


# Privacy Please: A Privacy Curriculum Taxonomy (PCT) For The Era Of Personal Intelligence

E. Vincent Carter, (E-mail: Sphere797@aol.com), California State University, Bakersfield

## ABSTRACT

*This paper extends forward thinking by information ethics and business education scholars to introduce a Privacy Curriculum Taxonomy (PCT) that repurposes business curricula around the emerging personal information privacy paradigm. The seminal challenge confronting business education leaders is to respond to the ontological paradigm shift from a physical society driven by material and monetary processes, towards a digital society driven by information supply and the growing demand for information privacy. The PCT is advanced as an initial framework for engaging business curriculum planners in the considerations required to repurpose existing disciplines around digital society information and privacy processes. After a current literature review, the PCT is developed using a foundational set of information assurance principles. The PCT is business discipline specific, to catalyze incubation and further development within and across functional areas.*

## FINDING THE POTENTIAL FOR PERSONAL INFORMATION PRIVACY IN THE BUSINESS CURRICULUM

thics is becoming a profitable business. Once an oxymoron, this is now the rule for a information intensive, computer-mediated, post 9-11, global e-commerce society. Peter Drucker [1954] is widely cited for defining the purpose of business as creating and satisfying customers. However, according to information technology sage Geoffrey Moore, America has crossed the “chasm” into a society where “...information about an asset is more valuable than the asset itself.” [Liataud 2001, p. 6]. Even Drucker might concur that the parallel business purpose for the future is to create and maintain information about customers. Herein lay the seed of ethics’ newfound profitability. With a growing business imperative to gather and analyze customer information, how does an enterprise sustain customer relationships without the assurance that information retrieval will be secure and sensitive? These converging trains of digital commerce and information ethics collide at personal information privacy.

If business commerce is reeling from the personal information privacy collision then how well prepared is the business education curriculum to further learners’ ability to frame and navigate this intersection of digital commerce and information ethics? Business and management education journals address information technology issues [Hoffman 2005; Hoffman 2002; Kearsley 2000; Liao 1996] but omit the “digital literacy” information techniques related to assurance, governance, integrity, and privacy of business intelligence – except in rare instances [Tyner 1998]. In other words, management education embraces the business of digital, but is not yet preparing business learners for “being digital” [Negroponte 1991].

Peterson and Ferrell [2005] challenge business education and management leaders to harness the power of business ethics for future corporate and curriculum success. Extending this directive into the realm of Internet technology and information ethics, Bush, et al. [2003] advocate a constructive alliance of values among corporate stakeholders – including business education. This paper extends this recent research to rectify the imbalance between information technology and information technique in the business education curriculum, by introducing a Privacy Curriculum Taxonomy (PCT) that guides the realignment primary business disciplines with the unfolding personal information privacy paradigm.

**FRAMING PERSONAL INFORMATION PRIVACY WITH BUSINESS CURRICULUM CATEGORIES**

Information privacy in the United States is an extension of constitutional individual privacy rights that is linked inextricably to information technology diffusion in a digital society [Friedman 2000; Paul, et al. 2000]. However, in practical terms, personal information privacy has come to the attention of the American psyche largely through the heightened concern with online consumer privacy, consumer credit fraud, and most recently cyber-terrorism. For that reason, consumer privacy in general [Goodwin 1991] and online consumer privacy in particular [Caudill and Murphy 2000] are exemplars of the ever expanding set of digital information ethics concerns that can be classified as personal information privacy [Raul 2002; Floridi 1999; Bennett and Grant 1999; Severson 1997]. Still, business curriculum planners must treat information privacy as a fundamental shift in ontology, affecting the nature of social and business reality. Namely, the transition from physically defined traditional societies towards information defined digital societies [Tapscott 2000, 1997; Cronin 2000]. Just as Guttenberg's printing technology catalyzed the formation of literature and education content that has furthered the collective fields of the academy – not simply print makers, digital technology is fostering new fields for the systematic study and application of information – not simply data security analysts. Therefore, the business curriculum's personal information privacy charge is to be relevant in terms of John Seeley Brown's [2000] "social life of information."

One need only chronicle the recent spate of personal information privacy regulation and legislation to get a glimpse of its social thrust and business muster. The Sarbanes-Oxley Act of 2002, the USA Patriot Act of 2001, and the Online Privacy Protection Act of 2001 are the trinity of information privacy regulation. Together, they frame the social and business boundaries in an information intensive computer mediated environment. Sarbanes-Oxley is precise in its terms of information security compliance, although originally for financial accountability, and has widespread adoption among major U.S. businesses. The Online Privacy Act directs attention to personal information risks exclusive to electronic data transactions, the leading privacy concern of online users. The USA Patriot Act responded to a post 9-11 atmosphere of heightened security by relaxing traditional Constitutional 4<sup>th</sup> Amendment privacy rights [Leiberman 1978; Westin 1967; Brandeis 1928]. Expanded surveillance, mobile tracking, and online monitoring raise a threatening sword to privacy concerns. At the same time, the Patriot Act seeds advance data security, digital forensics, cyber-terror defense, spy ware, and authentication software development. These information assurance components raise a protecting privacy plowshare. Add to this regulation triangle pertinent credit [FACTA 2003], education [FERPA 2002], and healthcare [HIPAA 1996] variants and the expanding circumference of personal information privacy becomes real.

