathways, at best, from its sender side (researchers) to its practitioner clients" (Gill & Bhattacherjee, 2007. p. 25). The IS graduate, i.e., the *output* of the MIS discipline, thus becomes an important component – the informer, as well as enabler of organizations and societies. This adds even more imperative to our central idea about making the IS curriculum more rooted in the Informing Science philosophy – i.e., teaching the *Information Society*.

What is the Information Society?

First, we need to gain a deeper understanding of what the term *Information Society* means. There is no single established definition for the phrase *Information Society*. It has often been used interchangeably with Nico Stehr's "knowledge society" (Stehr, 1999), Manuel Castells' and Jan van Dijk's "network society" (Castells, 1996; van Dijk, 1999), and Alain Touraine's "post-industrial society" (Touraine, 1988). For our purposes, we use the "Declaration of Principles" of the World Summit on the Information Society (WSIS) (International Telecommunications Union, 2003) as a guide to understand what is meant by the term, as well as how to operationalize it. (WSIS Summits and Forums are jointly sponsored by the International Telecommunications Union (ITU) and the United Nations General Assembly. The first WSIS was held in Geneva in 2003, and the second was held in Tunis in 2005. Annual WISI Forums have been held at the ITU headquarters in Geneva). The WSIS document sets several key principles for creating an "Information Society for all." Of particular relevance to our purpose here is Section B6, which lists specific "enablers of the Information Society," namely:

- *The need for rule of law, as well as supportive, transparent pro-competitive, technologically neutral, predictable policy and regulatory framework*
- *The need to foster ICT-supported productivity gains and innovation gains across all economic sectors (i.e. ICT for sustainable development)*
- *The need for IP protection, as well as the need for wide dissemination and sharing of knowledge*
- *The need for global standards, and the need for development of open, inter-operable and non-discriminatory standards*
- *The need for effective management of radio frequency spectrum*
- *The need to promote and facilitate a stable and secure Internet*

It should be noted that the WSIS document's list is not limited to any specific country or region. Any country that aims to be a successful participant in the *Information Society* should ensure that these enablers are in place, albeit in varying degrees of maturity.

From a curricular point of view, a promising interpretation is offered by Jack Balkin, Founder-Director of Yale University's Information Society Project (Yale ISP), who has designed and taught graduate courses on the *Information Society* in a law school setting since 2009. Balkin's syllabi (Balkin, 2010) offers a perspective that is grounded on the American legal environment and the American Constitution. It encompasses the following subject areas:

- *Democracy, Culture, and Free Speech*
- *Regulations and Legal Issues*
- *Identity and Privacy Issues*
- *Control, including Censorship, Copyright Protection, and Innovation Control Policy*
- *Software piracy*
- *Cybersecurity*
- *Search Engine Policies*
- *Wikipedia and the Politics of Information Production*
- *Democracy and the Public Sphere*

By combining the above sets of points and removing overlaps, we have arrived at a core set of topics which we believe would be ideal additions to contemporary IS curricula, while offering a solid coverage of the *Information Society*. These are:

1. ***Intellectual Property and Innovation*** *(Patents, Copyrights, International Agreements, Piracy and Fair Use)*
2. ***Freedom of Expression*** *(Internet Control, Censorship, and Ethical Issues)*
3. ***Information Privacy***
4. ***Open Source Software and Open Standards***
5. ***Telecommunications Policy*** *(Net Neutrality and Spectrum Allocation)*
6. ***Information Systems for Development***

Various model curricula have been suggested for IS education. Of particular interest are the undergraduate model IS curricula – the AIS/AITP/ACM 2002 model (Gorgone et al., 2003) and the most recent AIS/ACM 2010 model (Topi et al., 2010). These provide a list of IS core courses and electives and justification for their inclusion to the curricula (please see course sequence structures illustrated in Figures 3 and 4 in the Appendix). Upon analysis, the courses listed, while comprehensive, do not provide substantial link between information systems and the larger environment in which they exist, i.e., the *Information Society*. In our opinion, this severely "underprepares" IS students who are unable to go beyond perceiving information systems as a mere commoditized function, which could easily be shipped elsewhere.

While we realize that the core set of topics listed above are perhaps covered in varying degrees in various IS courses, we feel that there is a need to formalize, consolidate, and standardize these concepts of the *Information Society* in *all* IS curricula. We hope that what we discuss here will eventually become part of the IS core. Each of the above topics has sufficient materials for a 3-credit graduate course, with enough room for students to undertake more in-depth capstone projects.

In the rest of the paper we delve deeper into the list of *Information Society* topics provided above by looking at scenarios, cases, and examples. We discuss each of the issues along with IT impli-

cations and significant questions. Following that, we provide suggestions on how these issues and concepts could be incorporated within the existing IS curricula.

NOTE: *Many of the case-studies and examples below pertain to the United States and other industrialized countries. This is due to the fact that much of the developments in IT have originated in these countries, and, as a result, many of the issues pertaining to the 'Information Society' have garnered early attention in these countries. However, the rapid spread and expansion of the 'Information Society' make these issues as relevant to emerging economies as they are to developed economies. Thus, we believe that the topics listed will enhance* ***all*** *IS curricula regardless of the geographic location, albeit with appropriate localization. Another point to note is that the above list of 'Information Society' topics is comprehensive and, thus, is meant to provide a guideline. Individual IS curricula can use subsets of the same towards achieving the objectives we propose.*

Topic 1: Intellectual Property & Innovation (Patents, Copyrights, International Agreements, Piracy and Fair Use)

The ubiquity and proliferation of data collection, data analysis, data storage, and dissemination systems in the present society naturally lead to their use in every aspect of the creation of intellectual property (IP) – whether these be movies, music, genome sequences, works of art, pharmaceutical formulae, automobile design, or supply-chain techniques. Large databases also store and track customer and environmental data, which then are mined further to generate new IP. IP is an inherent component of the *Information Society.*

Introduction to IP

What is Intellectual property (IP)? According to the World Intellectual Property Organization (WIPO) IP refers to creations of the mind. Much of the following discussion is adapted from the World Intellectual Property Organization (WIPO, n.d.). These include inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. IP is divided into two categories:

1. Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source.
2. Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs.

Patents

IP laws are meant to reward innovators and spur new innovations. New innovations and developments in information technologies have led to a tremendous upsurge in IT-related patents. According to WIPO, 156,000 patent applications were filed in the year 2007 (Schlein, 2008). The WIPO Patent Report also states that a majority of the patents applications are related to information technology and telecommunications. The large numbers have led to numerous disputes over patent violations all over the world. Most recently, the patent dispute between Apple and Samsung has grown into a full-fledged and expensive legal war pits that Apple against Google – two technology giants – since Apple contents that Google's Android (which is used by a majority of smart phone and tablet manufacturers including Samsung) violates some of Apple's patents. Ap-

ple has also pursued legal battles with Motorola and HTC in this on-going war. This is a very high stakes war that delves deep into information technology and promises to last a long time (Barrett, 2012). It must be noted that as early as 1988 Apple pursued a legal battle with Microsoft, claiming that the Windows operating system copied significant features of Apple's *Lisa* and *Macintosh* computer interface. Apple lost that battle in 1994.

Copyrights

Large scale digitization of documents, movies, and images has also resulted in a tremendous upsurge in disputes pertaining to copyright violations and piracy issues. A major issue regarding purported copyright violations is the use or misuse of the "fair use doctrine." This doctrine originated in the United States but is generally recognized by courts in other common law jurisdictions. It seeks to balance the rights of authors and creators to reap benefits from their works of creation to the public's rights to create newer, derivative works based on the original creation (Pike, 2008). Yet, due to a misunderstanding of the fair use doctrine, by both sides, numerous lawsuits ensue.

Copyrights were formally legalized in 1886, at the Berne Convention. In 1996 the member countries of WIPO adopted the WIPO Copyright Treaty. Partly in response to the WIPO treaty, the U.S. Congress passed the Digital Millennium Copyright Act in 1998. The DMCA's Section 1201 has become very controversial. It contains two main provisions: 1201(a) and 1201(b). Section 1201(a) (1) "prohibits the act of circumventing a technological measure used by copyright owners to control access to their works ('access controls')", and sections 1201(a) (2) and 1201(b) "outlaw the manufacture, sale, distribution, or trafficking of tools and technologies that make circumvention possible. These provisions ban both technologies that defeat access controls, and also technologies that defeat use restrictions imposed by copyright owners, such as copy controls" (Electronic Frontier Foundation [EFF], 2008).

In the U.S., violations of Section 1201 of the DMCA have spurred numerous lawsuits from copyright owners or their representatives (mostly large media companies). Over the ten years that the DMCA has been in existence, critics of the DMCA , such as the Electronic Frontier Foundation (EFF) have contended that the DMCA is an ill-conceived Act which poses a threat to several public policies, such as (adapted from EFF, 2008):

- Free expression and scientific research
- Fair use
- Competition and innovation
- Privacy

Over the years, there have been numerous cases and decisions on copyright issues by the courts, which have often used their judgment on a case-by-case basis to decide on allegations of copyright violations (through the invocation of the "fair use" doctrine). However, with the passing of the DMCA, the courts have become very constrained, which leads to severe restrictions and constraints in the societal use of information systems and digitized artifacts. The extent to which the DMCA can restrict fair use, competition, innovation, and privacy can be seen by studying the case-laws discussed in EFF's (http://www.eff.org) and Stanford University's Center for Internet and Society (http://cyberlaw.stanford.edu/) web sites.

Brad Templeton has discussed restrictions pertaining to the fair use of copyrighted materials. According to Templeton and the EFF, acts such as posting e-mail, writing fan fiction, or even using "ripping" software by the owner of a CD/DVD to copy the media into another system owned by him/her is technically a violation, according to the DMCA (EFF, n.d.; Templeton, 2008).

We present below some interesting recent court cases that relate to the above discussion on free expression and fair use.

Fair Use, Free Expression, and Innovation

Rowling v. RDR Books (from Center for Internet and Society [CIS], n.d.**)**

The Harry Potter Lexicon (http://www.hp-lexicon.org/) began as a website on which contributors collected information about people, places, and things that inhabited the Harry Potter universe – as described in J.K. Rowling's books, the movies based on those books, and other associated products. It grew into what is widely regarded as the most complete and authoritative guide to the world of Harry Potter, and attracts upwards of 25 million visitors per year. In 2004, it won a fan site award from Ms. Rowling herself. In light of the website's popularity, the Lexicon's editor decided to publish it in book form, and RDR Books agreed to do so. Upon learning of this, Ms. Rowling and Warner Brothers filed suit against RDR, alleging claims for copyright and trademark infringement and seeking to enjoin publication of the Lexicon in printed form. On September 2008, Judge Patterson of the United States District Court Southern District of New York ruled in favor of Rowling (Wall Street Journal, 2008), and publication of the book was effectively blocked.

Oxford University Press, Cambridge University Press & Sage Publications v. Georgia State University (from Stiverson, 2008**)**

On April 15, 2008, three publishers, two of them non-profits, filed suit against the President, the Provost, the Provost for Information Systems and Technology, and the Dean of Libraries of Georgia State University (GSU), alleging copyright infringement. The complaint, which was filed in the U.S. District Court for the Northern District of Georgia, requests injunctive and declaratory relief and attorneys' fees, but not damages.

The complaint alleges that GSU has been engaged in "systematic, widespread, and unauthorized copying and distribution of a vast amount of copyrighted works . . . through a variety of online systems and outlets utilized and hosted by the University for the digital distribution of course reading material." Although the material is now in digital form, it is unclear how much was taken from print sources. The means of distribution include an electronic course reserve system, a Blackboard course management system, departmental web pages, and hyperlinked online course syllabi. The complaint further alleges that GSU made the works available not only to its own students, but to the public at large "until recently." The course reserve system lists more than 6,700 works for more than 600 courses, and the publishers allege that the defendants' practices "vastly exceed" the amount and type of copying that might be justified as fair use in an educational setting. The publishers state that they have complained to GSU officials, but to no avail; the University has refused to discuss the publishers' concerns and has continued to provide the materials. This case is still awaiting judgment at the time of writing this.

Piracy

P2P file sharing technology and the Pirate Bay trial

File sharing has proliferated since 1999, when Shawn Fanning, a student at Northeastern University, created Napster, an extremely popular file sharing platform service for sharing music files. The Recording Industry Association of America (RIAA), fearing loss of potential revenues, filed a lawsuit against Napster, citing illegal music downloads that was perpetuated using the Napster system. Napster's lawyers claimed that the platform merely provided a means to share files and that Napster could not be held responsible for illegal uses of the platform. Judge Marilyn Patel did not agree and issued an injunction to Napster to stop its file sharing service, which succeeded in killing the product (Borland & Barnes, 2000). However, since then the anti-copyright move-

ment has gained ground, and a plethora of file sharing software products and sites have emerged with regularity. Unlike Napster, these sites use increasingly sophisticated technologies and architecture and use numerous redundant servers across the globe, which makes them difficult to be shut down. However, organizations such as the RIAA, Motion Picture Association of America (MPAA), National Music Publishers' Association (NMPA), and several media companies in the U.S. have vigorously used the provisions of the DMCA to mount lawsuits to try and shut down the distributors of new generation P2P file sharing software.

