open.michigan

Author(s): Don M. Blumenthal, 2010

Data Security and Privacy:
Legal, Policy, and Enterprise Issues

Schedule: Friday, 8:30-11:30 am
Location: 412 West Hall
Credits: 3
Prerequisite:None

Instructor: Don M. Blumenthal, Adjunct Professor, School of Information

Course Description

As data collection and information networks expand (and stories of security breaches and the misuse of personal information abound), data security and privacy issues are increasingly central parts of the information policy landscape. Legislators, regulators, businesses, and other institutions of all kinds are under increasing pressure to draft and implement effective laws, regulations, and security and privacy programs under rapidly changing technological, business, and legal conditions. A strong need is arising for individuals with the training and skills to work in this unsettled and evolving environment.

This course will examine: 1) security issues related to the safeguarding of sensitive personal and corporate information against inadvertent disclosure; 2) policy and societal questions concerning the value of security and privacy regulations, the real world effects of data breaches on individuals and businesses, and the balancing of interests among individuals, government, and enterprises; 3) current and proposed laws and regulations that govern information security and privacy; 4) private sector regulatory efforts and self-help measures; 5) emerging technologies that may affect security and privacy concerns; and 6) issues related to the development of enterprise data security programs, policies, and procedures that take into account the requirements of all relevant constituencies; *e.g.,* technical, business, and legal.

This course is intended for students and professionals in information policy, public policy, law, business, computer science, and information science who have an interest in work or research in security and privacy fields, or in support of those fields. It also will be relevant to individuals with interests in other fields in

which traditional responsibilities may have new security considerations*; e.g.,* programming.

The course will include individual reading and writing assignments, class discussion, case studies, and a group assignment. Students will have some latitude to tailor the assignments to their skills and interests.

Course Objectives

The growth of importance of information security and privacy matters in the government and enterprise arenas has significantly broadened the scope of individuals who must be aware of relevant issues as part of their work. Security is becoming more of an element of existing roles such as records management, and new security roles such as Chief Information Security Officer are appearing in the enterprise. Finally, security considerations may become new elements of traditional responsibilities (*e.g.*, programmers historically have been expected to document code, but now should be aware that failure to document may be a factor in a law enforcement investigation of whether a data breach was foreseeable).

This course will examine legal, policy, and enterprise issues and problems related to security and privacy. Electronic data will be the focus but other forms of information also will be considered. Discussions will take general approaches and also focus on specific technologies.

Learning Objectives

The course will provide students with:

A general background in concepts of privacy in American society;

An understanding of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security;

Knowledge of laws and regulations concerning information security from both data protection and law enforcement perspectives. Policy questions related to these laws and regulations will be examined as part of discussions and readings. United States federal laws and policies will be the focus of the course but comparison will be draCoursewn to approaches taken by states and other nations and organizations.

Knowledge of the role of private regulatory and self-help efforts.

An understanding of how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices. These issues will be addressed largely through the context of examining mechanisms for the safeguarding of data.

At the end of the course, students in a variety of disciplines will have an understanding of the concepts and issues necessary to address emerging areas of security and privacy in their potential or current careers. Broadly defined roles include, but certainly are not limited to, systems managers, developers, and engineers; librarians, records managers and other archivists; business managers whose areas of responsibility include systems; data analysts; public and private sector policy professionals; and privacy and security professionals.

Course Format

Classes will consist of a lecture followed by a seminar discussion. Guest speakers, some still to be scheduled but hopefully including representatives of interest groups, private industry, and law enforcement, will be part of the course as availability and remote technologies allow. Students are expected to read the required readings for each class, be prepared to discuss the issues that they address, and raise questions and make comments pertaining to their content. Opportunities for students to initiate discussions of current issues and events related to information security and privacy also are important parts of the program.

Students may be called upon at least once during the semester to assume leadership roles (in conjunction with the instructor) in guiding individual class sessions. As part of this assignment, students will be required to prepare 1-2 page analyses of the week's readings for distribution to the class. These analyses may be distillations of what a student regards as the primary points of the readings or opinion pieces on issues raised.

Students also will be expected to complete two individual writing assignments and participate in a group project.

Course Program

Required Texts

International Guide to Privacy – American Bar Association (Privacy)
International Guide to Cyber Security – American Bar Association (Cyber Security)
Roadmap to an Enterprise Security Program - American Bar Association (Roadmap)
The Executive Guide to Information Security – Egan and Mather (Guide)
Case studies from the Harvard Business School. These materials are available from http://cb.hbsp.harvard.edu/cb/access/5263390

These materials should be on reserve in the library, except for the case studies. In addition, I have requested reserve copies of
Security Metrics: Replacing Fear, Uncertainty, and Doubt – Jaquith
Information Assurance for the Enterprise: A Roadmap to Information Security – Shoemaker and Schou

In addition, anyone who has or develops a particular interest in the increasingly important area of cloud computing may want to look at *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.*
Download at no charge from
http://www.cloudsecurityalliance.org/csaguide.pdf

Other readings are identified in the syllabus. In the interest of keeping up to date in evolving fields, the instructor also will supply materials of interest that are discovered or published during the course. Some supplemental materials on the list below will drop out along the way.