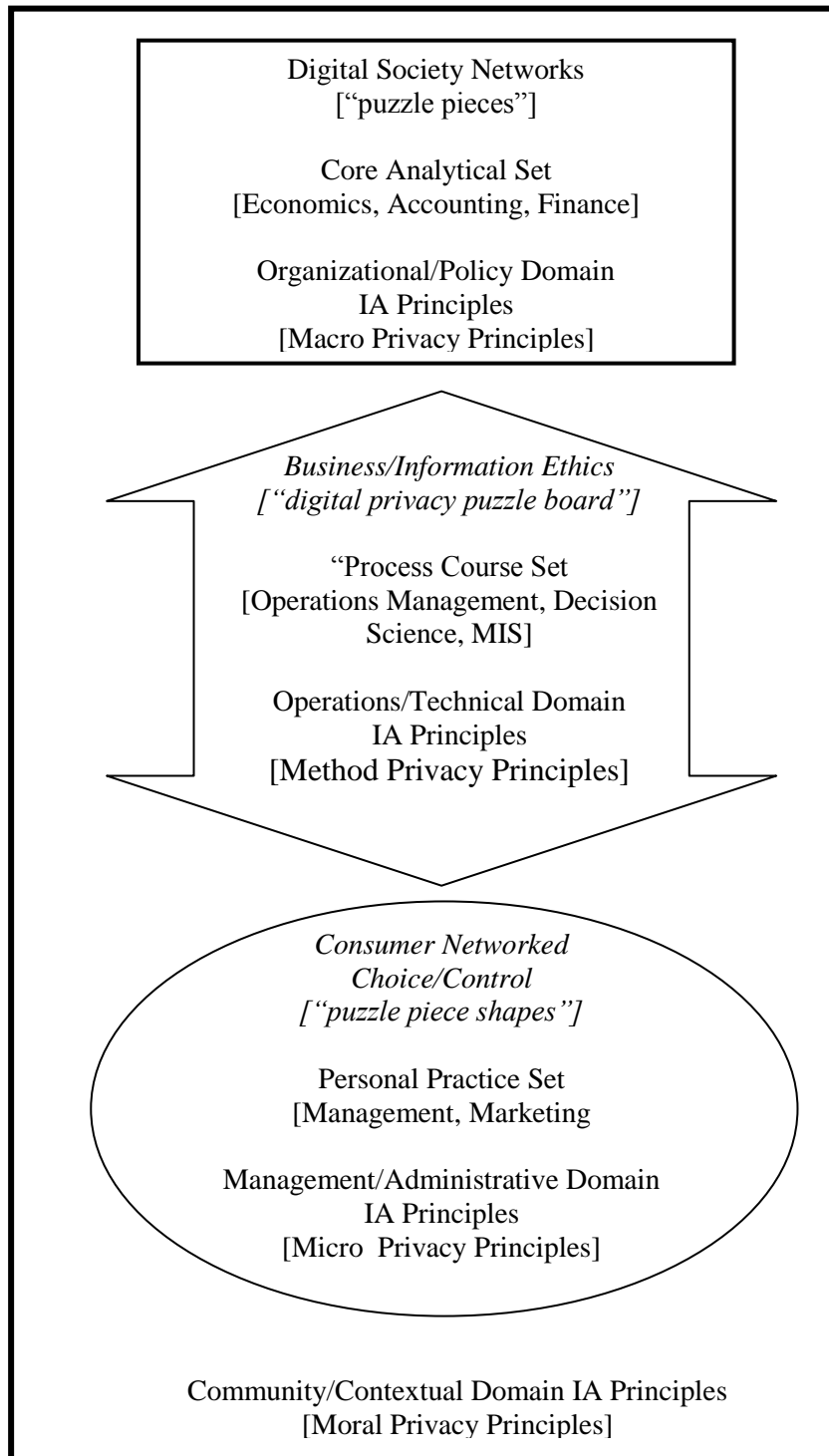
To get some sense of personal privacy's panoramic scope, simply open your wallet and literally lay out the cards of your life – and our society. Not only would the common person's wallet identification portray their profile, but they profile of society and business as well. Health card signifies healthcare sector. Bank cards signify financial sector. Driver's license signifies the criminal justice sector. Depending on the person, this information map might include libraries and schools, places of employment and enjoyment, as well as various digital device access codes. Such is the expanding ecology of personal information privacy where business purpose is indeed defined by customer information profiles.

*Companies that develop strategies to convince stakeholders to trust them will have a major competitive advantage over those that cannot [Gilbert 2006, p.74]*

Mapping the primary drivers of personal information privacy is an effective way for business and management educators to plot the privacy impacts on particular disciplines. Figure 1 shows a way of clustering the drivers of personal information privacy according to three prominent curriculum categories. Logically, the *core analytical set* of business disciplines like economics, accounting, and finance can derive curricular benefits by addressing personal information privacy dynamics. The digital networked economy scrambles the traditional marketplace puzzle-pieces. Traditional market exchange roles performed by companies and customers [Wigand 2003; Malone, et al. 1998; Benjamin and Wigand 1995] are inverted by the "logic of digital business networks." Instead of traditional one-to-many protocols that directed mass market transactions, many-to-many interactions are diverse and customized [Tapscott 2000; Pine 1998]. Customers dominate information flow and exercise choices when interacting with companies. Just as asset valuation and exchange lay the foundation for business economics, accounting, and

finance, newer constructs like privacy economics and intellectual capital, prepare learners for a future where information is currency, commodity, and channel [Turban, et al. 2004; Moore 2003; Evans and Wurster 1999].

**Figure 1**  
**The Drivers of Personal Information Privacy and Information Assurance Index**



If digital society networks scramble business and management education puzzle pieces, then the second driver consumer choice and control changes their shapes. The many-to-many “computer-mediated” customer networks [Hoffman and Novak 1996], relied upon by most American firms are becoming more information transparent. Customers information search and react to company motives, while companies digitally sense and respond” to customer metrics [Aiker 1998; Bradley and Nolan 1998]. More important, many-to-many networked customers can electronically coalesce to share information to support companies that are personal information privacy champions -- and punish companies that are not [Seybold 1998]. As personal information privacy becomes a consumer priority, transparent boundaries will make ethics profitable and marketable, in accordance with FTC “fair information practices”:

- a. *Notice/Awareness* – covers disclosure of information practices, including a comprehensive statement of information use – information storage, manipulation, and discrimination,
- b. *Choice/Consent* – includes both opt-in and opt-out options and gives consumers the choice to trade information for benefits, depending on the value consumers place on benefits,
- c. *Access/Participation* – allows for the confirmation of accuracy of information, necessary when information is aggregated in multiple sources
- d. *Integrity/Security* – controls for theft or tampering
- e. *Enforcement/Redress* – provides a mechanism to ensure compliance by participating companies; this mechanism is an important credibility cue for online companies but is extremely difficult to accomplish effectively [FTC 1998]

Although the “fair information practices” respond to consumer privacy concerns, they are the public extrinsic shield for an essentially personal intrinsic phenomenon. Customers as well as employees construct identities and lives with the personal information shared through digital society interaction. For these more private intrinsic reasons for public information rules, the personal practice oriented disciplines like management and marketing are best suited to direct business education curriculum development.

Mediating digital society information flows and networked consumer choice/control, is the third personal information privacy driver -- *business and information ethics*. Information ethics fashions new privacy puzzle boards that fit reshaped digital consumer choice/control pieces. Although business/information ethics is a qualitative driver, in the digital society context it is appropriately channeled within organizations and with markets by quantitative process systems and sciences. For that reason it is labeled here as the *process mediation set* of business education curriculum courses. Just like social agency [Bowie and Freeman 1992; Eisenhardt 1989] mediates the “moral hazard” of ethical dilemmas between traditional business stakeholders, “information ecologies” [Nardi and O’Day 1999; Davenport and Prusak 1997] embed digital ethics in the “information value chain” [Porter and Millar 1979] – and more recently “virtual value chain” [Rayport and Sviokla 1995]. This includes operations, management information systems, decision science, and logistics. Personal information privacy applications to these process courses will address the timing and method of operational intelligence use, as well as data safety protections. These mediating business fields contribute to privacy curricula by operationalizing information assurance as knowledge management systems [Wenger, et al. 2002] comprised of learning organizations, intellectual capital diagnosis, process engineering, and information architecture [Bontis 1999; Davenport 1993; Senge 1990].

