Final Exam – Summer 2004

Prepared for
Dr. Steven D. Zink, Ph.D.
2004 Winter Institute
Faculty in Doctoral Program
Nova Southeastern University

Prepared by
Derek J. Sedlack
Doctoral Student, Nova Southeastern University
School of Computer and Information Sciences

December 5, 2004

Task 1

1. As has been noted, the roots of U.S. information policy can often be traced to the U.S. Constitution. Look through the Constitution; URL is noted in the syllabus. In an essay, identify relevant passages in the Constitution that can be extrapolated to relate to contemporary policy issues covered in the class or in the coursework, i.e. privacy, right to information access. Explain the relationships to modern policies.

A number of sources (Zink, 2004; Hammitt, 2002; Tapscott, 1996) state that rights to privacy are explicitly granted in the constitution, or are directly derived from said document when no such privacies are denoted. Two overt references and one directly noted amendment provide oversight and guidance that has helped forge 200 years of fairly domestic tranquility, but more specific language should be added to provide law enforcement provisions to protect Americans' privacy during this information age. Article 1 (legislative powers) provides this possible indirect reference to privacy:

> *Section. 6.*
> *The Senators and Representatives shall receive a Compensation for their Services, to be ascertained by Law, and paid out of the Treasury of the United States. They shall in all Cases, except Treason, Felony and Breach of the Peace, be privileged from Arrest during their Attendance at the Session of their respective Houses, and in going to and returning from the same; and for any Speech or Debate in either House, they shall not be questioned in any other Place.*

Framers believed that policy makers should be immune to certain aspects of the law, specifically questioning, during session. I believe that the British invasion afforded the belief that questioning a legislator during session could compromise national security and that the most protection available over the law is given. There have been a number of laws affecting the general public that deal with the dissemination and access to information, perhaps relating to security as suggested by Zink (2004).

> *Article IV*
> *Section. 4.*
> *The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence.*

Article IV, section 4 provides citizens protection against invasion and domestic violence. It would be possible to construe modern identity theft as a domestic violence and therefore a number of Acts have been provided to protect the public:

Freedom of Information Act of 1966 – gives people the right to inspect information about themselves held in government files; also allows other individuals and organizations the right to request disclosure of government records based on the public's right to know.
Driver's Privacy Protection Act of 1994 – state motor vehicle department access is limited to those with legitimate business purposes, but anyone who wants to buy all of the records and resell them has a legitimate purpose. The driver is allowed to prevent disclosure of information to marketers and the general public, but an enterprising businessperson easily defeats this measure.
FCRA (1970) – credit investigating and report industry regulations. People have the right to inspect credit history ONLY if they have been denied credit. Also allows the correcting of information.
Computer Matching and Privacy Protection Act of 1988 – regulates matching of computerized files in possession of different government agencies.
FERPA (1974) – locks down school and college student information to the students and parents. Allows them to challenge and change information as well.
Right to Financial Privacy Act (1978) – regulates the financial industry's use of personal financial records; establishes procedures that federal agencies must follow to gain access to such records.
Cable Communications Policy Act of 1984 – regulates the cable industry's collection and disclosure of information concerning subscribers.
Privacy Act (1974) – regulates the federal government's collection, use, and disclosure of data collected by federal agencies. Allows individuals the right to inspect records and correct errors.

Amendment IV secures some individual privacy from illegal search and seizure. This is probably the single most relatable entrance in the Constitution with personal privacy and information security, but 200 years passed before it was interpreted in such a manner.

Amendment IV
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Privacy Protection act of 1980 prohibits government agents from conducting unannounced searches of press offices and files if no one in the office is suspected of committing a crime. This Act is a direct result of applying Amendment IV to the modern availabilities of electronic commerce and communications. The Electronic Communications and Privacy Act of 1986, fines and jail time for those who access, intercept, or disclose private e-mail communications of others, and the Computer Security Act of 1987, security infringement of computer-based files is illegal, are also derived from the liberty provided by the 4th amendment.