The movie and music-makers continued to file lawsuits against makers and distributors of file sharing software, such as Grokster and Morpheus, and, in 2005, won a major victory when the U.S. Supreme Court decided that companies producing and distributing file sharing software were indeed to be blamed for what their users do with the software (Harrison, 2006). However, any hope for completely eradicating piracy has diminished with the advent of yet another new technology provided by The Pirate Bay (TPB). TPB uses a sophisticated architecture to index and track Bit Torrent files. Bit Torrent is a peer-to-peer file sharing protocol in which a file is split up into smaller parts and each part is stored in different servers across the globe. When a Bit Torrent file is downloaded, the individual pieces are located and downloaded separately and finally combined to recreate the original file. The Pirate Bay website simply acts as an index to the Bit Torrent files and does not actually contain any copyrighted materials. The complete technology is described in TPB's web site (Pirate Bay, n.d.).

The case of Pirate Bay is especially interesting and requires further discussion. The site was started in 2003 in Sweden, where copyright laws are more lax than in the U.S. Sweden also has a strong anti-copyright movement, and the Pirate Bay site was originally a part of Piratbyrån, or Pirate Bureau, an NGO. The Pirate Bay web site became an independent operation in 2004. The creators of Pirate Bay openly acknowledge that it is a piracy site and have openly rejected "cease and desist" letters from media companies and their representatives in the U.S. and parts of the E.U. (Sarno, 2007). On May 31 2006, the Pirate Bay's web servers, located in Stockholm, were raided by the Swedish police and the servers were confiscated. But despite that, the site became operational in just three days. Pirate Bay claims to have over five million active users (Sarno, 2007). According to Pirate Bay's head software designer Peter Sunde, the technology that runs sites like Pirate Bay will continue to advance and keep a step ahead of the regulatory agencies. He, as well as the founders of the site, believes that the current copyright system is outmoded, and needs to be revamped (Sarno, 2007).

The 2006 raid on Pirate Bay eventually resulted in a lawsuit launched against Pirate Bay by the International Federation of Phonographic Industry (IFPI) in February 2009 (Parrack, 2009). Pirate Bay lost the trial, and the founders were sentenced to one year in prison and about US$ 3 million in fines. But it is interesting to note that the Pirate Bay web site was not part of the trial or sentencing – only the founders. The site continues to operate from servers based in various countries of the world (Hartley, 2009).

International Agreements: TRIPS and ACTA

Large-scale digitization, which includes production, storage, and rapid dissemination of all types of knowledge, is a key feature of globalization. It makes reproduction and transmission of data extremely easy. But this development has not been welcomed by some industry groups in developed countries. Digitization and transmission of data has enabled large-scale piracy of digitized, copyrighted information such as movies and music. The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have long spearheaded legal avenues to combat piracy around the world. Such industry groups have also used international trade-related agreements as weapons to protect their intellectual property. The *TRIPS* (Trade-Related aspects of Intellectual Property Rights) agreement is administered by the World

Trade Organization (WTO), and is Annex 1C of the Marrakesh Agreement establishing the WTO, signed in Marrakesh, Morocco on 15 April 1994. The TRIPs Agreement sets out minimum levels of standards concerning intellectual property in the form of copyrights, trademarks, patents industrial designs, geographical indicators, integrated circuits, and trade secrets (World Trade Organization [WTO], n.d.). The U.S. played a major role in framing the TRIPS agreement and winning (sometimes after applying pressure) the support of developing countries.

However, many developing countries, globalization enthusiasts, and global trade activists see the TRIPS agreement as just yet another way by which developed countries seek to control world trade and seek to protect their own interests and lobbies. It is also important to note that there are often differences in the way IP is viewed across nations and cultures. Thus many developing countries see the TRIPS agreement as the imposition of the cultural norms and standards of developed countries over developing countries. Initially there was resistance to TRIPS from the developing countries, but developed countries, led by the U.S., promised new investments and technology transfers. Developing countries were told that stronger IP protection would lead to create investments and more technology transfers, but there has been no real study of this (Machemedze, 2003).

Currently the debate for and against TRIPS has not been resolved. Battles rage between the supporters and detractors. Regardless of which side is correct, serious students of IT should be aware of TRIPS, its application in the IT and digital world, its plusses and minuses.

ACTA

In 2007, the U.S., E.U., and a number of other members of WTO started working on a new international agreement to tackle global counterfeiting of intellectual property (IP). The countries involved in the negotiations other than the U.S. and EU are Australia, Canada, Japan, Korea, Mexico, Morocco, New Zealand, Singapore, and Switzerland. IP is considered to be one of the key competitive assets of developed countries, and the idea of new agreement was to develop a mechanism to enforce IP rights strictly across the globe. The overall objective was to effectively combat international trade in counterfeit and pirated goods. But as noted by the Office of the U.S. Trade Representative, the scope of ACTA is broad, including counterfeit goods, generic medicines, and copyright infringement on the Internet (United States Trade Representative, 2009).

Announcement of the ACTA immediately aroused the ire and suspicion of trade and globalization activists, several developing countries, and those in favor of transparent negotiations. That is because ACTA negotiations were held in secret, and much of what was learned about ACTA features were those that were leaked to media. In the U.S., opposition to ACTA comes from academics, practitioners, and public interest organization and stems from the secrecy, lack of Congressional oversight, and lack of public participation. Since the negotiations started, initial discussion documents and some leaked information have emerged. These have been scrutinized and severely criticized by many public interest groups, organizations, and governments who argue that the ACTA poses a threat to freedom and fundamental human rights. For instance, the Free Software Foundation, as well as some academics, believes that the ACTA would remove liability protections to ISPs whose customers indulge in illegal IP violations (such as illegally downloading music). The ISPs would be required to provide information on customers who are suspected of such illegal activities. Individuals would be subject to a “three strikes” law that would require ISPs to punitively disconnect a customer for varying period from the Internet after the third violation. The agreement would also require ISPs to stop hosting free software that can access copyrighted material. This would, potentially affect many sites that offer free software (such as SourceForge) as well as the development of free software projects. Distribution of free software through peer-to-peer computing will also be negatively affected (Free Software Foundation, 2010b; Shaw, 2008).

At the present, ACTA is in its final negotiated stages, but the opposition to it, especially the process used for the negotiations, remains strong. Many people accuse the involved countries of "policy laundering," whereby a policy becomes a legal entity without much open discussion.

Topic 2: Freedom of Expression (Internet Censorship and Ethical Issues)

Internet Censorship

Even as new technologies are being used innovatively to express dissent and project local protests globally, censorship of such activities by repressive governments is also increasing. A notable example of such government-led censorship is the "Green Dam" project in China. On June 8, 2009, the Wall Street Journal reported that China mandated all personal computers sold in the country from June 1 to have censorship software preloaded. The software would prevent access to certain web sites. This would give the Chinese government unprecedented control over what Internet users to see in China. The government justified the move, saying that it was designed to protect young people from the harmful content in the Internet (Chao, 2009).

Many governments exert some level of censorship of the Internet. The governments purport to do so for reasons of national security. A recent example is the tussle between Blackberry, a mobile phone manufactured by Canadian company Research in Motion (RIM), and countries like Saudi Arabia, the UAE, and India. The Indian government recently demanded that RIM allow it to access encrypted messages sent through Blackberry. The Indian government's demand is based on national security. Even the Open Net Initiative (ONI) does not list India in the "countries that censor" list. The Indian government's justification is that the encryption technologies embedded in Blackberry systems enable terrorists to use such systems to exchange message without fear of interception by Indian security agencies (Taylor & Karam, 2010). However, the other side of the picture, espoused by RIM, is that this violates the privacy of users of Blackberry. The level of censorship is tracked nowadays by the "Open Net Initiative" (ONI). The ONI is a collaborative partnership of the Citizen Lab at the Munk Center for International Studies, University of Toronto, Canada, the Berkman Center for Internet and Society, Harvard University, MA, and the SecDev Group in Ottawa. Its aim is to "investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion (OpenNet Initiative, n.d.)."

The ONI maintains a database of almost fifty countries around the world and gathers and prepares reports on these countries and the specific presence (or absence) of Internet censorship and surveillance practiced in these countries. The Citizen Lab and the ONI also conduct field studies and participate in privacy advocacy activities in various countries. The ONI also develops and maintains interactive maps of places where popular social media sites such as Facebook, Twitter, and YouTube are filtered. Another initiative of the ONI is *Opennet.Asia.* Its aim is to "engage academic, policy, and civil society stakeholders in each of the countries of the regions concerned by surveillance and censorship to build institutional capacity and networked resources to conduct research and public policy advocacy around those issues" (CitizenLab, n.d.).

Technologies of Dissent

The global reach of the 'Net and the mushrooming of social networking software is enabling individuals and groups to communicate with each other more than ever and faster than ever. Applications such as blogs, YouTube, Facebook, Twitter, and Flickr enable individuals to become "citizen reporters" and allow various types of political dissenters to transmit news and actual happenings of protests, human rights marchers, hunger strikes, riots, and other political events rapidly across the globe to supporters, news media, and human rights organizations. The nature of the

software allows features such as anonymity, transience, and rapid transmission and publication through broadcast channel. This allows the dissenters to work around various censorship processes imposed on such transmission by the governments of nations from where such dissent originates. The importance of technology-enabled dissent was brought into focus at a recent "Access to Knowledge" workshop at the Yale Information Society Project (Yale Law School), which scheduled a session on the technologies of dissent. The panel pursued the following question among many others: "What is the nature of the technical architecture that enables these new types of democratic expression and protest? In what ways can the same technologies be used to violate human rights? Is there a human right to any particular form of technology, or rights *vis-à-vis* technology?" (Gardener, 2010).

Facebook, Google, and Privacy Ethics

While an individual's right to privacy, and privacy laws have already been discussed in an earlier section, we bring forth some new and recent issues here again as it relates to ethical obligations of corporations. A recent news item that has made waves is Facebook's (FB's) announcement at the April FB developer conference that Facebook was "building a Web where the default is social." To achieve that, FB has created technologies that include FB features on other sites, which then send information back to FB. In addition, as explained by Richard Esguerra (2010) of the EFF, FB considers "public information" as that information about a subscriber/member that it can share with its business partners without seeking further permission. This public information could be "*name, profile picture, current city, gender, networks, complete list of your friends, and your complete list of connections (formerly the list of pages that you were a "fan" of, but now including profile information like your hometown, education, work, activities, likes and interests, and, in some cases, your likes and recommendations from non-Facebook pages around the web)*" (Esguerra, 2010). FB does provide the subscriber with the option to "opt out" of information that can be considered public, but the procedure for this is likely to confuse him/her.

This led to a flurry of protests from users as well as privacy activists who have questioned the ethics and motivations of FB. To add to this situation, on July 28, 2010, it was reported that profiles of 100 million FB users were leaked to a Bit Torrent (peer-to-peer file downloading software) server, from where the profiles were downloaded by thousands of interested parties, including numerous commercial enterprises (Chen, 2010; Frucci, 2010).

Another notable case concerning users' privacy comes from Google. In 2010, Google launched a social network *Google Buzz* as competition to Facebook. Google Buzz was launched through Google's Gmail. Google allowed Gmail users to opt out of Buzz. However, users found out that the "opt out" option was ineffective. The Federal Trade Commission (FTC) also complained that Buzz users were provided confusing directions on limiting the sharing of their personal information. Google entered into a settlement with the FTC in 2011, agreeing to implement a comprehensive privacy program and independent privacy audits for the next 20 years (Federal Trade Commission [FTC], 2011).

However, on January 24, 2012, Google announced that starting from March 2012, it would roll sixty privacy policies into one, which would enable it to start following the activities of users of almost all of its ubiquitous sites, such as Gmail, YouTube, and the Google Search Engine. Google claimed that it was already collecting such information but would now be combining the data collected from various sites, so as to build a more comprehensive picture of its users. Most importantly, Google announced that its users would not be able to "opt out" of such information gathering, but noted that users can avoid logging into their accounts if they wanted to avoid this method of information collection. Of course, by not logging in, many useful features would not be available to these users (Kang, 2012).

Predictably, this move by Google also led to a flurry of protests by users and privacy activists. The Commerce, Manufacturing, and Trade Subcommittee of the U.S. Congress held a meeting with Google executives. However, they failed to succeed in changing Google's plans, which went into effect on March 1, 2012. The same day BBC News reported EU's Justice Commissioner Vivian Reding as stating that the privacy changes made by Google were in breach of European law ("Google privacy changes," 2012). As a result, a Europe-wide investigation has been launched. In March, 2012, Google users in New York and California filed lawsuits against Google alleging that the company violated users' privacy rights (Mills, 2012). The legal battle over Google's privacy changes promise to continue well into the future.

The Ethics of Playing God: Censor versus Savior

The role of global networks in disseminating information as well as controlling the same, albeit for "ethical" purposes, is powerfully illustrated in the case David Rhode, a New York Times reporter who was kidnapped by the Taliban in Afghanistan on November 10, 2008. The management of New York Times decided not to publicize the kidnapping – as that would only enhance the bargaining position of the Taliban. (It should be noted that the Taliban, as well as other extremists and terrorists frequently monitor Wikipedia and other news media to get information about their victims). Therefore all news of the kidnapping was kept away from the Times' hard-copy and online format. In addition, the executive editor of the Times persuaded other newspapers to follow suit and hide news of the kidnapping from the mainstream news media. However, soon after the kidnapping, the news started appearing on David Rhode's Wikipedia page, obviously because some contributor had edited Rhode's page. The Times editor then contacted Jimmy Wales, founder of Wikipedia, and requested that the new entries on Rhode be removed. Wales agreed. From then on, all news relating to Rhode's kidnapping was removed from Wikipedia within an hour of such news being posted or edited. Instead, Rhode's profile was altered, to portray him as somebody who had sympathized with Islamic causes before. On one occasion, news of Rhode's predicament was added to Wikipedia four times in four hours, only to be removed just as quickly (Andrefski, 2009; Perez-Pena, 2009). This went on for almost seven months, until David Rhode finally managed to escape from the Taliban. The ethics behind New York Times' decision to hide the news, as well as Jimmy Wales' decision to help the Times by removing certain news edits from David Rhode's Wikipedia, profile raises very interesting questions such as the power of the media and collusion of different types of media in hiding certain news from terrorists and criminals.