## **FORMULATING PERSONAL INFORMATION PRIVACY PRINCIPLES FOR THE BUSINESS CURRICULUM**

Information Assurance (IA) studies hold the best promise for providing sufficient comprehension of the digital, customer choice/control, and social ethics drivers of personal information privacy. When first initiated as an outgrowth of data security research for the U.S. National Security Agency [NSA] [www.nsa.gov](http://www.nsa.gov), IA focused on hardware/network “firewalls” and ant-virus patches. Eventually, IA became a more holistic study of the principles that further information integrity, confidentiality, accountability, and control [NSRB 2005]. IA is unique in its intended transfer of principles across academic disciplines and between research and practice, and among digital and traditional modes of interaction.

As the definitive body with authority over prescribing information assurance (IA) policy and practice, the National Standards Registration Board (NSRB), LLC is a logical reference for the information privacy taxonomy for the business curriculum. The NSRB's Information Assurance Principles are deliberately focused on "cyberspace" dynamics such as personal privacy. The comprehensive IA principles listed below are applicable in to the business curriculum as a whole, as well as to individual disciplines. In addition, these IA principles are cross validated with NSA best practices for securing intelligence assets, and are divided into four "domains":

- A. Organizational/Policy Domain
  1. Organizational Security – long term protection plan for information/technology assets
  2. Define Security Infrastructure – design and implement IA infrastructure/procedures
  3. Establish Education Plan – develop proactive IA awareness and practice programs to secure human resources and insure staff capability to protect intelligence assets
  4. Asset Management – devise intelligence asset identification processes and baseline control measures and maintain a record of audits in an asset accounting repository.
  5. Business Continuity – establish and maintain action plans to prevent disruption of core business and functional processes that are vital to organizational stakeholders
  6. Regulatory Compliance – develop and implement control procedures to ensure compliance with all regulations, laws, and security practices
- B. Managerial/Administrative Domain
  7. Information security life-cycle process development for all integral intelligence assets
  8. Personnel training in security policies and practices for information handling
  9. Physical asset security monitoring, including facilities and all tangible assets
- C. Operational/Technical Domain
  10. Information access and control procedures secure electronic and physical assets
  11. Operations security procedures align staff/skills with information tasks
  12. Network security protocols protect unauthorized intelligence network access or harm
  13. Application/software security procedures insure operability of intelligence systems
  14. Risk assessment and control assessments as ongoing audits of system vulnerability
- D. Community/Contextual Domain
  15. Ethics code adoption and adherence to preempt intelligence security threats for the organization, stakeholders, and constituents

The IA principles listed above help identify personal information privacy objectives for business education curriculum disciplines. Referring back to Figure 1, the IA considerations discussed here generally parallel the three modules representing personal information privacy drivers. These combined course design guidelines help business curriculum disciplines improve their digital society validity of courses. Describing examples from each domain will provide insight regarding the use of this IA based course index to repurpose business disciplines around the personal information privacy construct.

"Organizational/Policy" sets forth *macro privacy principles* associated with the analytical core business disciplines of economics, accounting, and finance – as well as organizational policy oriented management courses such as business law/ethics and organizational design/behavior. For economics, IA principles to improve the ability of courses to address information value, structures, and security as parallel to traditional economic value, structures, and growth. Business Law courses must incorporate the information policies, intellectual property rights, and asset intelligence protections which must be considered for organizational management. Accounting and Finance have the expertise to appraise and value the core economic assets exchanged [Acquisti 2004 <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm#new>; Stewart 1998; Urbany 1986; Stigler 1981]. Customers supply information to fuel the digital commerce intelligence demands of companies. Simultaneously, customers demand privacy for supplying information and companies profit by supplying information ethics, in order to secure the intelligence sources they demand.

Management disciplines support privacy economic analysis by adapting information privacy to organizational design and behavior constructs [Smith, et al. 1996]. These digital enterprise design objectives impart administrative science decision techniques [Simon 1997] for an era of virtual knowledge creating corporations, practicing strategic information governance in electronic markets. [Liataud 2001; Nonaka and Takeuchi 1995; Benjamin and Wigand 1995; Davidow 1992].

A similar gleaning of business curriculum privacy inclusion can be gained by finding relevant associations within the other three IA principle domains. For instance, the “Managerial/Administrative” domain addresses *micro privacy principles* that focus on the human element within information exchanges. IA principles adapt courses to emphasize the use of management and market metrics to digitally profile information value and privacy risks. Course constructs that enable these intelligence profiles to be synchronized into profitable relationships will also be stressed. These human intelligence interaction aspects, and their personal privacy implications, are the purview of marketing and management disciplines because they involve the psychology of trust [Rust, et al. 2002; Sirdeshmukh, et al. 2002; Serva, et al. 2001]. By addressing these micro privacy principles, the management/marketing disciplines leverage trust in a digital context [Jevons and Gabbot 2000; Urban, et al. 2000; Mayer, et al. 1995]. Thus, students learn about information as a consumed and created commodity.

When these marketing and management human information assurance synergies are supported by the third, “Operational/Technical” domain, a kind of “neo-motion study” skill set emerges for information handlers in the market and organization [Taylor 1998; Kanigel 1997]. However, unlike the efficiency maximization template of time/motion and method used to study Taylor’s industrial age assemblers, the digital society template minimizes data retrieval risks with digital tracking measures [Aiker 1998] and privacy exchange actuaries [Haberman, et al. 2003]. Accordingly, this set of IA considerations constitutes the *method privacy principles*. This type of information assurance process synchronization will typically involve operations management, decision science, and MIS disciplines.

Once operations courses are re-engineered, their digital privacy contributions to the business education curriculum come in the form of knowledge management skills [Shaw, et al. 2001] for effective intelligence generation and representation [Slater and Narver 2000; Paton and Neilsen 1999; Tufte 1997], efficient information product assembly [Meyer and Zack 1996], and efficacious data mining for customer relationship management [Hamell and Prashantham 2001; Tavani 1999; Young and Sauer 1996].

Returning to business law/ethics disciplines, corporate citizenship, information governance, and privacy compliance are the axes of information assurance for the “Community/Contextual” domain [Etzioni 2000; Langford 2000; Brown and Druid 2000]. These *moral privacy principles* embrace information ethics research supporting personal privacy rights comparable to Jeffersonian liberties for traditional society [Volkman 2003; Michelfelder 2001].

It was observed above that business and management education curricula have embraced information technology, but are far less enlightened about including information techniques for critical thinking about personal information privacy issues. This imbalance towards instructional technology tools hurt business curricular awareness of the need for information literacy techniques. However, the foundation for including personal information privacy in the business curriculum is solidly established in the general business and management literature.

Business ethics journals are foremost in validating the management advantages of information assurance and personal data privacy policies for preserving valuable digital era assets [Stead and Gilbert 2001; Reichheld and Scheffer 2000; Westin 1999; Bibas 1994], as well as to perform good corporate citizenship. Within disciplines, public and social policy outlets are more likely to present information privacy studies than are other journal categories [Sunder, et al. 2003; Buchholz and Rosenthal 2002; Wolfenburger and Gilly 2001; Caudill and Murphy 2000].