Americans have entered into an age of instant availability, unlimited access, and relentless cross-referencing of information that could either enables tremendous growth, or provide methods for criminal activity. It appears that a Constitutional amendment securing the American publics right

to the privacy of financial, personal, and health information is required since the laws enacted are doing little to inhibit identity theft. Tapscott (1996) discusses the implications of simply accessing hotel information and some potential solutions: government guidelines, private self-policing, nothing, but only a paradigm shift in the way citizens think about information will allow the real protection and security America needs.

2. The basis for the U.S. government's national cyber-security policy can be found in a 2003 publication entitled the National Strategy to Secure Cyberspace [www.securecyberspace.gov]. Read the executive summary as well as those sections that most closely pertain to your area of work. With the knowledge that you now have and additional commentary available about this report, prepare an evaluation of the report's suggestions in your area of expertise (I prefer in-depth analysis of a small area rather than a cursory evaluation of broader area). Be sure to comment on the proposed timetable, scope, and incident reporting outlined in the federal strategy.

The policy is quite expansive containing sections on key asset identification, cross-sector corroboration and communications, critical infrastructures, and nationally established policies and guidelines, but fails to include specific responsibilities at the national, state, and private levels or any proposed timetable. The policy emphasizes that this policy requires a national effort that includes not simply federal guidelines and assistance, but private sector cooperation and private citizen enforcement. This is no panacea and a successful implementation of this policy requires even the most innocuous home computer to be protected against illicit intentions. The best method of cybersecurity can only be achieved through training and structured learning. The more informed and prepared our tertiary components are and distinct open methods of communication exist, the more possible the ostentatious plans proposed in this policy become.

The training portion of the policy lists four major actions and initiatives for awareness, education, and training:

1. Promote a comprehensive national awareness program to empower all Americans— businesses, the general workforce, and the general population— to secure their own parts of cyberspace

2. Foster adequate training and education programs to support the Nation's cybersecurity needs

3. Increase the efficiency of existing federal cybersecurity training programs

4. Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications

"A lack of cybersecurity awareness" is cited as the major reason that vulnerabilities exist in the current infrastructure and the list of those responsible is extensive and inclusive. Just as Ficarrotta (2004) noted that a lack of licensure for computer engineers might be the cause for poorly written programs; priority III cites a lack of training and multi-level certification responsible for cyber vulnerabilities. While it is vital that federal forces cooperate with private industry, the training of average citizens connected to the Internet through high-speed connections may be the single-most threatening security risk and the most difficult to correct. If our professionals are not properly equipped to secure our cyber-infrastructure, as the Act mentions, aggressive training programs must be put in place quickly for laymen.

No document specifically relating to timetables was listed on the Whitehouse web site, but the initiatives required for securing a number of vital locations and critical infrastructure provided detailed methods for how security should proceed and why these assets required safeguarding. The actions and recommendations summery listed nine key measures of education and training:

A/R 3-1: DHS, working in coordination with appropriate federal, state, and local entities and private sector organizations, will facilitate a comprehensive awareness campaign including audience-specific awareness materials, expansion of the StaySafeOnline campaign, and development of awards programs for those in industry making significant contributions to security.

A/R 3-2: DHS, in coordination with the Department of Education, will encourage and support, where appropriate subject to budget considerations, state, local, and private organizations in the development of programs and guidelines for primary and secondary school students in cybersecurity.

A/R 3-3: Home users and small businesses can help the Nation secure cyberspace by securing their own connections to it. Installing firewall software and updating it regularly, maintaining current antivirus software, and regularly updating operating systems and major applications with security enhancements are actions that individuals and enterprise operators can take to help secure cyberspace. To facilitate such actions, DHS will create a public-private task force of private companies, organizations, and consumer users groups to identify ways that providers of information technology products and services, and other organizations can make it easier for home users and small businesses to secure their systems.