Thus, as seen in the above New York Times/David Rhode's case, as well as the cases of Facebook privacy and Blackberry versus Indian Government, the issues of ethics, privacy, censorship, and security often fall under "grey" areas. They often defy clear "black or white" classifications, which makes it more difficult for citizens as well as enforcement agencies to take appropriate actions.

National Security and Democratic Values

The leaked diplomatic cables (in early 2011) by Wikileaks (http://mirror.wikileaks.info/) raise the issues of freedom of expression, information security, and privacy and the values espoused by democratic societies. Wikileaks was registered in 2006 and was meant to be a web location where whistleblowers and dissenters could leak information held secret by organizations and governments. Wikileaks was founded by Julian Assange, an Australian national. After the leaks of sensitive and classified information pertaining to the U.S. led wars in Iraq and Afghanistan, the site and its founder began to attract the attention of U.S. national security agencies.

The site has many supporters and detractors. One main issue that directly relates to Wikileaks is the First Amendment to the United States Constitution, which prohibits the making of any law

that infringes on the freedom of speech and the freedom of the press, among other things. However, Wikileaks detractors question whether "crime-facilitating speech" can fit into the framework of protection guaranteed by the First Amendment. Other issues include the viability of applying the U.S. National Espionage Act of 1917 to stop and possibly prosecute Julian Assange, the on-going tussle between "old" and "new" information and news dissemination media; and the corporate censorship of such questionable media such as Wikileaks. Other aspects to consider are the encryption and other obfuscation technologies used by Wikileaks, and the efforts of some agencies to technologically restrict Wikileaks.

Topic 3: Privacy

Privacy in the U.S. Constitution

The notion of privacy is codified in the Fourth Amendment of the U.S. Constitution and provides protection against unreasonable searches and seizures by the government against an individual. Its origins come from the English common-law maxim "A man's home is his castle" and was discussed by Edward Coke in describing what he called *Semayne's Case* in 1604 (Coke, 1604; Cuddihy, 1990). Many other countries have similarly codified privacy.

In the U.S., invasion of privacy is a tort based on common law. The tort originated from an 1890 Harvard Law Review article by Samuel Warren and Louis Brandeis that included four categories of invasion of privacy: intrusion of solitude; public disclosure of private facts; publication of facts that place a person in false light; and appropriation of personal characteristics in order to attain some benefits. In the U.S., the Privacy Act of 1974 provides the main controls within federal government on the collection, use, and disclosure of personally identifiable information. The law was designed to protect individuals from an increasingly powerful and potentially intrusive federal government (ISPAB, 2009). Laws have also been enacted in other countries such as Canada, EU, and India, even though some of these countries themselves do not explicitly guarantee privacy in their Constitutions. However, in many of these countries, privacy of personal information has gradually gained ground through common-law court precedents.

Privacy Laws and their Application in the Information Society

The Privacy Act of 1974 is, however, just a first step in protecting privacy of individuals. As the Internet continues to permeate every aspect of society, and large scale digitization of every type of data becomes the norm, the privacy of personal information has emerged to be a critical concern. Protecting privacy, civil liberties, and the U.S. Constitution's First Amendment and Fourth Amendment provisions are currently the subjects of serious attention by scholars, governmental agencies, NGOs, and citizen groups.

Additionally, the rapid growth of second generation web and social computing has added to the sense of urgency, as new business models and social transactions are not covered by the older privacy laws. As noted by Daniel J. Chenok, Chairman of the Information Security and Privacy Advisory Board (created by the Computer Security Act of 1987), "The Privacy Act of 1974 is the basis for much of the legal and policy framework by which the U.S. Government handles personal information. At the same time, vast changes in technology since 1974 have transformed how Federal agencies collect, use, and distribute information in major ways. While the fundamentals of the Act—the principles of fair information practices— remain relevant and current, the letter of the Act and related law and policy may not reflect the realities of current technologies and information systems and do not protect against many important threats to privacy. Moreover, new technologies not covered by the Act, are generating new questions and concerns; and gov-

ernment use of private-sector databases now allows the collection and use of detailed personal information with little privacy protections" (ISPAB, 2009).

While the above statement from Chenok describes the inadequacies of privacy framework of the U.S. government, the same inadequacies can also be applied to private enterprises that have had to deal with new technologies and their applications, new methods of data storage and retrieval, and new uses of data.

The Privacy Act itself has several inadequacies, as pointed to by the Congressional Privacy Protection Study Commission (PPSC) in 1977 (PPSC, 1977). As noted by Chenok in the ISPAB report (ISPAB, 2009), no Administration has systematically updated the Privacy Act since 1975.

The ISPAB report also gives a history of privacy legislation, guidelines, and agreements over the years, applying to both public and private sectors. In 1980, the Organization for Economic Co-operation and Development (OECD) adopted guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (OECD, 1980). The guidelines provide eight principles that each member nation should follow in order to safeguard the privacy of individuals. These principles have become the baseline for evaluating privacy and data protection initiatives worldwide. The principles are (from ISPAB, 2009):

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle, and
- Accountability Principle

Many other privacy-related Acts, policies and guidelines in the U.S. have followed the Privacy Act of 1974. They include:

- The Computer Security Act 1987, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, where 'sensitive information' includes the privacy to which individuals are entitled under the Privacy Act 1974, and also to create the Information Security and Privacy Advisory Board (U.S. Congress, 1987).
- The Computer Matching and Privacy Protection Act of 1988, which amended the Privacy Act and added protections to records (subject to the Privacy Act) that are used in computer matching programs used to compare inter-agency as well as non-Federal agency records of an individual in order to make certain decisions (TN Criminal Law Resources, n.d.).
- The memorandum on Privacy Policies and Data Collection on Federal Web Sites, issued by Jacob Lew, Director of OMB, which barred the use of cookies stored in users' computers except under very limited circumstances (OMB, 2000).
- House Resolution (H.R.) 2458, The E-Government Act of 2002 Title II, Section 208, which stipulates that all agencies must post privacy notices on their web sites, to inform users of their information collection practices. The Act also required agencies to com-

plete "privacy impact assessments (PIA) before developing or procuring technologies that collect, store and disseminate personal information (U.S. Congress, 2002).

- H.R. 2458 Title III (The Federal Information Security Management Act 2002) Section 304, which tasks the Information Security and Privacy Advisory Board to advise the NIST, the Secretary of Commerce, and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems (U.S. Congress, 2002).
- The 2003 memorandum "Implementation Guidance for the E-Government Act of 2002"issued by Joshua Bolten, Director of OMB, which provides additional guidance to agencies on the implementation of the E-Government Act (OMB, 2003).
- The 2007 memorandum "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" issued by the OMB, which safeguards personally identifiable information in the possession of the government, and requires agencies to develop a breach notification policy (OMB, 2007).
- The 2008 Department of Homeland Security guidelines that clearly states the agencies maintain only that information which is "directly relevant and necessary to accomplish the specified purpose(s) and only retain *personally identifiable information* (PII) for as long as is necessary to fulfill the specified purpose(s)" (DHS, 2008).

While the above Acts, guidelines and memorandums offer a substantial base for privacy protection by governmental agencies, their implementation has been questioned by the Government Accountability Office (GAO) in a series of reports. In a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, the GAO states that the Privacy Act's protections may not apply to contemporary data processing technologies and applications. In today's highly interconnected environment, information can be gathered from many different sources, analyzed, and redistributed in very dynamic, unstructured ways that may have little to do with the file-oriented concept of a Privacy Act system of records. For example, data mining, a prevalent technique used by federal agencies for extracting useful information from large volumes of data, may escape the purview of the Privacy Act's protections (GAO, 2008).

The problem has been exacerbated since the September 11, 2001, terrorist attacks in the United States. Since then, security agencies have been given the authority to access inter-agency information without much limitation or oversight, which further erodes the privacy protection of citizens. This has set the stage for the new Obama administration to come up with enhancements and revisions to the Privacy Act of 1974. In addition to the GAO report, citizen privacy advocacy groups are also engaging themselves in strengthening privacy protection.

However, for the private citizen, governmental privacy protection is not the sole concern. Currently there is a proliferation of new technologies to track individuals. As noted in the ISPAB (2009, p. 17) report, traditionally, privacy concerns have focused on PII. But today there is privacy concern about the so-called *personally non-identifiable information*. Researchers have discovered that even when an individual's identity is hidden, by giving an anonymous ID, etc., his/her identity can be discovered by using sophisticated analysis and cross-database mining technology. For example, most search engines place cookies or an ID associated with an IP address. Using the combination of the cookie and the IP address, an individual's identity can be revealed, as noted by Barbaro and Zeller (2006), who studied search patterns of AOL users.

New Threats to Privacy

Other threats to privacy come from:

- **Social Networking applications:** Social networking sites have proliferated in the last few years. According to Pew Internet Research, one third (35%) of American adult Internet users have a profile on an online social network site, four times as many as three years ago. Also, 65% of online American teens use social networks" (Lenhart, 2009). The information that people put into applications such as Facebook, Twitter, and My Space can easily be captured by today's data mining tools deployed by third-party "data brokers" who create commercial databases which contain a multitude of information about individuals aggregated from a variety of sources. This data can then be analyzed across various dimensions to create a profile of an individual, by commercial as well as government agencies. Another interesting dimension that arises from these sites includes the ownership of the information that is uploaded into them. For example, who owns such data? Or, what happens to the data pertaining to a person that is already in the system, once the person terminates his/her account, or worse, once a person dies?
- **Locational data or Geo-coding:** Mobile telephones and PDAs have built-in GPS sensors, which can enable mobile telecommunications companies to determine the exact location of a mobile customer at any point in time. While this technology is seemingly innocent, this could raise serious privacy concerns, especially in an environment where government security agencies can request or order the mobile operators to reveal such information. In addition, commercial corporations could also potentially buy such services in order to target services and products to cell phone subscribers based on their locations.
- **The use of commercial databases by government and the private sector:** As mentioned earlier, commercial companies collect and aggregate a variety of information about shoppers, home buyers, library users, contributors to political parties, contributors to social networks, and even some medical information. The current Privacy Act does not monitor or provide any regulation or restriction on the use of such data by the government or by the private sector. In some cases, the private data can be combined with the data collected and maintained by the government, which would provide potent information about specific individuals. An important and revealing example is that of JetBlue, a commercial airline in the U.S. In September, 2003, *Wired* magazine reported that millions of JetBlue passenger records were used by the U.S. Army, ostensibly to "test" data mining techniques to mine data on potential terrorists (Singel, 2004).
- **Proliferation of Data Mining:** Today, data mining is used in a variety of applications, ranging from politics to matrimony or dating referral, using sophisticated data mining techniques combined with quantitative analysis, as noted by Stephen Baker in his book, *The Numerati* (Baker, 2008). As noted in the ISPAB report (2009), poorly designed data mining by governmental and security agencies of private and third party data can sometimes cause wrong inferences to be made about individuals. For example, "an investigator could determine that if two terrorist suspects call the same number three times in the same month, it may —on its face — seem reasonable to want to determine others that have called this same number multiple times. However, if this number were a popular pizza delivery company in a major city, the government could very well be wasting its investigatory resources while invading the privacy of innocent Americans"(ISPAB, 2009).
- **Increase in capability and portability of data storage devices:** Today, USB flash drives can hold several hundreds of thousands of records, ostensibly pertaining to indi-

viduals. It is quite possible that an employee working at a governmental (or private) organization might transfer such data and take it outside his/her place of work, either on purpose or accidentally. Either way, such data faces the risk of being exposed and the identities of those individuals revealed.

The Obama administration has actively been pursuing activities to use social networking and further increase transparency and participation in government using technology. Staff from the OSTP, GSA, and OMB are working on an Open Government Directive to instruct agencies and executive departments how to implement the principles of transparency, participation, and collaboration – and these will inevitably involve the use of technology in ways that are not anticipated in the Privacy Act.

Topic 4: Free & Open Source Software and Open Standards

Free and open source software (FOSS) and open standards are two similar concepts. The former seeks to make software source code freely available and open, so that others can improve upon them or tailor them to suit specific needs. The latter seeks to create a set of open standards that would enable different software and hardware (from different vendors) to inter-operate and work with each other. The operating system *Linux* and the Web server *Apache* are examples of FOSS. *Open Office* is an example of a software type that uses the open standard *Open Document Format* (ODF). Documents created using ODF (using say, Open Office) can be freely opened and modified using any other office productivity software.

One might question the importance of FOSS and Open Standards in our discussion on the *Information Society.* It should however be noted that FOSS has greatly risen in prominence in the last two decades. For instance, the British Internet services company Netcraft reports in its April 2012 web server survey that *Apache*, a free and open software, holds 65.24 percent of the web server market share, followed by Microsoft at 13.81 percent (Netcraft, 2012). According to an April 2012 Comscore Report, the Linux-based *Android* operating system developed and distributed by Google holds a 50.1 percent market share among smart phones in the U.S. (Netburn, 2012). In 2010, the open source and open standard *Open Office* had an international market share of about 12 percent, whereas *Microsoft Office* had a market share of about 78 percent. In Germany, France, Poland, and the Czech Republic, Open Office enjoyed a market share of about 20 percent (Thomas H, 2010). Given these figures, we believe that it is important to discuss pertinent issues about history, development and challenges of FOSS and open standards here.