Second to these business ethics organs in advancing information privacy research are the consumer affairs, consumer research, and customer relationship management [CRM] journals [Miyazaki and Krishnamurthy 2002; Franzak, et al. 2001; Allen 2001; Hamell and Prashantham 2001; Cronin 2000]. It is quite natural in a dynamic digital

commerce society for consumer studies to include the influence of personal information on customer tendencies and preferences.

Third, in order of business journals addressing information privacy, are the digital technology anchored MIS and decision science publications [Rykere 2002; Stewart and Segars 2002; Smith, et. al 1996]. Although these journals' topics emphasize digital systems more than social information strategies, real progress is being made towards embedding many social information variables in organizational intelligence networks [Christopher 2003; Gilhooly 2002; Wenger, et al. 2002].

The pattern found by this literature review is not coincidence. Framing personal information privacy with the three drivers of the phenomenon -- ethics, consumer choice/control, and the digital network infrastructure – trains the business curriculum on the academic research most likely to know. Most recently, this confluence of information ethics, digital technology and consumer choice/control has spawned a handful of edited volumes [Langford 2000; Paul, et al. 2000], journals, and think tanks advancing what might be termed digital information ethics. These include; Ethics and Information Technology Journal, Electronic Journal of Business Ethics and Organization Studies, Online Journal of Ethics, and privacy centers [Electronic Privacy Information Center [www.epic.org](http://www.epic.org); Electronic Freedom Foundation [www.eff.org](http://www.eff.org); Privacy Rights Clearinghouse [www.prc.org](http://www.prc.org)].

These relevant research sources add credence to the drivers of personal information privacy and strengthen the imperative to include privacy more prominently in the business curriculum. Timely research is solidifying the vital role of digital information ethics, and in particular personal information privacy, for future business and management practice. Spinello and Tavani [2001] capture these Internet-related ethics issues with a comprehensive index and theoretical framework. In fact these incubators of digital information ethics research reinforce the business privacy curriculum formulation modeled here using information assurance principles.

## **FACTORING PEDAGOGY INTO THE PERSONAL INFORMATION PRIVACY CURRICULUM FOR BUSINESS**

Information and technology ethics scholars have defined the evolution from traditional to digital society as a radical ontological change [Floridi 2002; Koepsell 2000; Graham 1999]. Agres, et al. [1998] describe the forces and issues inherent to this transition into “virtual society” and cast new information literacy skills at the forefront. When society undergoes these paradigm shifts in the nature of human being educational curricula are expected to guide and enlighten – not blindly lag. Like the digital age future foreseen by Bennett and Grant (2000), the business education curriculum should be “visioning privacy” as a central component of its disciplines academic credibility and professional relevance. Making this transition from studying digital society to creating “digital literacy” [Gilster 2000] will poise business and management education to fulfill society’s future intelligence demands [Tyner 1998]. By coupling information assurance principles with instructional techniques the business curriculum extends personal information privacy from an e-commerce paradigm into an educational pedagogy.

The personal information privacy construct is posited here as the nexus of these new intelligence pedagogies. The PCT introduces a pedagogically sound planning instrument to rectify a glaring imbalance between the information privacy labyrinth strangling business enterprise and the information privacy learning supporting business education. This vulnerable social and business education chasm has prompted Oravec’s [1999] proposed integration of information privacy into teacher education curricula. This rare response to information privacy’s educational imperative can serve as a benchmark for the business education curriculum.

*Teacher educators can work to introduce privacy notions to future teachers in ways that will enhance both their information technology studies and their understanding of other curricular areas (including citizenship, business, and social studies). [Oravec 1999, p.50]*

However, pockets of intellectual leadership exist for repurposing the business education curriculum around information privacy issues. The E-Business Ethics Center, under the auspices of the Center for Business Ethics and Social Issues at Colorado State University <http://www.e-businessethics.com/>, is advancing information ethics and

privacy studies with a central focus on improving curricula and pedagogy devoted to teaching business ethics. Notwithstanding these academic oases advocating inclusion of information privacy in educational curricula, the landscape is bare. Consequently, the proposed ACT provides a path out of this intellectual desert to enable business education to flourish.

Moreover, the PCT's inclusion of personal information privacy outcomes creates positive synergies between Bloom's pedagogical objectives and the IA principles for improving intelligence awareness [Desman 2001]. By coupling of academic knowledge with the IA skills required for organizational employment, the PCT offers a more pragmatic learner-centered template for addressing the expanding adult education and training population. Knowles [1984, 1980] and other instructional design scholars [Brookfield 1988; Burge 1988] use the term "andragogy" to contrast this more intrinsic, experiential, and self directed learning method with the standard "pedagogical" methods that are not as conducive to adult learners. Likewise, the PCT addresses the growing online education versioning of the business education curriculum. The PCT's emphasis on information assurance principles and digital literacy skills fulfill "technology-based learning" objectives, as well as other online business education prescriptions [Rosenberg 2001; Kearsley 2000; Marquardt and Kearsley 1998; Martin 1997]. In fact, as the transparency widens between the virtual realm of business practice and web-based realm of business education [Palloff and Pratt 1999; Tiffin and Rajasingham 1995], addressing personal information privacy issues in business education will become even more vital.

There is a general consensus in the education literature that pedagogy is guided by Bloom's Taxonomy of Educational Objectives [Bloom and Krathwohl 1956]. It is, therefore, fortunate that the pedagogical parameters and progression put forth by Bloom, parallels the information hierarchy [Haeckel and Nolan 1993; Ackoff 1989; Cleveland 1985], upon which the National Security Agency's information assurance "Signals Intelligence [SIGINT]" pyramid is based <http://www.nsa.gov/sigint/>. Figure 2 presents the ACT as a combination of these three pedagogical dimensions, and overlays the IA principles described above for business disciplines, to yield the proposed Privacy Curriculum Taxonomy [PCT]. The PCT imbues the business education curriculum with the capacity to plan and coordinate personal information privacy learning, just as SIGINT elevates information assurance and national security intelligence capabilities.