A/R 3-4: Large enterprises are encouraged to evaluate the security of their networks that impact the security of the Nation's critical infrastructures. Such evaluations might include: (1) conducting audits to ensure effectiveness and use of best practices; (2) developing continuity plans which consider offsite staff and equipment; and, (3) participating in industry wide information sharing and best practices dissemination.

A/R 3-5: Colleges and universities are encouraged to secure their cyber systems by establishing some or all of the following as appropriate: (1) one or more ISACs to deal with cyber attacks and vulnerabilities; (2) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (3) one or more sets of best practices for IT security; and, (4) model user awareness programs and materials.

A/R 3-6: A public-private partnership should continue work in helping to secure the Nation's cyber infrastructure through participation in, as appropriate and feasible, a technology and R&D gap analysis to provide input into the federal cybersecurity research agenda, coordination on the conduct of associated research, and the development and dissemination of best practices for cybersecurity.

A/R 3-7: DHS will implement and encourage the establishment of programs to advance the training of cybersecurity professionals in the United States, including coordination with NSF, OPM, and NSA, to identify ways to leverage the existing Cyber Corps Scholarship for Service program as well as the various graduate, postdoctoral, senior researcher, and faculty development fellowship and traineeship programs created by the Cyber Security Research and Development Act, to address these important training and education workforce issues.

A/R 3-8: DHS, in coordination with other agencies with cybersecurity training expertise, will develop a coordination mechanism linking federal cybersecurity and computer forensics training programs.

A/R 3-9: DHS will encourage efforts that are needed to build foundations for the development of security certification programs that will be broadly accepted by the

public and private sectors. DHS and other federal agencies can aid these efforts by effectively articulating the needs of the Federal IT security community.

Creating an awards program would definitely provide an incentive of recognition and prestige far beyond money to those in the private industry. This might allow some cohesion in the industry that is the overlaying theme throughout the Cyberspace strategy. Training and education must begin at an early level if a broad impact, proposed in the document, is a possibility. The document also states that computers are commonly used as hosts for cyber attacks because of a lack of training and basic security methods. As high-speed Internet access proliferates the suburbs, more and more computers should be subject to hostile occupation and lead to even greater attacks. The report also notes that high levels of coordination are required for massive cyber attacks and this is probably the reason that one has not occurred, but if more computers can easily be harvested over high-speed connections, an increase in possibility raises daily. Children are beginning to use the Internet at younger ages – Disney has developed a multi-user environment for children under 5 (Disney, 2004) – and must be educated in computer etiquette and security. The document stresses communication and community sharing that is a growing belief among scholars (Scalet, 2002; O'Neil & Senf, 2003). Sharing information regarding illicit activities between private corporations will help develop better methods of security and more prosecutions should provide some level of deterrence.

The cross-functional interaction and coordination these steps require presents a steep challenge of interoperability, timeliness, and trust. Directly after the attacks of 911 it seemed possible to ask the country to do anything; this measure might have been attainable at that time. No implication of anti-patriotism or isolationism is intended, only the reality of asking companies to share critical information for the sake of the country, even corporate partners may require some coercion to provide details of critical network infrastructure. The plan set forth in the Nation Strategy to Secure Cyberspace is truly vital to our nations ability to continue to function economically in the face of increasingly complex terrorism and it seems certain that electronic attacks will transpire in the near future, but a serious paradigm shift will have to take place across the nations private sector of the security provided by this Act can be fulfilled.

3. Choose any book or longer article you read for the class (must be an assigned or recommended reading) and provide a review of it. The review should be approximately seven or eight paragraphs (1,500 words in length). The review should embed the following elements (but the following should not be headings in the review):

Ficarrotta, J. C. (2004). Software engineering as a profession: A moral case for licensure. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 12, pp. 204-222. Hershey, PA: Information Science Publishing.

Understanding why serious issues like a rising moon nearly being fired on by a U.S. rocket arise because of software failures leads to introspection into the software industry and the engineers that man the gates of this centuries most infiltrating technology. Ficarrotta provides arguments for licensing the software engineering industry, either personnel or organizational, much in the same way and reasoning that other professions have embarked on such morally required pledges. Ficarrotta contrasts a number of professions that support and resist the licensure of software engineering.