The Free and Open Software Movement

The ***free software movement*** was started in 1983 by Richard Stallman, a computer scientist working at MIT's Artificial Intelligence Lab. He started the movement at least partly in response to AT&T's plan to commercialize the UNIX operating system, which it was until then freely licensing to universities and non-profit organizations. In an email addressed to friends and fellow computer scientists (Stallman, 1983), Stallman explained the launch of his GNU (Gnu's Not Unix) project as one that was meant to free computer users and software developers from software copyrights and restrictive use licenses. His idea was that when any software became freely available, allowing anybody to use and make changes to it, new innovations would result, the quality of software would improve, and the entire computing and user community would benefit as a result. To start the project, Stallman announced his intent to write and freely release a Unix-compatible system called GNU. GNU was to be a kernel containing all the utilities needed to write and run C programs: editor, shell, C compiler, linker, assembler, etc. After accomplishing that, the project was to add "a text formatter, a YACC, an Empire game, a spreadsheet, and hundreds of other

things. We hope to supply, eventually, everything useful that normally comes with a UNIX system, and anything else useful, including on-line and hardcopy documentation" (Stallman, 1983).

Stallman founded the non-profit Free Software Foundation (FSF) in October 1985 to spread the message and philosophy of free software. The FSF defines free software as follows (adapted from Free Software Foundation, 2010c):

> "Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it means that the program's users have the four essential freedoms:
>
> - The freedom to run the program, for any purpose (freedom 0).
> - The freedom to study how the program works, and change it to make it do what you wish (freedom 1). Access to the source code is a precondition for this.
> - The freedom to redistribute copies so you can help your neighbor (freedom 2).
> - The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this."

Stallman authored the "General Public License" or GPL which is the most widely used free software license. The GPL is called a *copyleft* license (Free Software Foundation, 2007), and its unique characteristic is that works derived from a software product (or any other creative endeavor) by using this license can only be distributed under the same (GPL) license terms.

Today the GNU project and FSF are very well established, and numerous software projects have been released under the GPL. It must be noted that there are numerous "open" or "free" licenses today. Examples among them are the BSD License, MIT License, and Apache license. The free software licenses each come with its own restrictions and level of openness, and can be categorized based on whether the license allows derivative works to link to proprietary software, and whether the derivative can be freely distributed. The distinctions between what each license allows and does not allow is very important for software developers as it could have important ramifications with regards to their use and prospects of future commercialization. Because of this there is currently much debate on the virtues and benefits of one license over another. Comparisons of the licenses are listed and commented upon by the FSF (Free Software Foundation, 2010a), the Open Source Initiative (Open Source Initiative, n.d.), and in the KDE development site (Rusin, n.d.).

Another development that took place during the late 1980s was the formation of the ***"Open Software Foundation"*** (OSF) by seven computer manufacturers. This group, consisting of Apollo Computer, Groupe Bull, Digital Equipment Corporation, Hewlett-Packard, IBM, Nixdorf Computer, and Siemens AG banded together as a reaction to what was perceived to be an attempt at controlling the UNIX operating system by AT&T and Sun Microsystems. As noted earlier, AT&T wanted to commercialize the software, and began implementing very restrictive licensing arrangements. However, there were already several flavors of UNIX in the market, marketed by various companies which had earlier been licensed by AT&T. But AT&T wanted to exercise more control over UNIX and also profit from the software. AT&T developed a close working relationship with Sun Microsystems, a microprocessor manufacturer. Other computer vendors saw this as a move by AT&T and Sun to control UNIX and formed their own "open standards group" called the Open Software Foundation. They tried to develop and popularize a UNIX vari-

ant called OSF-1 and also worked towards creating open standards for the UNIX environment. This consortium, however, was not very effective. In fact, by the early 1990s it became apparent to the UNIX vendors that the real threat to UNIX was not another competing UNIX flavor, but Microsoft Windows operating system. Therefore the former rivals were forced to join together under an initiative named the "Common Open Software Environment" (COSE), and AT&T and Sun Microsystems joined the OSF.

Some of the companies that formed the original consortium do not even exist now. A notable work in standardization that was achieved by this group is in the area of UNIX windowing environments (i.e., Motif X-Windows system). The OSF exists now as "The Open Group" and remains an industry consortium focused on developing common and open standards in computing.

While the free software movement was started in 1983 Stallman, it found resistance in industry. Many conservative business people found Stallman's fervent "free software is freedom" approach too radical and libertarian, and thus the free software movement did not gain much traction initially. It was not until 1998 that the concept of ***Open Source Software*** was initiated by Bruce Perens and Eric S. Raymond. By then the idea of *free* software was not new. Perens and Raymond were supporters of the principle of free software and tried to find a way to make the principle of free and open software politically palatable to industry.

Perens is a former project leader at *Debian*, a well-known Linux distribution. He authored the "Open Source Definition" as a policy document for Debian GNU/Linux Distribution in July 1997. Perens describes the creation of the Open Software Definition thus:

> "Debian, an early Linux system and one still popular today, was built entirely of free software. However, since there were other licenses than the *copyleft* that purported to be free, Debian had some problem defining what was free, and they had never made their free software policy clear to the rest of the world. I was the leader of the Debian project, at that time, and I addressed these problems by proposing a *Debian Social Contrac*t and the *Debian Free Software Guidelines* in July 1997. Many Debian developers had criticisms and improvements that I incorporated into the documents." (Perens, 1999)

Around the same time, on May 27, 1997, Eric Raymond, a computer programmer who had worked on both the GNU project and Linux project synthesized his experiences in working on open and free software projects and presented the essay "The Cathedral and the Bazaar" at the Linux Kongress at Wurzburg (Raymond, 1997). In that essay, he contrasted two free software development models, the *Cathedral Model* and the *Bazaar Model.* The Cathedral model is exemplified by a few select programmers, or a close-knit team, that work on a project and then make the source code open at every release. Important open source software resulting from this model are GNU Emacs and the GCC (GNU C Compiler). The Bazaar model is exemplified by code development by the public at large, through the Internet, in an open code development regime. Any interested party can have access to the code developed at any point, and make additions or changes based on common consensus. An important software resulting from this model is the Linux operating system spearheaded by Linus Torvalds. After publication of "The Cathedral and the Bazaar," Raymond was invited by Netscape Communications Inc. as consultant for their project to make the Netscape software open source.

Perens and Raymond teamed up to author the Open Source Definition which removed certain Debian-specific language from Perens' Debian Free Software Guidelines. The Open Source Definition has ten clauses that emphasize free redistribution, inclusion of source code, allowance for modifications and derived works, protection of the integrity of the author's source code, nondiscrimination against persons, groups, and certain fields of endeavor, and the stipulation that an open source license should not be specific to a product or restrict other software and should be

technology neutral. The entire definition can be found at http://opensource.org/docs/osd. It is important to note that the Open Source Definition is not a license. Rather, it provides criteria that licenses should follow in order to be considered as open source. Several open source licenses exist currently in addition to the GPL. Perens compares some of them with respect to the Open Source Definition in Perens (1999). In developing new software, it is important for a software developer to be aware of these licenses to determine what level of open source criteria the author wishes to adhere to.

The open source software and free software movements have spurred numerous software projects, products, innovations, and new software companies. Red Hat, a Linux distributor is a notable success story. Undoubtedly, the Linux project, with its multifarious distributions, has been the poster-child of the success of open source. Other very successful projects include the *GNU project*, the GNOME windowing environment, the *OpenOffice* project, the *Apache* web server project, the Mozilla *Firefox* browser project, and Google *Chrome* browser project. Google, Inc.'s *Android* operating system, a Linux variant, is a successful open source project. Linux has been incorporated into numerous cellular phones and personal computing devices. Major components of Mac OS X, including the UNIX core, are made available under Apple's Open Source license. IBM Corporation joined the open source world in the late 1990s and gave the movement mainstream credibility.

The Browser Wars

The StatCounter, which collects online visitor statistics, reported on March 2012 that the market share of open source Firefox web browser was 25 percent, the open source Chrome was 31 percent, and Microsoft's Internet Explorer was 35 percent. The data was for the period March 2011 to March 2012 (StatCounter, 2012). This shows that open source web browsers are rapidly increasing in market share. However, the battle for domination of web browsers, and especially the moves made by Microsoft to gain market share in the web browser market and the court battles that ensued, are all important topics of study to the student of information systems.

Interest in open source web browsers has gradually increased over the last two decades, especially as the Internet moved from its academic moorings and individual and commercial usage of the Web increased. The web browser became the primary user interface to traverse and interact with the Web. Netscape was an early leader in developing the web browser that could work in multiple operating systems. The immense success of the Netscape browser, along with the promise of E-Commerce, led Microsoft to develop its own Web browser, Internet Explorer (IE). Soon a full-fledged browser war was in progress between Netscape and IE. Microsoft was accused of using its clout in demanding that PC manufacturers bundle IE with their hardware in order to license the Windows 95 system. On October 27, 1997, the U.S. Department of Justice filed an antitrust lawsuit against Microsoft as a result. On December 11, 1997, in a preliminary injunction, U.S. District Court Judge Thomas Jackson ordered Microsoft to stop requiring PC makers to ship Internet Explorer along with Windows 95 (Wired News Report, 2002). Microsoft promptly appealed the ruling, and since then there have been a series of antitrust lawsuits filed against Microsoft in the U.S., followed by a series of rulings and appeals by both parties. Starting in 2001, twenty States had filed class-action lawsuits against Microsoft. By 2007, Microsoft had reached agreement with The U.S. Department of Justice and 18 out of the 20 of those States.

However, the problems of Microsoft were not over. In the EU, Microsoft faced lawsuits from Opera Software as well as scrutiny by EU regulators. Opera Software ASA is a Norwegian company that provides innovative web browsers that can work on any device – from computers to cell phones to game consoles. On December 13, 2007 Opera filed a complaint with the European Commission, claiming that Microsoft was illegally bundling IE with the Windows operating system, and as a result, was not providing a level playing field for other browsers (Opera Press Re-

leases, 2007). (The European Commission is the antitrust regulator for the 27-nation EU). After investigating Opera Software's antitrust complaint, the European Commission confirmed on January 17, 2009, that it sent Microsoft a Statement of Objections, accusing it of illegally tying Internet Explorer to the Windows PC operating system (Opera Press Releases, 2009). On December 16, 2009, Microsoft settled with the European Commission. Under the terms of the agreement, Microsoft would "provide a 'choice screen' on PCs sold within the European Economic Area that lets users choose which of a dozen or so browsers they would like to set as their default. The screen will be made available for five years and will enable users of Windows XP, Windows Vista, and Windows 7 to choose from a randomly displayed list of browsers. The choice screen will be provided to users via Windows Update" (Johnston, 2009).

Antitrust and the EU

It should be noted that Microsoft is not the only company that has been investigated by the EC for antitrust violations. Literally hundreds of companies from all over the world have been investigated, including several top IT companies headquartered in the U.S. On May 13, 2009, the EC levied its largest ever anti-competitive fine of EURO 1.6 billion against Intel Corporation, after its investigations revealed several instances of anti-competitive practices by Intel in the microprocessor business against Advanced Micro Devices (AMD) (Hodgin, 2009). On February 24, 2010, the EC announced that it was starting an antitrust investigation against Google Inc., in response to complaints filed with the Commission by U.K. price comparison site Foundem, a French legal search engine called eJustice.fr, and a German search site called Ciao that was recently acquired by Microsoft Corp (Meller, 2010). On July 26, 2010, the EC announced that it had opened two antitrust investigations against IBM Corp. in response to complaints by emulator software vendors T3 and Turbo Hercules, which accuse IBM of tying the sale of mainframe hardware to its mainframe operating system (Larson & Hoffman, 2010).

The Open Document Format (ODF) War

Today's documents are increasingly created, maintained, used, and archived in digital form. Individuals, groups, organizations, and governments create and maintain digital documents. Digital documents have several advantages – they are portable, easy to create, revise and edit, allow for collaborative creation, and do not require too much physical storage space. They can be stored in a format that can be read for years.

In this environment, it is useful to note that the majority of digital documents produced in the past two decades have been done so with Microsoft Word or similar proprietary software like Apple's iWork. The market share of Microsoft Office in enterprises is about eighty percent and this lead is not about to be overtaken (Montalbano, 2009). Microsoft holds a complete monopoly over office document formats and, moreover, periodically revises the formats with new releases, making it incompatible with other document formats or other software which may be developed which would accept the MS Word formats. This protects the market position of Microsoft while leaving organizational documents vulnerable to format changes made to MS Word.

Activists, academics, corporate and some governmental organizations started organizing to advocate open document format standards. In November 2002, the Organization for the Advancement of Structured Information Standards (OASIS) announced the formation of a technical committee to advance an open, XML-based format specification for office applications (OASIS, 2002). Sun Microsystems announced its intention to participate and contribute to this process. After several revisions to the original format, a final Open Document Format (ODF) was approved by the OASIS as an OASIS standard in May 2005 (Macnaghten, 2007).