*SIGINT plays a vital role in our national security by employing the right people and using the latest technology to provide America's leaders with the critical information they need to save lives, defend democracy, and promote American values. [U.S.A. National Security Agency, 2005].*

Using Bloom's six stage education framework as a benchmark, the PCT adds a pre-stage beneath the first stage of Bloom, to represent the lack of personal information privacy "knowledge." This pre-stage is the "information ignorance," "privacy poor" and "digitally illiterate" mode that largely typifies the existing business education curriculum. This traditional business education pre-stage, therefore, is stage one – followed sequentially by each of Bloom's original six stages. These Bloom stages correspond consistently with the five stages of the NSA's SIGINT Information Assurance classification system. The far right column labeled "get, know, use" is from the SIGINT model's short hand description of the informational focus of technology at various stages. Keeping in mind that the SIGINT system is designed for intelligent technology systems, not human learners, the terminology for each stage is understandable. Information technology "knows" at a base level when it "senses." Information technology "comprehends" when it can codify sensory impulses into "data states." Information technology processes "data" into "information" for the purpose of "applying" data to a specific situation or problem. Information technology derives "knowledge" about "information" through programmed application "analysis." Information technology systems acquire "intelligence" through parallel processing or other artificial intelligence modes of "synthesis." Above the SIGINT "intelligence" stage, a sixth stage is added from the information science literature [Haeckel and Nolan 1993; Ackoff 1989; Cleveland 1985] and labeled alternatively "action," as the use of "intelligent" technology in mobile activity [e.g., robots, smart appliances], and "wisdom," as the use of intelligent" technology for simulating omniscience [e.g., astronomy telescopes, physics atom "smashers," advanced financial market forecasting models]. This level of "action"/"wisdom" is the use of "intelligence" in abstracted "evaluation" to discern acts or values.



Combining the heuristics suggested by each stage of Bloom and SIGINT, personal information privacy directives are deducted for the three primary discipline sets of the business education curriculum. These derived directives are supported by trends in the information privacy and digital markets literature, which pertain to each of the three discipline sets. The fundamental shift in these directives from the existing direction of business education disciplines can be ascertained through a probing inquiry into the basic premise for each of the three discipline sets.

Bloom's Taxonomy, and other curriculum design rubrics [Reigeluth 1999; Provenzo, et al. 1998; Merrill 1994] informs business curriculum planners to question the relation of privacy to the foundation of disciplines. Beginning with the fundamental disciplines of economics and accounting/finance, the validity of assumed truths should be probed. Is the effect of personal information privacy central or peripheral to the theorems that define economics as a science of scarce resource decision making, when information is the primary resource and privacy the decision criterion? [Noam 1997; Laudon 1996] Do the valuation equations in accounting and asset appreciation formulae in finance accurately estimate intrinsic parabolic privacy appraisal functions for information transactions? [Kahn, et al. 2000]

Continuing with the interpersonal social science disciplines of management and marketing, theories formulated for physical social interaction should be examined for their viability in digital environments. Are virtual organization design, behavior, and planning conducive to core management theory and method when physical structures are informational architectures [Paton and Neilsen 1999; Tufte 1997] and human resources are privacy profiled digital representations [Floridi 2002; Zack 1999; Miles, et al. 1999]. Will marketing's consumer behavior constructs and brand strategy value propositions sustain competitive differentiation when not being identified, or anonymity, is consumers prime motivation and information value propositions are as easily satisfied by web-based consumer-to-consumer barter and auction – frequently conducted by intelligent digital agents [Cohen 2002; Hoffman, et al. 1999; Esmahi and Bernard 2000].

Looking at the business process disciplines, systems concepts should be assessed based on their capacity to synchronize symbiotic information flows. Do the linear productivity calculations of operations management processes pertain to digital content continuously refashioned by an ecology of information technology systems [Nardi and O'Day 1999; Cubitt 1998; Davenport 1997; Meyer and Zack 1996]. Even management information systems (MIS), which is definitively an information discipline, must ask whether the programs and network applications facilitate or merely fortify digital society intercourse, in a liberated organizational and market context consisting of autonomous human interaction? This set of privacy queries for business disciplines are likely to receive disaffirming responses, and reinforce for information privacy curricula what Rothwell and Cookson [1997] describe as the need for “comprehensive business and education program planning.”

For instance, in the *core analytical set* of the business curriculum, the Pct orients economic, accounting, and finance towards the literature of electronic markets and information currency [Moore 2002], then progressively parallels traditional analytical methods with new information privacy realities such as privacy economics and even ethics profitability – when the privacy actuaries formulated to assuage consumer risks actually become a profitable business model in digital information markets. Likewise, for the *mediating process set* of business education disciplines, information privacy oriented operations begin with data materials or information objects. These are subsequently codified for representation, processed for information product assembly, and the output is optimally allocated throughout the enterprise using knowledge management. The higher levels of information privacy operations synchronize the intelligence systems within the enterprise and marketplace, and ultimately regenerate intelligence as simulations, artificial systems, or virtual holographic information matrices. Thirdly, the personal practice set of business disciplines connect with human customers and employees as information nodes at a base level. However, recognizing the information privacy dynamics, the access is made ubiquitous [e.g., mobile, embedded, etc.] for greater choice. Continuing in the direction of enabling human information providers and consumers, customized agents enable digital identities to be created – some taking the form of specialized animated icons associated with particular digital society transactions. As digital identity is adopted a greater need for digital literacy will result to raise and upgrade the intelligence of users and their agents in the electronic marketplace. This widespread digital literacy and continuous digital society interaction will elevate the value of anonymity – as control and freedom from electronic marketplace pressure. Anonymity, for human inter-actors, becomes the embodiment of personal

information privacy in a digital society. Ultimately, consumers and employees confer loyalty and relationship upon organizations that earn their information/privacy trust.

The graduated directives for each discipline are conceptually consistent and at each level maintain the same three module symbiosis that was established at the onset in Figure 1. Therefore, the PCT affords business curriculum planners a comprehensive, yet specific, tool for engaging the logical deductions thrust upon the academy by digital society.

**Figure 2**  
**The Privacy Curriculum Taxonomy: Business Education Guidelines for the Digital Society**

	BLOOM's TAXONOMY Educational Objectives	BUSINESS EDUCATION CURRICULUM Personal Information Privacy Discipline Considerations			SIGNET Intelligence Pyramid [NSRB]	
		Core Analytical Set	Mediating Process Set	Personal Practice Set	Info. Assurance	
7	Evaluation	Ethics Profitability	Process Regeneration [learning organization]	Trust Architectures [comfort]	Wisdom/Action*	
6	Synthesis	Intelligence Portfolio	Intelligence Synchronization	Anonymity [control]	Intelligence [Applied Knowledge]	U S E
5	Analysis	Intellectual Capital	Knowledge/Process Management	Digital Literacy [competence]	Knowledge [Facts in Context]	K N O W
4	Application	Privacy Economics	Information Product Assembly	Digital Identity [character]	Information [Discrete Facts]	
3	Comprehension	Data Valuation	Digital Representation	Digital Access [choice]	Data [Bytes/States]	G E T
2	Knowledge	Information Currency	Information Objects	Information Node [connection]	Signal [Impulses/Sensors]	
1		TRADITIONAL BUSINESS EDUCATION MODE a) Information Ignorance b) Privacy Poor c) Digital Illiteracy			* Haeckel & Nolan(1993) * Ackoff (1989) * Cleveland (1985)	