Current certifications and accredited degrees do not provide the professionalism or morality required by the overwhelming entrenchment of software in America's most critical systems relating to security and infrastructure. The author provides a theme of support for licensure including solid arguments against the ACM task force that voted strongly to resist licensing the profession.

It is easy to agree with Ficarrotta while using products from any aspect of the software industry, specifically Microsoft products that require constant "critical security patches" and have become synonymous with "blue screens of death". There are five compelling comparisons with other professionals: training, autonomous regulation, ethical standards, monopolistic qualifications, and societal impact. These cohesively form a very compelling stand supporting licensure and concise reasons for developing a more accountable software engineering community.

Software engineers, like lawyers, doctors, or architects are formally trained with exposure to accepted theories and models and are expected to practice a strong sense of professional judgment. It would be negligent to allow another industry to regulate medicine or similar professions, and since software can claim that same liability, it should be self-regulated. In subscribing to a cryptic vocation, the software industry must also look at strategic decisions that require a formal code of ethics. Designers provide a service that has become vital to national industries like public safety, transportation, banking, and defense that demands the highest level of ethics, arguably more important than medicine. Finally, software engineers require a skill set that has a national, if not global impact where macroeconomic mishaps potentially cost billions of dollars and loss of life. This alone appears to be the major indicator, according to the author, that lends software engineering to professional licensure.

The level of significance that should be placed on software engineering is similar to a cousin in the industry, information systems/science. This policy class has provided a single point

of focus to my understanding: the information industry is weakly regulated, if at all, and requires a level of ethical value and commitment that should be unparalleled, but currently is not. The number of troops a general can commit to physical harm is limited to the number enlisted, but information collectors are responsible for the well being on their lists that easily number in the millions. The consolidation of information becomes of great concern when sales to tertiary, unethical sources are not subject to inspection or when the systems that information resides on was designed without consideration of national import. The ACM task force decided on very weak arguments that the software industry should not pursue a professional licensing paradigm: professional licenses would be difficult to pass and would cause strain on an already short workforce and subjecting software engineering to malpractice suits would further damage the fragile industry. The Framers of the Constitution provided for a more free country, but also ensured that checks and balances existed between the governmental bodies so that security, at the cost to freedom, would provide a more perfect union. The ACM seems more concerned with maintaining their subscription level than designing a practice of computing professionalism that would advance the industry toward a more respected, strategic industry, like medicine or architecture. The compromise of losing software engineers for better performing, less buggy software seems well worth the tight constraints the industry might feel for several years. The exposure of the Y2K flaw, known for decades, only provides additional fuel for licensing the software industry as a true engineering practice.

The author draws great comparisons to corroborating industries and leverages a task force report created by a well-respected engineering association. The author's position begins with a solid position of how large the impact of software engineering, positive and negative, is on society and forges this ethical position into a solid argument. The author also looks at the possibility of inclusion into existing professional licenses and also provides a basis for exclusion. The level of neutrality provided by the author, while slanted toward licensure, allows the reader to develop a view of the industry that draws on the real potential impact contributed to by even the smallest software company. Providing some advances in medicine, architecture, or other professions would have solidified Ficarrotta's belief in professionally certifying or licensing the software engineers in America. Additionally, I was interested in how many licensed professionals have their license revoked due to negligence and if it was a result of a lawsuit, or simply a peer-review process. With a growing percentage of American software being engineering outside our borders, do other countries have software engineering licenses and are they effective? Overall I found the paper to be compelling and thought provoking.