In June 2006, the Open Document Format (ODF) Alliance was formed to promote the use of ODF. The founding members were Sun Microsystems, IBM Corporation, the Open Source Software Research Center and the International Congress on E-Government. As stated in the mission of the ODF Alliance,

> "As documents and services are increasingly transformed from paper to electronic form, there is a growing problem that governments and their constituents may not be able to access, retrieve and use critical records, information and documents in the future. To enable the public sector to have greater control over and direct management of their own records, information and documents, the ODF Alliance seeks to promote and advance the use of Open Document Format (ODF)." (ODF Alliance, 2006)

On November 30, 2006 the International Standards Organization (ISO) ratified the ODF v1.0 as an international standard (ISO, 2006). The concept of open document format continued to gain ground in the EU and other parts of the world such as Brazil and India. In October 2007, the Open Doc Society was formed in the Netherlands to promote and spread the principle of open document standards.

However, the hope of achieving a single document standard became moot when Microsoft announced on November 2005 that it was releasing its own open document format, namely the Office Open XML (OOXML). The OOXML was primarily developed for Microsoft's Office 2007 suite. Later in the same month Microsoft submitted OOXML for ECMA certification as a standard, even though, it was developed without any public consultation or participation, according to some analysts (Macnaghten, 2007). ECMA approved OOXML as a standard in December 2006. After the ECMA certification, OOXML was submitted to the ISO for a "fast-track" certification as an international standard. Microsoft released a draft of over 6000 pages in January 2007 to ISO members for comments that were to be submitted within thirty days.

The "fast-track" certification attempt was met with much disapproval by many of the ISO members as well as open document format activists. Critics were openly voicing their suspicion that Microsoft was making a move towards opening up its document format only to kill the ODF and further cement its control over documents and productivity software. They scrutinized the Microsoft documents and found that many of the openness requirements were not part of Microsoft's OOXML offering. Two clear factions emerged – one consisting of IBM, Sun Microsystems and their affiliates, including the open document activists such as the OpenDoc Society and Open Document Alliance; and the other made up primarily of Microsoft and its affiliates. Needless to say, the former opposed accepting OOXML as an international standard, while the latter supported it. Within a month of the release of the document, an unprecedented twenty countries commented and contradicted aspects of the document. Several nations joined in expressing their opposition to OOXML. The 87 member countries were required to vote on their acceptance of OOXML by September 2, 2007, at the end of a five-month ballot. Finally when the votes were counted, OOXML was approved by 51 countries, while it was disapproved by 18 countries, and the remaining 18 abstained. The ISO approval requires at least two thirds of the votes cast to be positive, and that no more than twenty-five percent of the votes to be negative (ISO, 2007). Since neither of these criteria was achieved, Microsoft's OOXML was rejected in its attempt at standardization in 2007. What was unusual was the level of discord and suspicion that seemed to persist during the ISO voting process. There were accusations that Microsoft used its considerable weight in influencing certain countries and padding their standards bureaus with Microsoft sympathizers, thereby "buying the votes" in many countries. A case in point is Sweden, where several new companies affiliated with Microsoft were allowed to join the voting process at the last minute, which then proceeded to vote in favor of Microsoft. Strident opposition to this change in process eventually led Sweden to change its original "yes" vote to an "abstain" vote.

During the ballot process, many national bodies expressed their reservations on various shortcomings of OOXML. Some examples are the invalid date calculation, differences in the way trigonometric calculations such as sine, cosine, and AVEDEV were actually computed, the use of Windows proprietary formats for graphics, and using non-standard cryptographic methods (Vaidya, n.d.).

The ISO vote then went for a "Ballot Resolution Meeting" in early 2008, where many of the 873 proposed changes were addressed by the ISO members. Members were also given one month to change their ballots. Microsoft was required to give assurances regarding its (future) compliance of the changes requested. Finally, after protracted negotiations between Microsoft and the national bodies, on April 2, 2008 the ISO and IEC formally announced that DIS 29500 (OOXML) had been approved for acceptance as an ISO/IEC standard (Mick, 2008). Four countries, namely South Africa, Venezuela, Brazil, and India appealed the standardization. However, since the ISO process focuses on achieving consensus rather than abandoning any progress made, the appeals did not change the final outcome concerning standardization.

Currently there are two open document "standards." The controversy regarding Microsoft OOXML's compliance to internationally accepted open standards continues to this day, with critics of OOXML protesting that Microsoft has not complied with many of the changes in formats that were conditions to accepting OOXML as an open standard. ODF continues to gain ground among various governments around the world. An ODF status document release by the ODF Alliance states that of date, twenty five governments have adopted ODF standards (ODF Alliance, n.d.; "YearAhead-ODF-2010" n.d.)

Open versus Proprietary Bibliographic Formats

Today much research is conducted on computers on the web. Researchers have often used specialized software to manage their bibliographic collections. In fact, these bibliographic collections form a raw compendium of knowledge sources in any particular area. Taken together, such collections are very valuable sources of knowledge that would benefit not only librarians but also academic and corporate researchers. Today there are several bibliographic software tools available to researchers to organize their research. Some follow proprietary formats whereas others are open source and free software. The open document community does not seem to have focused much on bibliographic software. In the future, open access to these software and their formats will become critical. Such access will enable researchers to access research compendia created and stored in different formats.

Some popular bibliographic software currently in use are Citation, CiteProc, CiteULike, Connotea, Endnote, RefWorks, Mendeley, Zotero, Papers, Bibus, ProCite, Reference Manager, and LaTex/BibTex. Some are stand-alone systems, while others are web-based. Some are specific to certain operating systems and word-processing software (i.e. MS Windows/MS Word). Some are open software and completely web based, such as Zotero from George Mason University.

Given the potential of bibliographic software, it is interesting to note that there is no standard format existing for such software. As a result, there is not much interoperability between the different software. Bibliographic collections maintained in one proprietary software product cannot be easily accessed at present using another software product. Some efforts are underway to standardize bibliographic formats. These are listed in OpenOffice.org's Bibliographic/Software and Standards Information web page (OpenOffice.org, 2010). The *OASIS OpenDocument Technical sub-committee on metadata* is looking at standards for bibliographies (OASIS, 2009). The *Openoffice Bibliographic project* is proposing to use bibliographic citation and reference list generation using a process called CiteProc (OpenOffice.org, n.d.). *Bibliophile* is an initiative founded by Mark Grimshaw (Wikindx), Matthias Steffens (RefBase) and Daniel Pozzi (PHPBibMan) in

2004 to align the development of bibliographic databases for the web. It aims to promote standards, discussion among users on necessary features and a variety of specific solutions for different fields of research. The *Metadata Object Description Schema (MODS)* is a schema for a bibliographic element set that may be used for a variety of purposes, and particularly for library applications. The standard is maintained by the Network Development and MARC Standards Office of the Library of Congress with input from users (Library of Congress, 2010).

Despite these efforts, we believe that the fight for open bibliographic standards is just beginning. On September 5, 2007, Thomson Reuters, owners of *EndNote* (a commercial, proprietary format) fired the first salvo against George Mason University, developer of *Zotero* (an open source, Firefox browser plug-in) by filing a lawsuit against it in the civil division of Richmond City Circuit Court. Thomson Reuters claimed that George Mason was violating its end-user license agreement by including a function within Zotero that would convert EndNote's format to one that was usable by Zotero. EndNote's license agreement contains the following restriction: "End User may not modify, translate, decompile, reverse engineer, retransmit in any form or by any means (electronic, mechanical, photocopied, recorded or otherwise), resell or redistribute the Product, or any portion thereof, without the prior written consent of ResearchSoft. Except as expressly set forth in this Agreement, End User may not make any use of the Product.)" Reuters claimed that Zotero had reverse-engineered its product and format, which violated its rights to its intellectual property and destroyed its customer base, and sought $10 million in damages (Murray, 2008). However, this lawsuit was dismissed in June 2009, as noted by Sean Takat, co-director of the Zotero project (Takat, 2009). Subsequently, the Virginia Supreme Court granted an appeal in this case on December 18, 2009. The journal *Nature* editorialized the decision by stating that while proprietary data formats may be legally defensible, it is open standards (such as those promoted by Zotero) that would spur innovation (Nature Editorial, 2008).

Topic 5: Telecommunications Policy

The rapid spread of computer networks and the invention of innovative applications, such as peer-to-peer computing/file sharing, social networking, "blogs," collaborative authoring, and e-commerce, has necessitated that appropriate public policy positions are taken by governments and corporations in order to protect consumers, corporate intellectual property, and a nation's security. Some hot policy issues that are currently being debated by governmental agencies, activists, consumers and corporate entities are Net neutrality and wireless spectrum allocation and auctions. We briefly address these issues here.

Net Neutrality

The term Net Neutrality refers to the principle that Internet Service Providers (ISPs) should not block or slow down Internet traffic from competing content providers with a view to speed up their own content. In the (not-so-distant) past, ISPs merely acted as transmitters (or carriers) of Internet traffic. However, in recent times they have increasingly become content providers. Net Neutrality activists and other interest groups protested that slowing down a competitor's traffic in order to speed one's own content went against the grain of free choice and was an anti-competitive act. The problem really started in 2005 when incumbent ISPs successfully lobbied with the FCC to repeal their categorization as "common carriers," as that required them to grant bandwidth to new ISPs at discounted rates. However, the FCC continued to manage network traffic of ISPs, and in 2008 the body barred Comcast from using certain peer-to-peer management techniques that would in effect slow down other traffic. But this action by the FCC was rejected by a Washington, D.C. appeals court in 2009. As a result, the FCC wants to now re-classify ISPs as common carriers, albeit with slightly relaxed rules with respect to how they treat other, new ISPs. The FCC also held talk with industry leaders on how to manage the Net Neutrality issue.

However, these talks were called off in early August, 2010, amid reports that Google and Verizon were conducting their own negotiations which would give Google's traffic preferential treatment by Verizon – a charge that both Verizon and Google reject. At present, the state of Net Neutrality (at least in the U.S.) is still not decided (Reed, 2010).

Wireless Spectrum Allocation and Auctions

Radio frequency spectrum is a method to map electromagnetic waves. Radio spectrum ranges from 3 kHz to 300 GHz and may be used for wireless communication. Wireless spectrum is considered a national resource. It is a reusable public good, unlike, say, water or minerals. Its allocation and use is usually managed by individual nations' governments. The wireless spectrum is subdivided into 1G, 2G, 3G, etc., depending on the frequency of transmission of the radio waves. The transmission frequencies further define the capabilities of the waves. Thus a 2G wireless transmission, which uses digital transmission mode, has more capability (can carry more voice, data) and flexibility than a 1G (a voice-only, analog cellular telephone standard) wireless transmission. 2G is divided into CDMA and TDMA, with the latter being used by GSM wireless networks. Almost 80% of the wireless subscribers in the world use GSM networks. Most 2G GSM networks operate at the 900MHz and 1800 MHz frequency bands, with some (as in the United States) operating at 850MHz and 1900MHz bands. 3G GSM networks mostly operate at the 2100 MHz frequency band (Worldtimezone.com, n.d.). 3G transmission standards adhere to ITU standards. Application services provided by 3G networks include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment. 3G systems provide simultaneous speech and data services, at rates of at least 200 Kbits/s. National governments usually release only a limited spectrum range to commercial operators such as mobile phone companies. A few ranges are usually allocated to the military for national-defense and related needs. In several countries, the wireless spectrum allocation to commercial entities such as telecommunications companies is done through auctions run by the government. In some cases, like India, spectrum allocation is split between public and private sector telecommunications companies. Wireless spectrum auctions have to be planned very carefully by national governments, for their ability to attract big revenues or losses. Auctions are more an art than science, and the conditions of an auction can either attach or deter bidders. Some auctions have resulted in loss of revenues or a colossal under-selling of a nation's spectrum. An example is New Zealand, where in 2000 an auction was held for mobile licenses. However the auction allowed very small bid increments and very weak activity rules. As a result, the auction lasted almost a year as bidders hid demand as long as possible (Marsden, 2009). India recently conducted a very successful auction for 3G spectrum, which yielded almost US $ 15 billion (Tripathy, 2010). There have been as many "bad" auctions as there have been "good" auctions, and telecommunications ministries should be aware of auction techniques that are likely to yield successful results.