**REFERENCES**

- Acquisti, A. (2004). *The Economics of Privacy*. Carnegie Mellon University, Software Engineering Institute, February 2004. 2004 <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm#new>;
- Acquisti, A.; Dingedine, R. & Syverson, P. (Fall 2003). On the economics of Anonymity. *Financial Cryptography*, Springer Verlag, LNCS, 2003.
- Agres, C.; Edberg, D. & Igbaria, M. (1998). Transformation to Virtual Societies: Forces and Issues. *The Information Society*, Volume 14, Number 2, pp.71-82.
- Aiker, P. H. (April 1998). Reverse Engineering of Data. *IBM Systems Journal*, Volume 37, Issue 2, pp.246-269.
- Allen, M. W. (2001). A Practical Method for Uncovering the Direct and Indirect Relationships Between Human Values and Consumer Purchases. *Journal of Consumer Marketing*, Volume 18, Number 2, pp.102-120.
- Benjamin, R. & Wigand, R. (1995). Electronic Markets and Virtual Chains on the Information Superhighway. *Sloan School of Management Review*, pp. 62-72.
- Bennett, C. J. & Grant, R. (1999). *Visions of Privacy: Policy Choices for the Digital Age*. University of Toronto Press, Toronto, Ontario, Canada.
- Bernard, L. (2001). *e-Business Intelligence: Turning Information into Knowledge into Profit*. New York: McGraw-Hill.
- Bibas, S. A. (1994). A Contractual Approach to Data Privacy. *Harvard Journal of Law and Public Policy*, Volume 17, Number 2, pp.591-611.

10. Bloom, B. S. & Krathwohl, D. R. (1956). *Taxonomy of Educational Objectives: The Classification of Educational Goals*. By a committee of college and university examiners. Handbook I: Cognitive Domain. New York: Longmans, Green.
11. Bontis, N. (1999). Managing Organizational Knowledge By Diagnosing Intellectual Capital: Framing and Advancing the State. *International Journal of Technology Management*, Volume 271, Chapter XVI.
12. Bowie, N. E. & Freeman, R. E., Editors (1992). *Ethics and Agency Theory: An Introduction*. New York: Oxford Press.
13. Bradley, S. P. & Nolan, R. L. (1998). *Sense and Respond: Capturing Value in the Networked Era*. Boston: Harvard Business School Press.
14. Brandeis, Judge Lewis (1928). *Olmstead v. United States*, Dissenting, 277 U.S. 438, 478.
15. Brookfield, S.D. (1988). *Developing Critical Thinkers*. San Francisco, CA: Jossey-Bass Publishers.
16. Brown, J. S. & Duguid, P. (2000). *The Social Life of Information*. Boston: Harvard Business School Press.
17. Buchholz, R. A. & S. B. Rosenthal (Winter 2002). Internet Privacy: Individual Rights and the Common Good. *SAM Advanced Management Journal*, Volume 67, Number 1.
18. Burge, L. (1988). Beyond Andragogy: Some Explorations for Distance Learning Design. *Journal of Distance Education*, Volume 3, Number 1, pp. 5–23.
19. Bush, V.; Ferrell, L.; Bush, A. & Ferrell, O.C. (Fall 2003). Investigating the Relations Between Corporate Values and Practices of Marketing Organizations and Internet Ethics, *Journal of Marketing Management*, Volume 13, Number 2.
20. Caudill, E. M. & Murphy, P. E. (Spring 2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing*, Volume 19, Number 3, pp.7-19.
21. Christopher, A. (May 26, 2003). The Human Firewall, *Network World Fusion*.
22. [<http://www.nwfusion.com/research/2003/0526human.html> ]
23. Cohen, A. (2002). *The Perfect Store – Inside eBay*. Boston: Little Brown & Company.
24. Cronin, M. J. (2000), *Unchained Value: The New Logic of Digital Business*. Boston: Harvard Business School Press.
25. Cubitt, S. (1998). *Digital Aesthetics*. London: Sage
26. Davenport, T. H. (1993). *Process Innovation: Reengineering Work through Information Technology*. Harvard Business School Press, 1993
27. Davenport, T. H and Prusak, L. (1997). *Information Ecology: Mastering the Information and Knowledge Environment*. New York: Oxford University Press.
28. Davidow, W. H. (1992). *The Virtual Corporation: Structuring and Revitalizing the Corporation for the 21st Century*. New York: Harper-Business 1992.
29. Desman, M. B. (2001). *Building an Information Security Awareness Program*. New York: Auerbach Publications.
30. Drucker, P. F. (1954), *The Practice of Management*. New York: Harper.
31. *E-Business Ethics Center, of the Center for Business Ethics and Social Issues*. Colorado State University. <http://www.e-businessethics.com/>
32. Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review, *Academy of Management Review*, Volume 14, Number 1, pp.57-74.
33. Esmahi, L. & Bernard, J. C. (January 2000). MIAMAP: A Virtual Marketplace for Intelligent Agents. Proceedings of the 33<sup>rd</sup> HICSS. Maui, HI.
34. Etzioni, A. (2000). *The Limits of Privacy*. New York: Perseus Books.
35. Evans, P. & Wurster, T. S. (1999). *Blown to Bits: How the New Economics of Information Transforms Strategy*. Boston: Harvard Business School Press.
36. Floridi, L. (December 2002). On the Intrinsic Value of Information Objects and the Infosphere. *Ethics and Information Technology*, Volume 4, Number 4, pp. 287 – 304.
37. Floridi, L. (1999), Information Ethics: On the Philosophical Foundation of Computer Ethics. *Ethics and Information Technology*, Volume 1, Number 1, pp. 33-52.
38. Franzak, F.; Pitta, D. & Fritsche, S. (2001). Online Relationships and the Consumers' Right to Privacy. *Journal of Consumer Marketing*, Volume 18, Number 7, pp. 631-641.
39. Friedman, D. (2000). Privacy and Technology. *Social Philosophy & Policy* Volume 17, pp. 186-212.
40. FTC (May 2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace*. Federal Trade Commission Report to Congress.
41. Gilhooly, R. (2002). The Social Approaches to Enforcing Information Security. *SANS Institute*.
42. Gilbert, J. (2006). A Matter of Trust. in *Marketing Ethics: Cases and Readings*, editors P. E. Murphy and G. R. Laczniak, Upper Saddle River, NJ: Pearson Prentice-Hall, p.73 – 77.