I have often thought that self-taught programmers lack the structure and breadth of knowledge required in the industry, especially with the global implications that the smallest company can have both economically and medically. The first horrific example I thought of related to research conducted on emerging wireless devices for Dr. Metcalf at Nova Southeastern. Organic material capable of carrying fiber optic signals has been woven into a shirt that laser tag players wear, creating a much more flexible, enjoyable performance (Sedlack, 2003). The shirt is capable of monitoring blood pressure, heart rate, and other life threatening situations. Imagine now that this shirt is worn by our troops during a conflict and is now capable of helping guide fire away from friendly troops because the shirt is communicating with the weapon. But, our army of over one million highly trained individuals is entirely wiped out in

several minutes because a poor programmer developed the software with a backdoor that allowed a foreign power to hack into and control the software. Imagine also at the same time that our mechanized division and entire air force grounded because of small glitches that are appearing at precisely the wrong time.

I don't think this doomsday scenario is unlikely considering the level of outsourcing taking place in the software industry to countries that are merely friendly to the United States. Even allies like England, which have died with us, should be carefully controlled concerning software development and integration. Our ability to innovate and develop complex solutions to combat difficult problems only compound the necessity to license and regulate the software industry, provide a method of strategic instruction, and ensure that solid methods and procedures are continuously developed by leaders in the industry. The compromise for security must stifle some creativity, but allowing the industry to continue growing uncontrolled with potentially explosive growth in the near future will only contribute to catastrophic failures and massive loss of life.

Bibliography

Cook, J. S., & Cook, L. L. (2004). Compliance with data management laws. *Social, Ethical and Policy Implications of Information Technology*. In L. L. Brennan & V. E. Johnson, chapter 15, 251-273. Hershey, PA: Information Science Publishing.

Disney. (2004). Toontown. Retrieved on November 3, 2004 from the World Wide Web at http://play.toontown.com/test/browserTest.php?r=437762

Federal Trade Commission (FTC). (September, 2003). FTC releases survey of identity theft in U.S. 27.3 million victims in past 5 Years, billions in losses for businesses and consumers. *Federal Trade Commission for the Consumer*. Retrieved from the World Wide Web on October 12, 2004 from http://www.ftc.gov/opa/2003/09/idtheft.htm

Ficarrotta, J. C. (2004). Software engineering as a profession: A moral case for licensure. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 12, pp. 204-222. Hershey, PA: Information Science Publishing.

Garfinkel. S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. Cambridge, MA: O'Reilly and Associates.

Gaudin, S. (1999, December 27). The perils of privacy [risks of not developing policy]. *Network World*, 81-84.

Hammitt, H. (1997, November). Privacy trumps access, and it ain't cheap. *Government Technology,* 18.

Hammitt, H. (1998, June). A constitutional right of informational privacy. *Government Technology,* 22.

Krawiec, K. D. (2003). Cosmetic compliance and the failure of negotiated governance. *Washington University Law Quarterly, 81*, 487-544.

O'Neil, M. & Senf, D. (2003a). Strategies to manage the spam menace: part 1. CIO, Analyst Corner. Retrieved on July 12, 2004 from the World Wide Web at http://www2.cio.com/analyst/report1746.html

O'Neil, M. & Senf, D. (2003b). Strategies to manage the spam menace: part 2. CIO, Analyst Corner. Retrieved on July 12, 2004 from the World Wide Web at http://www2.cio.com/analyst/report1840.html

Rosen, J. (2001, December). Privacy, reconsidered. *CIO Insight*

Scalet, S. D. (2002, June 15). They want you for a safer infrastructure. CIO. Retrieved on July 12, 2004 from the World Wide Web at http://www.cio.com/archive/061502/safer_content.html

Sedlack, D. (2003). Wireless Technology Trends. Retrieved on November 2, 2004 from the World Wide Web at http://www.scis.nova.edu/~sedlack/691/Assignment%204/Wireless%20Technology%20Trends.html

Tapscott, D. (1996). The digital economy: promise of peril in the age of networked intelligence. New York, New York: McGraw-Hill.

Zink, S. D. (2004). Information policy, DISS 770. *Graduate School of Computer and Information Sciences Summer 2004 Doctorate Lectures*.