Topic 6: Information & Communications Technologies for Development (ICT4D)

As computer networks extend their global reach, many developing countries and emerging economies are beginning to see the potential of the networks as a premier tool for delivery of information and knowledge to under-developed areas and under privileged populations. Falling prices of computer hardware and developments in wireless and satellite technologies have enhanced these attempts. The power of computer and communications technologies can be used to aggregate appropriate information and deliver them to rural areas. In many cases, the available technologies are adapted to local conditions. Examples are computer interfaces in different local languages and development of wireless transmitters and receivers and associated hardware that can function in adverse weather conditions, non-standard and unsteady electric voltages, power

failures, etc. Several A2K projects are currently underway in India as well as numerous other developing countries. For the purposes of illustration, we describe an Indian example here (this is adapted from Subramanian & Arivanandan, 2009):

> The M.S. Swaminathan Research Foundation (MSSRF) is a non-profit organization founded by the noted Indian Food and Agricultural scientist, Dr. M.S. Swaminathan. The foundation was registered in 1988 to research, advance, and promote coastal systems, biotechnology, biodiversity, eco technology, food security and information, education, and communication in developing countries, with a specific focus on India. In 1998, the foundation started the "Village Knowledge Centers" project. The idea was to select villages in rural Tamil Nadu and the Union Territory of Pondicherry (both in southern India) and provide adequate telecommunications infrastructure that would enable the dissemination of appropriate information regarding farming, education, health, weather, governmental news, job, loans, and aid opportunities. The objectives were to reduce the digital gap and gender divide in rural India using technology – especially telecommunications technology. Each Village Knowledge Center (VKC) would serve one or more villages and would act as the knowledge repository for the villages it served. Pertinent information was stored in databases in these sites, with appropriate technology for easy access and dissemination of this knowledge to persons seeking them. The long term objective was to eventually set up VKCs in each of the approximately 638, 000 villages in India, thus creating a nation-wide rural knowledge repository.
>
> The MSSRF project uses a Hub and Spokes model. The highest tier is the State-level hub at the MSSRF headquarters. The informatics center at the State-level hub is connected to the Internet through Internet Service Providers (ISPs) and to the ISRO up-link satellite through a Very Small Aperture Terminal (VSAT) antenna. The informatics center is connected to universities, scientific institutions, governmental agencies, and other panels of experts. Information from these external sources are collected, collated, and transmitted using the VSAT connection.
>
> The next tier is the Village Resource Center (VRC). Each VRC serves as a hub, typically connected to 20-30 VKCs spread over a 60Km radius. The VRC is designed to act as a rural library and technology resource center. Each VRC consists of at least three networked computers, one scanner, two web cameras, Internet access, one printer, one digital camera, solar backup facility, and training rooms. Each VRC is also connected to other VRCs and the MSSRF headquarters in Chennai through satellite link-ups, in collaboration with the Indian Space Research Organization (ISRO). The ISRO-MSSRF network uses one of the Extended C-band transponders of ISRO's satellite INSAT-3A. Users at each VRC and at the headquarters in Chennai can communicate through video and audio links provided by the satellite connection (ISRO, 2004). The Village Resource Centers at various rural locations are connected to the tier-1 State-level informatics center (and ISRO satellite) through VSAT. Internet connectivity to the various VRCs is achieved through the ISRO-MSSRF network.
>
> The VRCs in turn provide network connectivity to the Village Knowledge Centers (VKCs), which serve a particular village. The VKCs form the third tier of the MSSRF architecture. Each VRC is connected to the VKCs and other VRCs using Motorola very high frequency (VHF) radios for voice and data transmission. In 2001, spread spectrum wireless technology was introduced for VRC-VKC and

> VKC-VKC communications. The VKCs are usually equipped with desktop computers, printer, radio communications equipment, wireless tower antenna, a video kiosk, and applications such as desk-top publishing. The applications vary from VKC to VKC, depending upon specific need.

The MSSRF model is a highly successful model that is focused on development and A2K. In addition to this, there are other models currently operating in India, with various degrees of success. A detailed description of these models is beyond the scope of this paper but can be studied for understanding A2K technologies and models in developing countries.

One promising ICT4D project that is currently garnering attention is the One Laptop per Child (OLPC). What is interesting here is the technology and software that would be supplied through this project. This gives rise to interesting questions such as: What operating system would be used? What will be the configuration of the laptop? What accessibility features will be built in? Who will hold the licenses for this product? Will only open source software be installed on this laptop? Who will provide training to the end-users as well as the trainers? How will these machines be maintained?

Conclusion: How does the Information Society Affect IS Educators and IS Education?

As can be inferred from the above discussion, we believe that in order for a student of IS to succeed in today's environment, it is important for her/him to be knowledgeable about issues that affect the information society. That requires that every educator actively acquires the appropriate knowledge and then tailors and disseminates (i.e., *informs*) that knowledge in the classroom environment, as well as through conferences and consultative practices (i.e., transformation). The IS student who experiences this is the *client* in this scenario. Upon graduation, the IS graduate uses his/her knowledge of the use, relevance, and application of IT in the day-to-day environment. In addition, the graduate becomes the informer, transforming her acquired information to fit the organizational requirements in the context of the *Information Society.* The clients in this scenario also include colleagues, subordinates, and other stake holders. This idea of a particular player performing different roles within the informing context has been noted by William Murphy Jr., in his article elucidating the Informing Science Institute's role as the "informing system" of the IS transdiscipline (Murphy, 2011).

We represent the ideas of viewing IS education as an informing science, as well as the different roles that an individual can assume (i.e., an IS student – a client – can later assume the role of IS manager – an informer) by incorporating them within Cohen's representation of an informing system in *Figures 1* and *2*, respectively.

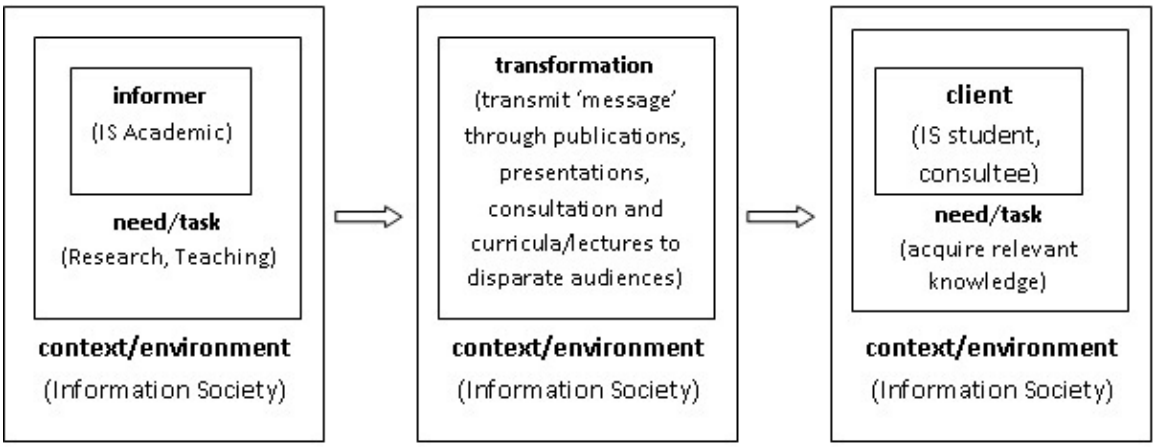


Figure 1: The IS academic as informer and IS student as client

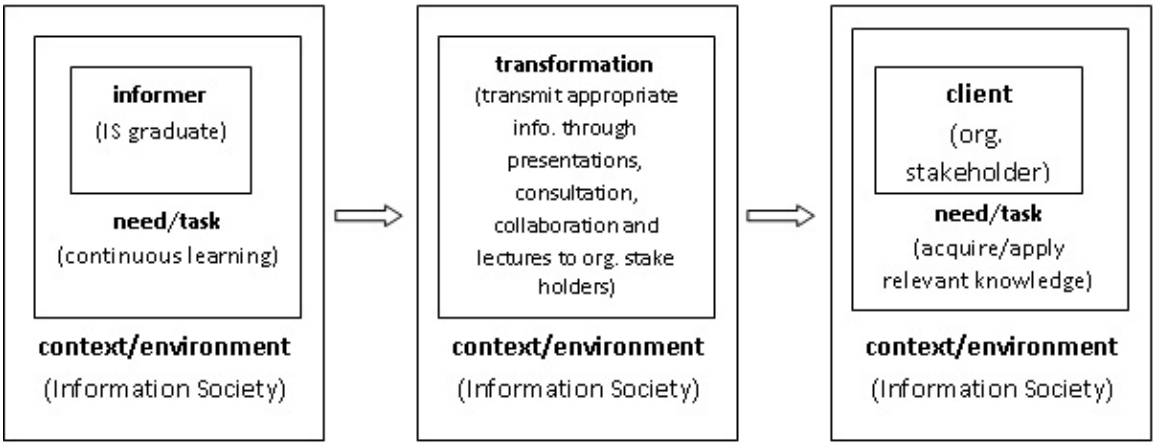


Figure 2: The IS Graduate as informer and organizational stakeholder as client

In conclusion, we submit that every IS educator, IT specialist, or IT manager needs to address the issues that inform the *Information Society*. At present, these topics are not adequately addressed in the existing IS curricula in the U.S. While it is possible that non-U.S.-based institutions may use IS curricula that may include some of these topics pertaining to the *Information Society,* it is highly likely that these institutions may be following the AIS/AITP/ACM 2002 model and the recent AIS/ACM 2010 model. As noted earlier, the concepts presented in this paper are present in very few places, if at all, in these model curricula.

Despite this, we still feel that it is important to take the first steps in addressing the shortcomings. We suggest two possible places for Information Society coverage among the courses listed in the IS 2010 model curriculum: Course IS 2010.1 - Foundations of Information Systems, and course IS 2010.7 - IS Strategy, Management and Acquisition.

IS2010.1 Foundations of Information Systems has this partial course description: *"Information systems are an integral part of all business activities and careers. This course is designed to introduce students to contemporary information systems and demonstrate how these systems are used throughout global organizations. The focus of this course will be on the key components of information systems - people, software, hardware, data, and communication technologies, and how these components can be integrated and managed to create competitive advantage"* (Topi et

al., 2010). We suggest that that is not necessarily a good fit for coverage of *Information Society* concepts, although some concepts might fit into the IS2010.1 bailiwick.

IS2010.7 Strategy, Management and Acquisition has this partial course description towards the end of the overall description: *"The remainder of the course is focused on developing an intellectual framework that will allow leaders of organizations to critically assess existing IS infrastructures and emerging technologies as well as how these enabling technologies might affect organizational strategy. The ideas developed and cultivated in this course are intended to provide an enduring perspective that can help leaders make sense of an increasingly globalized and technology intensive business environment"* (Topi et al., 2010).

We suggest that the Information Society would fit into the framework of IS2010.7 – under the "intellectual framework", "organizational strategy", "increasingly globalized and technology intensive" terminology.

These are just a few suggestions. Unfortunately, they barely touch the tip of the iceberg – metaphorically speaking. Much more needs to be done by the IS community to herald a more relevant, modern, "systems approach" to IS curriculum issues. We believe that it is time the IS academic community embraced the broader perspective – one based on the notion that the information systems field is a "trans-discipline." If that is done, then it will prepare IS students to gain a deeper understanding of not just the technical aspects, but also the societal aspects of information systems in general.

We believe that the Informing Science Institute is ideally positioned to undertake the task of informing the IS discipline on the value of teaching the *Information Society* to students of information systems. It would thus be of value to create a "teaching information society" working group within the Informing Science Institute that will focus on this very important and relevant issue.

References

Andrefski, J. (2009, June 29). Wikipedia gets behind the NY Times to help hide story of kidnapping by Taliban. *Gadgetell*. Retrieved August 11, 2010, from http://www.gadgetell.com/tech/comment/wikipedia-gets-behind-the-ny-times-to-help-hide-story-of-kidnapping-by-tali/

Baker, S. (2008). *The Numerati*. Houghton Mifflin Harcourt.

Balkin, J. (2010, Spring). *The Information Society: Spring 2010 Syllabus*-- Professor Balkin. Retrieved June 15, 2011, from http://www.yale.edu/lawweb/jbalkin/syllabi/theinformationsocietysyllabusspring2010.htm

Barbaro, M., & Zeller, T. (2006, August 9). A face is exposed for AOL searcher No. 4417749 - *New York Times*. Retrieved July 1, 2009, from http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000

Barrett, P. M. (2012, March 29). Apple's war on Android - *Businessweek*. Retrieved April 6, 2012, from http://www.businessweek.com/articles/2012-03-29/apple-s-war-on-android

Borland, J., & Barnes, C. (2000, July 26). Judge issues injunction against Napster. *CNET News*. Retrieved June 26, 2009, from http://news.cnet.com/2100-1023-243698.html

Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review*, *81*(5), 41–49.

Castells, M. (1996). *The rise of the network society: The information age: Economy, society, and culture*. Information Age Series (1st ed., Vol. 1). Blackwell. Retrieved from http://www.amazon.com/The-Rise-Network-Society-Information/dp/1405196866

Chao, L. (2009, June 8). China squeezes PC makers. *Wall Street Journal.* Retrieved August 9, 2010, from http://online.wsj.com/article/SB124440211524192081.html

Center for Internet and Society [CIS]. (n.d.). *Rowling v. RDR Books*. Retrieved June 25, 2009, from http://cyberlaw.stanford.edu/case/rowling-v-rdr-books

Chen, J. (2010, July 29). Major corporations are downloading those 100 million Facebook profiles off Bit-Torrent. *Gizmodo*. Retrieved August 11, 2010, from http://gizmodo.com/5599970/major-corporations-are-downloading-those-100-million-facebook-profiles-off-bittorrent

CitizenLab. (n.d.). *Projects – The citizen lab.* Retrieved August 10, 2010, from http://citizenlab.org/projects/

Cohen, E. B. (2009). A philosophy of informing science. *Informing Science: the International Journal of an Emerging Transdiscipline*, *12*, 1–15. Retrieved from http://www.inform.nu/Articles/Vol12/ISJv12p001-015Cohen399.pdf

Coke, S. E. (1604). *Online library of liberty - Semayne's case. - Selected writings of Sir Edward Coke* (vol. I.) Retrieved August 13, 2010, from http://oll.libertyfund.org/?option=com_staticxt&staticfile=show.php%3Ftitle=911&chapter=106328&layout=html&Itemid=27

Cuddihy, W. (1990). *The fourth amendment: Origins and original meaning* (Ph.D. Dissertation). Claremont Graduate School, Claremont, CA.