42. Gilster, P. (1997). *Digital Literacy*. New York: John Wiley and Sons.
43. Goodwin, C. (1991). Privacy: Recognition of a Consumer Right. *Journal of Public Policy and Marketing*, Volume 10, Number 2, pp.149-166.
44. Graham, G. (1999). *The Internet: A Philosophical Inquiry*. London and New York: Routledge.
45. Haberman, S.; Day, C.; Fogarty, D.; Khorasanee, M. Z.; McWhirter, M.; Nash, N.; Ngwira, B.;
46. Hamell, J. & Prashantham, S. (2001), Internet Supported Customer Relationship Management: A Key Opportunity for the Twenty-First Century. *International Marketing Review*, Volume 18, Number 1, pp.102-104.
47. Health Insurance Portability and Accountability Act of 1996. August 21, 1996. P.L. 104-191. 104<sup>th</sup> United States Congress.
48. Hoffman, D. L. & Novak T. P. (2005), A Conceptual Framework for Considering Web-Based Business Models and Potential Revenue Streams. *International Journal Marketing Education*, Volume 1, Issue 1, pp.7-24.
49. Hoffman, D. W. (August 2002). Internet-Based Learning in Higher Education. *Teledirections*.
50. Hoffman, D. L. & Novak, T. P. (July 1996). Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations. *Journal of Marketing*, Volume 60, pp.50-68.
51. Jevons, C. & Gabbott, M. (2000). Trust, Brand Equity and Brand Reality in Internet Business Relationships: An Interdisciplinary Approach. *Journal of Marketing Management*, Volume 16, Number 6, pp. 619 – 634.
52. Kahn, C. M.; McAndrews, J. & Roberds, W. (November 2000). A Theory of Transactions Privacy. Federal Reserve Bank of Atlanta, Working Paper 2000-22,
53. Kanigel, R. (1997). *The One Best Way: Frederick Winslow Taylor and the Enigma of Efficiency*. New York: Penguin - Viking Press.
54. Kearsley, G. (2000). *Online Education: Learning and Teaching in Cyberspace*. Belmont, CA: Wadsworth.
55. Knowles, M. S. (1980). *The Modern Practice of Adult Education: From Pedagogy to Andragogy*. New York: Cambridge Books.
56. Knowles, M. S. (1984). *Andragogy in Action*. San Francisco: Jossey-Bass.
57. Koepsell, D. R. (June 2000). An Emerging Ontology of Jurisdiction in Cyberspace. *Ethics and Information Technology*, Volume 2, Number 2, pp. 99-104.
58. Langford, D., Editor (2000). *Internet Ethics*. London: Macmillan.
59. Laudon, K. (1996). Markets and privacy. *Communications of the ACM*, Volume 39, Number 9.
60. Leiberman, J. K. (1978). *Privacy and the Law*. New York: Lothrop, Lee, and Shepard Company.
61. Liao, T. T. (Ed.). (1996). *Advanced Educational Technology: Research Issues and Future Potential (NATO ASI series. series F, computer and systems sciences, no 145)*. New York: Springer. Verlag.
62. Liautaud, B. (2001). *e-Business Intelligence: Turning Information into Knowledge into Profit*. New York: McGraw-Hill.
63. Malone, T. W.; Yates, J. & Benjamin, R. I. (May-June 1989). The Logic of Electronic Markets. *Harvard Business Review*. 166-172.
64. Marquardt, M. J. & Kearsley, G. (1999). *Technology-Based Learning*. Boca Raton, FL: St. Lucie Press.
65. Martin, L. E. (1997). *The Challenge of Internet Literacy: The Instruction-Web Convergence*. Haworth Press.
66. Meyer, M. H. & Zack, M. H. (Spring 1996). The Design and Development of Information Products. *Sloan Management Review*, Volume 37, pp. 43-59.
67. Michelfelder, D. P. (June 2001). The Moral Value of Information Privacy in Cyberspace. *Ethics and Information Technology*. Volume 3, Number 2, pp. 129-135.
68. Miles, G.E.; Howes, A. & Davies, A. (1999). A Framework for Understanding Human Factors in Web-Based Electronic Commerce. *International Journal of Human-Computer Studies*, Volume 52, pp. 131-163.
69. Miyazaki, A. D. & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, Volume 36, Number 1, pp.28-50.
70. Moore, G. A. (2002). *Living on the Fault Line: Managing for Shareholder Value in any Economy*. New York: Harper-Collins.
71. Nardi, B. A. & O'Day, V. L. (1999). *Information ecologies: Using technology with heart*. Cambridge, MA: MIT Press.
72. National Standards Registration Board, LLC (accessed August 1, 2005) Information Assurance Compliance Principles <http://www.nsrp.us/PrinciplesofInformationAssurance.html>
73. Negroponce, N. (2001). *Being Digital*. New York: Vintage.
74. Noam, E. (1997). Privacy and Self-Regulation: Markets for Electronic Privacy. in *Privacy and Self-Regulation in the Information Age*. U.S. Department of Commerce.
75. Nonaka, I. & Takeuchi, H. (1995). *The Knowledge-Creating Company*. New York: Oxford University Press.