Readings will include laws, regulations, and technical standards. These materials will be used as part of the framework to address the core issues in the course. Students will not be expected to master legal or technical intricacies.

Guest speakers from the public and private sectors also will show up on the syllabus as their schedules permit. Guests in the past have included representatives from UM, the FBI, FTC, and an e-commerce privacy certification organization (the person now is with DHS). I hope to have someone from a security auditing firm this year.

Assignments

Writing Assignment 1: Prepare a 4-6 page, double spaced, paper which explores the approach of the federal government toward issues of privacy and security

and compares it to the ideas followed by states or international governments and organizations. This paper may be an overview or focus on specific subjects and laws. Due by midnight of the Friday of the week 6 class, 2/12.

Writing Assignment 2: Prepare a 4-6 page, double spaced, paper exploring security risks and potential consequences of breaches in any of the data or system topics discussed in the class. Present your views concerning appropriate roles of industry self-regulation or law enforcement with respect to the problem that you discuss. Due by midnight of the Friday of the week 10 class, 3/19.

Group Project: The group project will require examination of enterprise settings in which to examine the concepts of integrated enterprise security planning discussed in the course. Students will be required to study interdisciplinary approaches to ensuring the security and integrity of systems and information, with reference to business issues, technology, and relevant laws, regulations, and law enforcement precedent. The instructor will assign groups to study real-world enterprises, which will involve in part interviews with staff of the organizations.

The final products will be group class presentations in Week 13 and 14, and a group 10-12 page double spaced paper due by midnight of the last day of class of a date TBD during the finals period..

All written materials shall be submitted in electronic form to CTools drop boxes or to the instructor by email.

Grading

Formal assignments will count for 30% each.

Class participation, through questions, comments, current issue discussions, posts to CTools Forums and Discussions, and possible short presentation assignments, will be 10%.

Accommodations for Students with Disabilities

If you think you need an accommodation for a disability, please let me know at your earliest convenience. Some aspects of this course, such as the assignments, the in-class activities, and the way I teach may be modified to facilitate your participation and progress. As soon as you make me aware of your needs, we can work with the Office of Services for Students with Disabilities (SSD) to help us determine appropriate accommodations. SSD (734-763-3000; www.umich.edu/~sswd) typically recommends accommodations through a Verified Individualized Services and Accommodations (VISA) form. I will treat any information you provide as private and confidential.

General Writing Requirements

Original Work

All written submissions must be your own original work. You may incorporate selected excerpts from publications by other authors, but they must be clearly marked as quotations and must be attributed. If you build on the ideas of prior authors, you must cite their work. You may obtain copy editing assistance, and you may discuss your ideas with others; collaborative learning is valuable. However, all substantive written work and ideas must be your own, or be attributed explicitly to another.

See the Rackham Graduate policy on Academic and Professional Integrity at www.rackham.umich.edu/policies/gsh/appb for the definition of plagiarism, and associated consequences.

Writing Guidelines

These guidelines should help in framing your writings. Some of them are standard advice. Others reflect my own biases.

1) Put your name on the paper **and** in the filename of electronic assignment submissions.
2) Follow the assignment. If you have other ideas or topics that you really want to explore, talk to me first.
3) Be clear and, most important, concise; frame your topic, follow it with a discussion, and then wrap it up in a final paragraph or two.
4) Don't make conclusory statements. Support statements of fact with citations or arguments with logical steps that led you to your belief; present conclusions rather than opinions.
5) Don't let your biases get in the way. Let the thesis fit the facts; don't force the facts into a preconceived notion. The latter approach often leads to "facts" that cannot be documented.
6) Avoid being overbroad. "Always," "never," etc., may work but are risky in general.
7) Avoid sentence fragments. Make sure that the sentence has an object, subject, and verb.
8) Proof read. It often helps to have a colleague read your paper. Reading a printed version yourself also will catch mistakes that you might not see on the screen.
9) I'm not a stickler for citation form or location. However, the citation must have enough information for me to find it online or on a shelf.
10) The first two assignments are academic policy essays.

a. Be assertive. State your position or conclusions without, for example, “I think” or “I believe.” For example, “Google will rule the world someday,” not “I think that Google will rule the world someday.”
b. Stay away from first and third person; *e.g.,* I will examine, we will analyze, you would expect.