DHS. (2008, December 29). *Memorandum 2008-01 - The fair information practice principles: Framework for privacy policy at the Department of Homeland Security*. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Electronic Frontier Foundation [EFF]. (2008). *Unintended consequences: Ten years under the DMCA | Electronic Frontier Foundation* (White paper). Retrieved from http://www.eff.org/wp/unintended-consequences-ten-years-under-dmca

Electronic Frontier Foundation [EFF]. (n.d.). *Defending freedom in the digital world*. Retrieved June 25, 2009, from http://www.eff.org/

Esguerra, R. (2010, April 28). *A handy Facebook-to-English translator*. Electronic Frontier Foundation. Retrieved August 11, 2010, from http://www.eff.org/deeplinks/2010/04/handy-facebook-english-translator

Federal Trade Commission [FTC]. (2011, March 30). *FTC charges deceptive privacy practices in Google's rollout of its Buzz Social Network*. Retrieved April 6, 2012, from http://www.ftc.gov/opa/2011/03/google.shtm

Free Software Foundation. (2007, June 29). *The GNU General Public License Version 3.* GNU Project - Free Software Foundation (FSF). Retrieved July 23, 2010, from http://www.gnu.org/licenses/gpl.html

Free Software Foundation. (2010a). *Various licenses and comments about them*. GNU Project - Free Software Foundation (FSF). Retrieved July 24, 2010, from *http://www.gnu.org/licenses/license-list.html*

Free Software Foundation. (2010b, June 16). *Speak out against ACTA — Free Software Foundation — working together for free software*. Retrieved August 11, 2010, from http://www.fsf.org/campaigns/acta/

Free Software Foundation. (2010c, July 1). *The free software definition.* GNU Project - Free Software Foundation (FSF). Retrieved July 23, 2010, from http://www.gnu.org/philosophy/free-sw.html

Frucci, A. (2010, July 28). 100 million Facebook profile pages leaked to Torrent site. *Gizmodo*. Retrieved August 11, 2010, from http://gizmodo.com/5598825/100-million-facebook-profile-pages-leaked-to-torrent-site

GAO. (2008). *PRIVACY - Congress should consider alternatives for strengthening protection of personally identifiable information*. Retrieved from http://www.gao.gov/new.items/d08795t.pdf

Gardener, J. (2010, February 10). A2K4 Panel II: Technologies of dissent: Information and expression in a digital world : Information Society Project at Yale Law School. *Information Society Project at Yale Law School*. Retrieved August 9, 2010, from http://yaleisp.org/2010/02/a2k4dissent/

Gill, G., & Bhattacherjee, A. (2007). The informing sciences at a crossroads: The role of the client. *Informing Science: the International Journal of an Emerging Transdiscipline*, *10*, 17-39. Retrieved from http://www.inform.nu/Articles/Vol10/ISJv10p017-039Gill317.pdf

Google privacy changes 'in breach of EU law.' (2012, March 1). *BBC News.* Retrieved April 6, 2012, from http://www.bbc.co.uk/news/technology-17205754

Gorgone, J. T., Davis, G. B., Valacich, J. S., Topi, H., Feinstein, D. L., & Longenecker, H. E. (2003). Model curriculum and guidelines for undergraduate degree programs in information systems. *Database for advances in Information Systems*, *34*(1).

Harrison, A. (2006, March 13). The Pirate Bay: Here to stay? *Wired*. Retrieved from http://www.wired.com/science/discoveries/news/2006/03/70358

Hartley, A. (2009, April 17). Pirate Bay Four get a year in prison. *TechRadar UK.* Retrieved June 27, 2009, from http://www.techradar.com/news/internet/pirate-bay-four-get-a-year-in-prison-592931

Hodgin, R. (2009, May 13). *Analysis: EU Commission's antitrust ruling against Intel Corporation – Computer Chips & Hardware Technology*. Geek.com. Retrieved July 29, 2010, from http://www.geek.com/articles/chips/analysis-eu-commissions-antitrust-ruling-against-intel-corporation-20090513/

International Telecommunications Union. (2003, December 12). *WSIS: Declaration of principles*. Retrieved March 22, 2012, from *http://www.itu.int/wsis/docs/geneva/official/dop.html*

ISO. (2006, November 30). *ISO/IEC 26300:2006 - Information technology -- Open Document Format for office applications (OpenDocument) v1.0*. Retrieved July 31, 2010, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485

ISO. (2007, September 4). *ISO - News - Vote closes on draft ISO/IEC DIS 29500 standard*. Retrieved August 2, 2010, from http://www.iso.org/iso/pressrelease.htm?refid=Ref1070

ISPAB. (2009). *Toward a 21st century framework for federal government privacy policy*. Retrieved from http://www.ostp.gov/galleries/opengov_inbox/ISPAB_Report_dc_w_lh.pdf

ISRO. (2004, October 18). *Inauguration of ISRO-MSSRF village resource centre (VRC) project by Prime Minister*. Retrieved May 5, 2009, from http://www.isro.org/pressrelease/Oct14_2004.htm

Johnston, S. J. (2009, December 16). Microsoft settles with the European Commission. *Datamation.com*. Retrieved July 29, 2010, from http://itmanagement.earthweb.com/entdev/article.php/3853896/Microsoft-Settles-With-the-European-Commission.htm

Kang, C. (2012, January 24). Google tracks consumers' online activities across products, and users can't opt out. *The Washington Post*. Retrieved April 6, 2012, from http://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html

Larson, E., & Hoffman, K. (2010, July 27). *IBM investigated by EU regulator over mainframe market - Bloomberg.* Retrieved July 29, 2010, from http://www.bloomberg.com/news/2010-07-26/ibm-probed-by-eu-for-alleged-abuse-of-dominant-mainframe-computer-position.html

Lenhart, A. (2009, January 14). *PEW Internet project data memo*. Retrieved July 3, 2009, from http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf

Library of Congress. (2010, June 14). *Metadata object description schema: MODS* (Library of Congress). Retrieved August 5, 2010, from http://www.loc.gov/standards/mods/

Machemedze, R. (2003, January). TRIPs agreement factsheet. *SEATINI*. Retrieved August 10, 2010, from http://www.seatini.org/publications/factsheets/trips.htm

Macnaghten, E. (2007, February 5). *ODF/OOXML technical white paper*. Retrieved July 30, 2010, from http://www.freesoftwaremagazine.com/node/2138/pdf?page=0,0

Marsden, R. (2009, April 29). *spectrumauctionsintro.ppt - Powered by Google Docs*. Presented at the SKMM Spectrum Economics Workshop, Cyberjaya, Malaysia. Retrieved from http://docs.google.com/viewer?a=v&q=cache:JFcRJv-QdAkJ:www.dotecon.com/publications/spectrumauctionsintro.pdf+new+zealand+spectrum+auction+low+bid&hl=en&gl=in&pid=bl&srcid=ADGEESiJInCaYcW1jRlC2JMh0m4AoY_4ovfyVj62Fyv4jlNNvR8HmmdZn-Ve0N8zZD-lWGu3g2-90dsty2_CZ0JU2PGrkNnzbNE54aVdjonku9O6EE1FLKJF957lY02KywNVL1QTSIkj&sig=AHIEtbQhn_xK1qld7l8_DDTCMYl30FmUnw

Meller, P. (2010, February 24). Update: EC confirms Google antitrust probe. *Computerworld*. Retrieved July 29, 2010, from http://www.computerworld.com/s/article/9161398/Update_EC_confirms_Google_antitrust_probe

Mick, J. (2008, April 2). Microsoft wins document format standards battle. *DailyTech*. Retrieved August 5, 2010, from http://www.dailytech.com/Microsoft+Wins+Document+Format+Standards+Battle/article11338.htm

Mills, E. (2012, March 22). Google users sue over changes to privacy policy. *InSecurity Complex - CNET News*. Retrieved April 6, 2012, from http://news.cnet.com/8301-27080_3-57402965-245/google-users-sue-over-changes-to-privacy-policy/

Montalbano, E. (2009, June 4). *Forrester: Microsoft Office in no danger from competitors*. Retrieved July 30, 2010, from http://www.networkworld.com/news/2009/060409-forrester-microsoft-office-in-no.html?fsrc=netflash-rss

Murphy, W. F., Jr. (2011). The Informing Science Institute: The informing system of a transdiscipline. *Informing Science: the International Journal of an Emerging Transdiscipline*, *14,* 91-123. Retrieved from http://www.inform.nu/Articles/Vol14/ISJv14p091-123Murphy598.pdf

Murray, P. E. (2008, September 27). George Mason University sued by Thomson Reuters over Zotero. *Disruptive Library Technology Jester*. Retrieved from http://webcache.googleusercontent.com/search?q=cache:http://dltj.org/article/endnote-zotero-lawsuit/

Nature Editorial. (2008). Beta blockers? *Nature*. Retrieved from http://www.webcitation.org/5py7np6z6

Netburn, D. (2012, April 3). *Comscore: Google's Android is most popular operating system in US - latimes.com*. Retrieved April 7, 2012, from http://www.latimes.com/business/technology/la-fi-tn-comscore-google-android--smartphone-market-20120403,0,3349703.story

Netcraft. (2012, April). *Web server survey*. Retrieved April 7, 2012, from http://news.netcraft.com/archives/category/web-server-survey/

OASIS. (2002, November 20). *OASIS - News - 11_20_2002*. Retrieved July 30, 2010, from http://www.oasis-open.org/news/oasis_news_11_20_02.php

OASIS. (2009, December 8). *Bibliographies and Citations - Office Wiki.* Retrieved August 5, 2010, from http://wiki.oasis-open.org/office/Bibliographies_and_Citations

ODF Alliance. (2006, June 14). *About the ODF Alliance.* Retrieved July 30, 2010, from *http://www.odfalliance.in/About.html*

ODF Alliance. (n.d.). *ODF Alliance update: State of ODF and Outlook for 2010*. Retrieved from http://www.odfalliance.org/resources/YearAhead-ODF-2010.pdf

OECD. (1980, September 23). *OECD guidelines on the protection of privacy and transborder flows of personal data.* Retrieved June 30, 2009, from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

OMB. (2000, June 22). *Memorandum M-00-13: Privacy policies and data collection on federal web sites*. Retrieved from http://www.whitehouse.gov/omb/memoranda_m00-13/

OMB. (2003, August 1). *Memorandum m03-18: Implementation guidance for the E-Government Act of 2002*. Retrieved from http://www.whitehouse.gov/omb/memoranda/m03-18.pdf

OMB. (2007, May 22). *Memorandum m07-16: Safeguarding against and responding to the breach of personally identifiable information.* Retrieved June 30, 2009, from http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

Open Source Initiative. (n.d.). *Open Source licenses by category*. Retrieved July 24, 2010, from http://www.opensource.org/licenses/category

OpenNet Initiative. (n.d.). *About ONI*. Retrieved August 10, 2010, from http://opennet.net/about-oni

OpenOffice.org. (2010, July 20). *Bibliographic/software and standards information*. Retrieved August 5, 2010, from http://wiki.services.openoffice.org/wiki/Bibliographic/Software_and_Standards_Information

OpenOffice.org. (n.d.). *bibliographic: CiteProc - Main Page.* Retrieved August 5, 2010, from http://bibliographic.openoffice.org/citeproc/index.html

Opera Press Releases. (2007, December 13). *Opera files antitrust complaint with the EU*. Retrieved July 29, 2010, from http://www.opera.com/press/releases/2007/12/13/

Opera Press Releases. (2009, January 17). *European Commission accuses Microsoft of illegally tying Internet Explorer to Windows*. Retrieved July 29, 2010, from http://choice.opera.com/press/releases/2009/01/17/

Parrack, D. (2009, February 16). *The Pirate Bay trial begins in Sweden: IFPI begins fight against file-sharers everywhere*. Retrieved June 27, 2009, from http://www.webtvwire.com/the-pirate-bay-trial-begins-in-sweden-ifpi-begins-fight-against-file-sharers-everywhere/

Perens, B. (1999). *The open sources definition. Open Sources: Voices from the open source revolution* (1st ed.). O'Reilly. Retrieved from http://oreilly.com/catalog/opensources/book/perens.html

Perez-Pena, R. (2009, June 28). Keeping news of David Rohde's kidnapping off Wikipedia. *NY Times.* Retrieved August 11, 2010, from http://www.nytimes.com/2009/06/29/technology/internet/29wiki.html?_r=1

Pike, G. H. (2008, June). Putting academic fair use to the test. *Information Today*. Retrieved from http://www.infotoday.com/IT/jun08/Pike.shtml

Pirate Bay. (n.d.). *The Pirate Bay - Technical specs!* Retrieved June 27, 2009, from http://static.thepiratebay.org/

PPSC. (1977). *Personal privacy in an information society*. Retrieved from http://aspe.hhs.gov/DATACNCL/1977privacy/toc.htm

Reed, B. (2010, August 7). Net Neutrality: What's really going on? *PCWorld*. Retrieved August 8, 2010, from http://www.pcworld.com/article/202835/net_neutrality_whats_really_going_on.html?loomia_ow=t0:s0:a38:g26:r11:c0.009145:b36362862:z0

Raymond, E. S. (1997, May 27). *The cathedral and the bazaar.* Presented at the Internationaler Linux-Kongreß in Würzburg auf der Festung Nachlese (Linux-Kongress), Wurzburg. Retrieved from http://www.linux-kongress.org/1997/raymond.html

Rusin, Z. (n.d.). *Open source licenses comparison.* Retrieved July 24, 2010, from http://developer.kde.org/documentation/licensing/licenses_summary.html

Sarno, D. (2007, April 29). The Internet sure loves its outlaws. *Los Angeles Times.* Retrieved June 27, 2009, from http://www.latimes.com/entertainment/news/la-ca-webscout29apr29,0,1261622.story?coll=la-home-entertainment

Schlein, L. (2008, February 21). *Record number of patents filed in 2007*. Retrieved June 24, 2009, from http://www.voanews.com/english/archive/2008-02/2008-02-21-voa64.cfm?CFID=239723608&CFTOKEN=22196403&jsessionid=8830156157d3db1114681d4f97a31154e373

Shaw, A. (2008). The problem with the Anti-Counterfeiting Trade Agreement (and what to do about it). *KEStudies*, *2*. Retrieved from http://www.kestudies.org/ojs/index.php/kes/article/view/34/59

Singel, R. (2004, August 23). Army: JetBlue data use was legal. *Wired Magazine*. Retrieved from http://www.wired.com/politics/law/news/2004/08/64647

Stallman, R. M. (1983, September 27). *About the GNU Project*. GNU Project - Free Software Foundation (FSF): Initial Announcement. Retrieved July 22, 2010, from http://www.gnu.org/gnu/initial-announcement.html

StatCounter. (2012, March). *Top 5 browsers from March 2011 to March 2012*. Retrieved April 7, 2012, from http://gs.statcounter.com/

Stehr, N. (1999). *Knowledge societies*. Presented at the Globalitás – tudástársadalom – lokalitás" of the Third Millenium Foundation, Fot, Hungary. Retrieved from http://www.inco.hu/inco3/kozpont/cikk0h.htm#1

Stiverson, K. A. (2008). *AALL Issue Brief 2008-1*. AALL Copyright Committee. Retrieved from http://www.aallnet.org/aallwash/ib042008a.pdf

Subramanian, R., & Arivanandan, M. (2009). Rural development through village knowledge centers in India. *Communications of the IIMA*, *9*(2).