76. Oravec, J. (1999). Integrating Privacy Studies into Teacher Education Curricula. *Journal of Information Technology for Teacher Education*, Volume 8, Number 9, pp.55-70.
77. Palloff, R. M. & Pratt, K. (1999). *Building Learning Communities in Cyberspace: Effective Strategies for the Online Classroom*. San Francisco, CA: Jossey-Bass.
78. Paton, R. & Neilson, I. (1999). *Visual Representations and Interpretations*. New York: Springer Verlag.
79. Paul, E. F.; Miller Jr., F. D. & Paul, J. (2000). *The Right to Privacy*, edited by Cambridge University Press.
80. Peterson, R. A. & Ferrell, O. C., Editors. (2005). *Business Ethics: New Challenges for Business Schools and Corporate Leaders*. New York: M.E. Sharpe, Inc.
81. Pine, B. J. (1992). *Mass Customization: The New Frontier in Business Competition*. Boston: Harvard Business School Publishing.
82. Porter M.E. & Millar V.E. (1985). How Information Gives You Competitive Advantage. *Harvard Business Review*, Volume 63, Issue 4, pp. 149-160
83. Posner, R. (May/June 1978). An economic theory of privacy. *Regulation*, pp. 19-26.
84. Provenzo, E. F.; Brett, A. & McCloskey, G. N. (1998). *Computers, Curriculum, and Cultural Change: An Introduction for Teachers*. Hillsdale, NJ: Lawrence Erlbaum Associates.
85. Raul, A. C. (2002). *Privacy and the Digital State*. Boston: Kluwer Academic Publishers.
86. Rayport, J. F. & Sviokla, J. J. (November-December 1995). Exploiting the Virtual Value Chain, *Harvard Business Review*, pp. 75-85.
87. Reichheld, F. F. & Shefter, P. (July/August 2000), E-Loyalty: Your Secret Weapon on the Web. *Harvard Business Review*, 105-113.
88. Reigeluth, C. (1999). *Instructional Design: Theories and Models*. (Vol. 2). Hillsdale, NJ: Erlbaum Associates.
89. Rosenberg, M. J. (2001). *E-Learning: Strategies for Delivering Knowledge in the Digital Age*. New York: McGraw-Hill.
90. Rothwell, W. J. & Cookson, P. S. (1997). *Beyond Instruction: Comprehensive Program Planning for Business and Education*. San Francisco, CA: Jossey-Bass.
91. Rust, R. T.; Kannan, P. K., and Peng, Na (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, Volume 30, Number 4, pp.455-464.
92. Rykere, R., et al. (Summer 2002). Online Privacy Policies: An Assessment. *Journal of Computer Information Systems*.
93. *Sarbanes-Oxley Act of 2002*. July 30, 2002. 107<sup>th</sup> United States Congress. 107 P.L. 204, § 1, 116 Stat. 745.
94. Senge, P. (1990). *The Fifth Discipline*. New York: Doubleday.
95. Serva, M. A., Fuller, M. A. & Mayer, R. C. (2001). The Evolution of Trust Between Interdependent Teams: Risk Taking and Reciprocal Trust over Time. Paper Presented at the Technology Policy Group Conference.
96. Severson, R. J. (1997). *The Principles of Information Ethics*. Armonk, NY: M.E. Sharpe.
97. Seybold, P. B. (1998). *Customers.Com: How to Create a Profitable Business Strategy for the Internet and Beyond*. New York: Times Business.
98. Sirdeshmukh, D.; Singh, J. & Sabol, B. (January 2002). Consumer Trust, Value, and Loyalty in Relational Exchanges. *Journal of Marketing*, Volume 66, pp.15-37.
99. Shaw, M. J.; Subramaniam, C.; Tan, G. W. & Welge, M. E. (2001). Knowledge Management and Data Mining for Marketers. *Decision Support Systems*, Volume 31, Number 1, pp. 127 – 139.
100. SIGINT (Accessed August 1, 2005). The Information Assurance Classification for Signal Intelligence. *United States National Security Agency* <http://www.nsa.gov/sigint/>
101. Simon, H. (1997). *Administrative Behavior: A Study of the Decision Process in Administrative Organizations* 4<sup>th</sup> edition. New York: The Free Press.
102. Slater, S. F. & Narver, J. C. (2000). Intelligence Generation and Superior Customer Value. *Journal of the Academy of Marketing Science*, Volume 28, Number 1, pp.120-127.
103. Smith, J. H.; Milberg, S. J. & Burke, S. J. (June 1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, Volume 20, pp. 167-196.
104. Spinello, R. A. & Tavani, H. T. (June 2001). The Internet, Ethical Values, and Conceptual Frameworks: An Introduction in CyberEthics. *Computers and Society*.
105. Stead, B. A. & Gilbert, J. (November 2001), Ethical Issues in Electronic Commerce. *Journal of Business Ethics*, Number Volume 34.
106. Stigler, G. J. (1980). An introduction to privacy in economics and politics. *Journal of Legal Studies*, Volume 9, pp.623-644.

107. Sunder, S.; Jamal, K. & Maier, M. S. (May 2003). Privacy in e-Commerce: Development of Reporting Standards, Disclosure and Assurance Services in an Unregulated Market. *Journal of Accounting Research*, Volume 41, Number 2, pp.285-309.
108. Tapscott, D. (2000). *Digital Capital: Harnessing the Power of Digital Webs*. Boston: Harvard School of Business Press.
109. Tapscott, D. (1997). *Digital Economy: Promise and Peril in the Age of Network Intelligence*. New York: McGraw-Hill.
110. Tavani, H. T. (1999). Information Privacy, Data Mining, and the Internet. *Ethics and Information Technology*, Volume 1, Number 2, pp. 137 – 145.
111. Taylor, F. W. (1998). *The Principles of Scientific Management*. New York: Dover Press.
112. *The Fair and Accurate Credit Transaction Act of 2003 (FACTA)*. HR 2622. December 4, 2003. Pub. L. 109<sup>th</sup> United States Congress. 108-159, 111 Stat. 1952.
113. *The Family Education Rights and Privacy Act (FERPA) of 2002*. 20<sup>th</sup> United States Congress, 1232g, 34 CFR Part 99.
114. Thomas, T. A. (October 12, 1998). Knowledge, the Appreciating Commodity. *Fortune*, pp.199-200.
115. Tiffin, J. & Rajasingham, L. (1995). *In Search of the Virtual Class: Education in an Information Society*. London: Routledge.
116. Tufte, E. R. (1997). *Visual Explanations: Images and Quantities, Evidence and Narrative*. Norcross, GA: Graphics Press.
117. Tufte, E. R. (1992). *The Visual Display of Quantitative Information*. Graphics Press. -
118. Turban, E.; King, D.; Lee, J. K. & Viehland, D. (2003). *Electronic Commerce 2004: A Managerial Perspective*. Upper Saddle River, NJ: Prentice Hall
119. Tyner, K. (1998). *Literacy in a Digital World: Teaching and Learning in the Age of Information*. Hillsdale, NJ: Lawrence Erlbaum Associates.
120. United States National Security Agency website [www.nsa.gov](http://www.nsa.gov)
121. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. October 24, 2001. HR 3162. 107<sup>th</sup> United States Congress.
122. Urban, G. L., Sultan, F. & Qualls, W. J. (2000). Placing Trust at the Center of Your Internet Strategy. *MIT Sloan Management Review*, Volume 42, Number 1, pp. 39-48.
123. Urbany, J. E. (September 1986). An Experimental Examination of the Economics of Information. *Journal of Consumer Research*, Volume 13, pp.257-271.
124. Volkman, R. (2002), Privacy as Life, Liberty, Property. *Ethics and Information Technology*, Volume 5, Number 4, pp.199-210.
125. Wenger, E.; McDermott, R. & Snyder, W. M. (2002). *Cultivating Communities of Practice: A Guide to Managing Knowledge*. Boston: Harvard Business School Press.
126. Westin, A. F. (1967). *Privacy and Freedom, Volume 7*. New York: Atheneum Press.
127. Westin, A. F. (November 1999). Personalized Marketing and Privacy on the Net: What Consumers Want. *Privacy and American Business*, Volume 11.
128. Wigand, R. (November 2003). Facing the Music: Value-Driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products. *In Digital Rights Management: Technological, Economic, Legal and Political Aspects*. E. Becker, W. Buhse, D. Günnewig, et al. Editors. Springer, Lecture Notes in Computer Science 2770, pp. 250 – 270.
129. Wolfenbarger, M. & Gilly, M. G. (2001). Shopping Online for Freedom, Control, and Fun. *California Management Review*, Volume 43, Number 2, pp. 34-55.
130. Wright, I. D. & Yakoubov, Y. (2003). A Stochastic Approach to Risk Management and Decision Making in Defined Benefit Pension Schemes. *British Actuarial Journal*, Volume 9, Number 3, pp. 493-586.
131. Young, M. A. & Sauer, P. L. (1996). Organizational Learning and Online Consumer Information Services. *Journal of Consumer Marketing*, Volume 13, Number 5, pp. 35-46.
132. Zack, M. H. (Summer 1999). Managing Codified Knowledge. *Sloan Management Review*, Volume 40, pp. 45-58.