Rules for research papers, such as the final project, are different with respect to #10. Research can produce “we discovered,” “the subject told us,” etc., statements.

Online Research Guidelines

1) Cite the complete URL and date retrieved. Include a page number or section name if the article has discrete links to pages or sections.
2) Wikipedia and other wiki-based materials are not acceptable primary resources; do not cite them in your papers. They can be useful as guides to research but, by their nature, are not authoritative. So that you don’t think I’m being a complete Luddite, I will add that encyclopedias never have been acceptable primary sources in academic writing.
3) Make some attempt to vet your sources. The fact that somebody has a keyboard and a broadband connection doesn’t automatically make the person worth citing or quoting.

SI 510 Weekly Course Schedule

I. Early (comparatively) Privacy Protections
Week 1 – Introduction – 1/8
Objectives
Expectations
Description

Overview of the origins of the concept of privacy: tort, religion, common law, and early U.S. statutes

Readings: U.S. Department of Heath, Education & Welfare, "*Records, Computers and the Rights of Citizens,"* 1973
http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm
(you may need to copy/paste this URL into your browser)

Privacy Protection Study Commission, 1977 – Center for Democracy and Technology Summary of Findings
http://web.archive.org/web/20060206164013/www.cdt.org/privacy/guide/basic/ppc.html

If the short pieces above really grab you:
HEW Study Summaries and Recommendations
http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm

PPSC Report Text
http://epic.org/privacy/ppsc1977report/
These sections of the Introduction are particularly instructive:
"The Objectives of a National Policy" to subheader "Minimizing Intrusiveness"
First paragraph under Implementation Choices
"Therefore the Commission recommends" to header "Presentation of the Commission's Findings"

Week 2 – Privacy Meets Security – Data Protection Statutes – 1/15
Federal Trade Commission (starting in 1998)
decided that companies that violate their published privacy statements or that suffer data breaches may be engaging in *"unfair or deceptive acts or practices in or affecting commerce"*
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Children's Online Privacy Protection Act of 1998 (COPPA)
Gramm-Leach-Bliley Act of 1999 (GLBA)
Sarbanes-Oxley Act of 2002 (Sarbox)
Fair and Accurate Credit Transactions Act of 2003 (FACTA)
ID Theft Laws

Readings: Privacy, Chapter 1, pp. 11-70
Gramm Leach Bliley Safeguards Rule, www.ftc.gov/os/2002/05/67fr36585.pdf,
Concentrate on the official language on pp. 11-12. The rest provides background on the considerations involved in issuing the final language.
HIPAA Security Rule, www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf.
Concentrate on the official language on pp. 41-end. The rest provides background on the considerations involved in issuing the final language.
Where We're Headed: New Developments and Trends in the Law of Information Security, Smedinghoff

Week 3 – Approaches by other jurisdictions – 1/22
States provisions:
Breach notification – CA, MI
"Reasonable security" standard – TX, RI, CA

International: Convention on Human Rights – 1950; OECD Guidelines – 1980; EU Data Protection Directive – 1995; EU Directive on Privacy and Electronic Communications – 2002

Readings: Privacy, Chapter 1, 72-end
Privacy, Chapter 2
Consumer Privacy and Identify Theft, California Senate Research Office
Massachusetts Law on Credit Freezes and Security Breaches
Massachusetts "Standards for the Protection of Personal Information of Residents of the Commonwealth"
Choicepoint case study

Week 4 – Public-Private Interrelation – 1/29

Issues which may affect cooperation between government and the private sector in protecting security in a broad sense and individuals in a narrower one. Government adoption of private standards through mechanisms such as Safe Harbor provisions in GLBA and COPPA.

Readings: Cyber Security, Chapter 3
Statutes adopting language of private sector Payment Card Industry Digital Security Standards
www.transactionworld.com/articles/2007/July/security1.asp
www.transactionworld.com/articles/2007/November/security1.asp
www.privsecblog.com/archives/security-breaches-state-laws-to-shift-some-data-breach-costs-to-businesses-with-weak-security.html
www.complianceweek.com/article/3680/pci-standard-catches-lawmakers-eyes
[Sometimes it displays and sometimes it prompts for a login. I'm looking for an alternative]
www.storefrontbacktalk.com/securityfraud/the-ultimate-cyberthief-gift-cas-veto
Article discussing reasons for veto of California law that, among other provisions, adopted PCI-DSS language
www.scmagazineus.com/Schwarzenegger-shoots-down-California-data-protection-bill/article/57998
Flayton Electronics Case Study

Section II. Interaction among Law and Technology; Intersection of issues, laws, and reality