Takat, S. (2009, June 4). Thomson Reuters lawsuit dismissed. *The Quintessence of Ham*. Retrieved from http://quintessenceofham.org/2009/06/04/thomson-reuters-lawsuit-dismissed/

Taylor, S., & Karam, S. (2010, August 6). *Canada aids RIM as BlackBerry ban looms*. Retrieved August 10, 2010, from http://in.reuters.com/article/idINIndia-50664820100805

Templeton, B. (2008, October). *10 Big myths about copyright explained.* Retrieved June 25, 2009, from http://www.templetons.com/brad/copymyths.html

Thomas H. (2010, February 5). International OpenOffice market shares. *Webmasterpro.de*. Retrieved April 5, 2012, from http://www.webmasterpro.de/portal/news/2010/02/05/international-openoffice-market-shares.html

TN Criminal Law Resources. (n.d.). *A citizen's guide on using the Freedom of Information Act and the Privacy Act of 1974 to request government records: VII. B. THE COMPUTER MATCHING AND PRIVACY PROTECTION ACT.* Hosted by TnCrimLaw. Retrieved July 4, 2009, from http://www.tncrimlaw.com/foia/VII_B.html

Topi, H., Valacich, J., Wright, R., Kaiser, K., Jay Nunamaker, J., Sipior, J., & Vreede, G. J. de. (2010). IS 2010: Curriculum guidelines for undergraduate degree programs in Information Systems. *Communications of the Association for Information Systems*, *26*(1). Retrieved from http://aisel.aisnet.org/cais/vol26/iss1/18

Touraine, A. (1988). *Return of the actor*. Minneapolis: University of Minnesota Press.

Tripathy, D. (2010, May 19). Vodafone, Bharti pay total $5.1 billion for 3G spectrum. *Money - DNA*. Retrieved August 9, 2010, from http://www.dnaindia.com/money/report_vodafone-bharti-win-key-india-3g-spectrum_1385059

U.S. Congress. (1987). *Public Law H.R. 145 - Computer Security Act of 1987*. Retrieved from http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf

U.S. Congress. (2002). *HR2458 - The E-Government Act of 2002*. Retrieved from http://csrc.nist.gov/drivers/documents/HR2458-final.pdf

United States Trade Representative. (2009). *The Anti-Counterfeiting Trade Agreement - Summary of key elements under discussion*. Retrieved from http://www.ustr.gov/sites/default/files/uploads/factsheets/2009/asset_upload_file917_15546.pdf

Vaidya, A. (n.d.). *Microsoft OOXML/ECMA376: Get the facts*. Retrieved from http://noooxml.wdfiles.com/local--files/arguments/ODF-vs-OOXML-v1.2.pdf

van Dijk, J. (1999). *The network society: Social aspects of new media* (1st ed.). SAGE Publications Ltd.

Wall Street Journal. (2008, September 8). Judge Patterson's ruling, at the Wall Street Journal. Retrieved June 25, 2009, from http://online.wsj.com/public/resources/documents/potterdecision.pdf

World Intellectual Property Organization [WIPO]. (n.d.). *Understanding intellectual property.* WIPO. Retrieved from http://www.wipo.int/freepublications/en/intproperty/895/wipo_pub_895.pdf

Wired News Report. (2002, November 4). *U.S. v. Microsoft: Timeline.* Retrieved July 28, 2010, from http://www.wired.com/techbiz/it/news/2002/11/35212

World Trade Organization [WTO]. (n.d.). *Understanding the WTO - Intellectual property: Protection and enforcement*. Retrieved August 10, 2010, from http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm

Worldtimezone.com. (n.d.). *GSM world coverage map- GSM country list by frequency bands*. Retrieved August 9, 2010, from http://www.worldtimezone.com/gsm.html

YearAhead-ODF-2010.pdf. (n.d.). Retrieved from http://www.odfalliance.org/resources/YearAhead-ODF-2010.pdf

Appendix: Course Sequence Structures

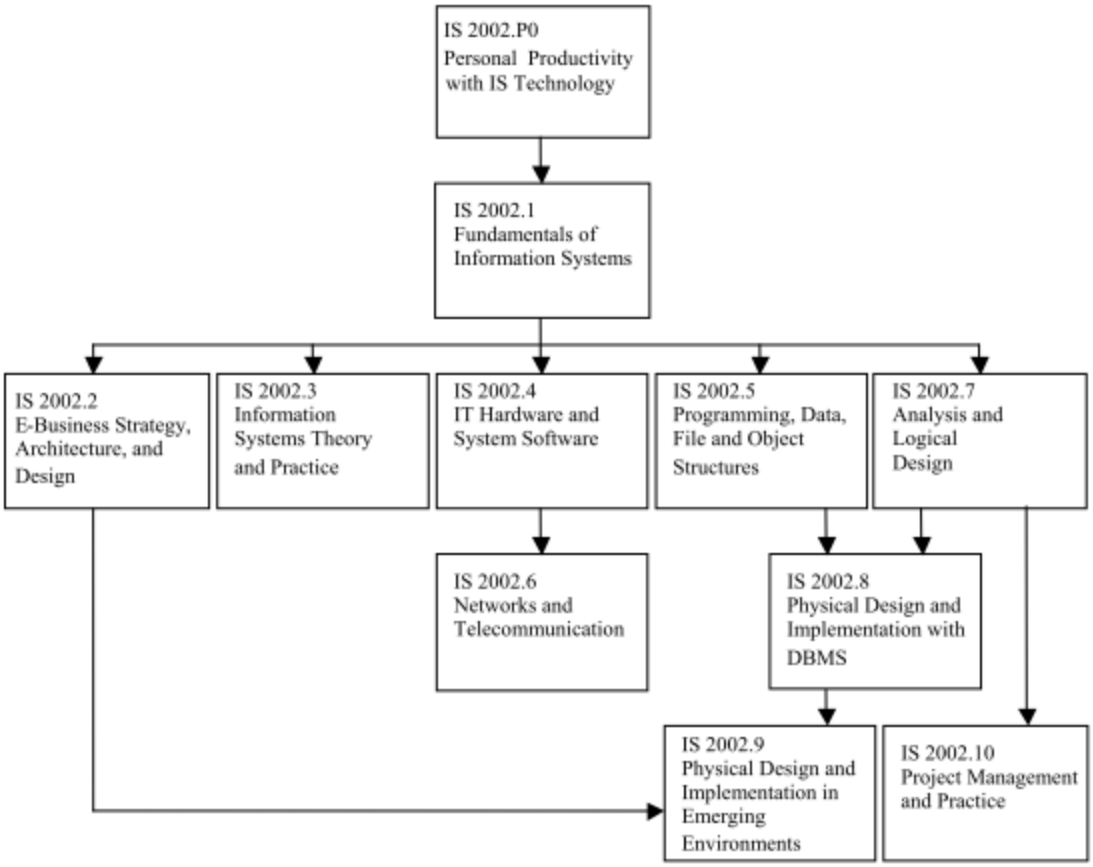


Figure 3: IS 2002: Representative Course Sequence

Structure of the IS Model Curriculum:Information Systems specific courses

Career Track:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Core IS Courses:																	
Foundations of IS	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Enterprise Architecture	○	●	○	○	○	●	○	○	○	○	●	○	○	○	●	○	○
IS Strategy, Management and Acquisition	○	●	○	○	○	●	○	○	●	○	●	○	○	○	●	○	○
Data and Information Management	●	○	○	●	●	○	○	●	●	○	●	○	●	○	○	○	○
Systems Analysis & Design	●	●	●	○	○	○	●	○	○	○	○	○	○	○	●	●	●
IT Infrastructure	○	○	○	●	○	○	○	●	●	●	○	○	●	●	○	○	○
IT Project Management	●	○	○	○	○	●	○	○	○	○	●	○	○	○	●	●	●
Elective IS Courses:																	
Application Development	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●
Business Process Management		●	●			○	○	○		○	●				○		
Collaborative Computing						○								○			○
Data Mining / Business Intelligence		●		●	●	○	○	○	●		○	○	○	○	○		○
Enterprise Systems		●	●	○	○	○	●	●	○		●	●	○	○			
Human-Computer Interaction	●					○	○				○					●	
Information Search and Retrieval		○		○	●								○				●
IT Audit and Controls	○		●	○	○	○	○	●		●	○		○	○	○		○
IT Security and Risk Management	○			○	○	○	○	●	●	○	○		●	●	○		○
Knowledge Management		●		○		○	○			○							
Social Informatics													○		○		

Key:

● = Significant Coverage

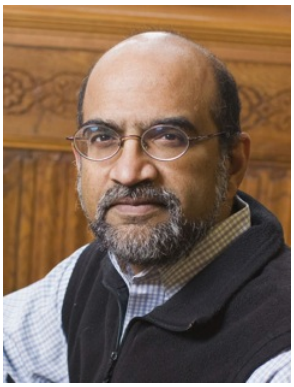
○ = Some Coverage

Blank Cell = Not Required

A = Application Developer
B = Business Analyst
C = Business Process Analyst
D = Database Administrator
E = Database Analyst
F = e-Business Manager
G = ERP Specialist
H = Information Auditing and Compliance Specialist
I = IT Architect
J = IT Asset Manager
K = IT Consultant
L = IT Operations Manager
M = IT Security and Risk Manager
N = Network Administrator
O = Project Manager
P = User Interface Designer
Q = Web Content Manager

Figure 4: Structure of the IS 2010 Model Curriculum

Biographies



Ramesh Subramanian (B.Sc. in Applied Sciences, 1980, Madras University, India; P.G. Honors Dip. in Management, 1984, XLRI, India; M.B.A., 1990 and Ph.D., 1992, Rutgers University) is the Gabriel Ferrucci Professor of Computer Information Systems at the School of Business, Quinnipiac University, and Visiting Fellow at the Yale Law School's "Information Society Project." In 2008-2009, Dr. Subramanian was awarded a Fulbright Senior Researcher grant to study the effects and consequences of Internet spread in rural India.

Dr. Subramanian's current research interests include Information Systems Security, History of Technology, ICT4D, Technology and Public Policy (including privacy, access to knowledge and network neutrality). He is especially interested in the intersection of security, privacy and politics, and has published several peer-reviewed articles and papers in these areas. Published books include "Access to Knowledge in India: New Research on Intellectual Property, Innovation and Development," (Dec 2011), Bloomsbury Academic Publishing, London, UK; "The Global Flow of Information: Legal, Social and Cultural Perspectives," (August 2011), New York University Press, NY; "Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions," (March 2008), IGI-Global Publishing, Hershey, PA, U.S.A.; and "Peer-to-Peer Computing: The Evolution of a Disruptive Technology," (2005), Idea Group Publishing: Hershey, PA, U.S.A.

Bruce White (B.S. in Mathematics, 1969, Winona State University, Winona Minnesota, USA; M.S. in Mathematics, 1973, Winona State University, Winona, Minnesota, USA; Ph.D. in Management Information Systems, 1990, University of Nebraska, Lincoln, Nebraska, USA) is a Professor of Computer Information Systems at Quinnipiac University in Hamden, Connecticut, USA.

Dr. White's current research interests include: critical thinking in IS education; IT outsourcing, tablet computing, and IS education.

He has received the 2008 AITP-EDSIG Information Systems Educator of the Year; the 2008 Quinnipiac University Center for Excellence in Teaching award; the 2012 James Marshall Award for Outstanding Service to the Quinnipiac Community; the 2011 Quinnipiac University Outstanding Faculty Award of the Student Government Association, and is an AITP EDSIG Fellow. He also is active as an ABET program evaluator. He is a co-author of Web 2.0 for Business: Learning the New Tools, published by John Wiley & sons in 2010.