Week 5– System Hacks and Attacks – 2/5
DDOS
Bots
Hacks
Exploits
Malware

Readings: Cyber Security, Chapter 1
"Immunizing the Internet, or: How I Learned to Stop Worrying and Love the Worm"
www.harvardlawreview.org/issues/119/june06/note/immunizing_the_internet.pdf
Root Server Attack on 6 February 2007. ICANN fact sheet
www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf
Report on Team Evil cyberterror web defacement attack. Prepared by Beyond Security
"Digital Fears Emerge After Data Siege in Estonia"

http://www.nytimes.com/2007/05/29/technology/29estonia.html
Estonian Cybercrime Security Strategy
Boten Ana clip

Week 6 – Data security – 2/12
Breached and lost data
Law enforcement actions
Private reaction
Necessary changes in business attitudes and processes

Readings: Cyber Security, Chapter 5
Datagate: the Next Inevitable Corporate Disaster?, McAfee
Read press releases (more if you want) for cases under:
www.ftc.gov/privacy/privacyinitiatives/promises_enf.html and
www.ftc.gov/privacy/privacyinitiatives/safeguards_enf.html

Read closing letter for Compaq Computer Corp under
www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

Providence Hospital HIPAA data loss enforcement action
Background story. Read all 6 sections. Note "Challenge" in the Base Case tab.
http://www.baselinemag.com/c/a/Health-Care/Identity-Theft-Providence-Healths-Serious-Pain/
HHS HIPAA order
www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index2.html
www.healthleadersmedia.com/content/215412/topic/WS_HLM2_TEC/HHS-Providence-Health-Services-Reach-Resolution-Agreement.html

Piedmont Hospital rumored HIPAA audit\
www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024921
www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025253

HIPAA criminal proceedings
www.ama-assn.org/amednews/2006/10/16/gvsb1016.htm

iPremier case study, section A. We'll read the rest during the class.

Week 7 - Enterprise Roles - 2/19
Technology
Law
Business

Readings: Roadmap

Week 8 – Self-Regulation and Privacy– 3/26
Privacy policies and security claims
Privacy seal programs
Chief privacy officers
Chief security officers

Readings: Privacy Chapter 3
Privacy pp 171-196 (top)
TRUSTe standards, www.truste.org/requirements.php
www.truste.org/businesses/faq.php
www.truste.org/articles/seals_comparison.php
A National Information Assurance Strategy, UK Central Sponsor for Information Assurance
www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/nia_strategy.pdf
FTC "eHavioral" report and supporting statements by commissioner
www.ftc.gov/opa/2009/02/behavad.shtm

Week 9 – Standards and Best Practices – 3/12
Finding and using the benchmarks for establishing what needs to be addressed in analyzing system security. The issues and sources will vary depending on an organization's location and purpose, and whether it is public or private.
Industry codes and voluntary guidelines

FISMA
NIST 800-53
ISO 27001, 27002
PCI-DSS

Readings: Cyber Security, Chapter 4.
ISO 27001/27002 standards plain English summaries
www.praxiom.com/iso-27001.htm
www.praxiom.com/iso-17799-2005.htm
Payment Card Industry Data Security Standard,
https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

Week 10 – *Real World Considerations - 3/19*
Laws and standards exist and are expanding. These requirements may not square with real world business realities.

Readings: *A Holistic View of Risk,* Institute of Internal Auditors, www.theiia.org/download.cfm?file=49987
Toward a Quantitative Model for Measuring the Operational Performance of Information Security Programs, Edward G. Schwartz
Measuring the Effectiveness of Security using ISO 27001, Steve Wright
Andrew Jaquith videos on security metrics in software development
www.informit.com/podcasts/episode.aspx?e=3759a5c3-a4fc-4c6a-8d96-f6db8b915a4a
www.informit.com/podcasts/episode.aspx?e=c841fe32-55a3-4e95-8b4c-7de899c2722b
www.informit.com/podcasts/episode.aspx?e=f5717f92-765d-4cce-a1ca-bdd4d8f202b2

Section III. Putting It All Together

Week 11 – Enterprise Security Program – People and Process – 3/26
Developing a coordinated program for prevention and crisis
People
Processes

Readings: Guide Chapters 1-5
Setting Long Term Goals for Internal Audit, Dan Swanson
http://www.complianceweek.com/index.cfm?fuseaction=article.viewArticle&article_ID=3008

Week 12 - Enterprise Security Program – Technologies – 4/02
Developing a coordinated program for prevention and crisis
Systems
Components
Business Continuity

Readings: Guide Chapters 6-9

Week 13, 14 - Putting It All Together – 4/09, 16
Real world examples
Final project discussions