History will record what we, here in the early decades of the information age, did to foster freedom, liberty, and democracy. Did we build information technologies that protected people’s freedoms even during times when society tried to subvert them? Or did we build technologies that could easily be modified to watch and control?


Protecting privacy and ensuring security requires “watch and control” technology. How much should we build and how should we use it? We should answer this question in a way fully informed by our fundamental values. Unfortunately, this is not happening. The economic concerns of businesses—not our values—are driving a rapid and extensive development of “watch and control” technology.

*Unless otherwise indicated, all readings are available on the course websites.* For the Chicago-Kent website go to www.kentlaw.edu/classes, click on "Richard Warner,” click on “Privacy and Security.”

Assignments: (1) Setting up PGP encryption; (2) short comment on user and privacy policies; (3) final paper.

**I. INTRODUCTION TO AMERICAN LAW (for non-law students)**

Tutorials (go to www.kentlaw.edu/classes, click on “Richard Warner,” click on “Introduction to American law.”)

Aalberts et al., Trespass, Nuisance, and Spam: 11th Century Common Law Meets the Internet

Warner, *Adjudication* (recommended)

**II. WHY PRIVACY MATTERS**

**A. Privacy Values and Interests**

Asimov, *The Dead Past* (Xerox)

Kang, *Information Privacy in Cyberspace Transaction* (selections)

1. Privacy values: Spatial, decisional, informational

   a. Relations among these interests
Warner, *Surveillance and the Self* (selections)
Warner, *Why Privacy Matters* (selections)

2. The Common Knowledge Background
3. Privacy and the Self

**B. Information and Market Efficiency**

Charles E. Lindblom, *THE MARKET SYSTEM: WHAT IT IS, HOW IT WORKS, AND WHAT TO MAKE OF IT* (recommended only--book available on Amazon).

1. Targeted Advertising


2. Price Discrimination

Varian, *Price Discrimination*

**C. Privacy Norms**

Daniel Solove, *A Taxonomy of Privacy*

Ann Bartow, *A Feeling of Unease about Privacy Law*

Warner, *Norms*

1. The common law privacy torts

Dwyer v. American Express

Topheavy Studios, Inc. v. Jane Doe (recommended)

Remsberg v. Docusearch, Inc. (recommended)

Michaels v. Internet Entertainment Group, Inc., et al (recommended)

**III. PRIMER ON THE INTERNET**

Warner, *Introduction*

Solomon and Chapple, *INFORMATION SECURITY ILLUMINATED*, Chapter 6.1
A. Structure of the Internet

B. Intelligent Versus Dumb Networks

C. The End-To-End Principle

D. Openness and Its Costs
   1. Non-Proprietary Protocols
   2. No Gatekeeper
   3. Implied-permission access

IV. PRIVACY: WHAT TECHNOLOGY HAS CHANGED

A. Increased Powers of Surveillance, Aggregation, and Analysis

Odlyzko, Privacy and the Clandestine Development of E-Commerce

Odlyzko, Privacy, Economics, and Price Discrimination on the Internet

Levinson and Odlyzko, Too Expensive to Meter

Privacy International, A Race to the Bottom: Privacy Ranking of Internet Service Companies

Privacy International, 2007 Privacy Rankings

Warner, Surveillance and the Self (selections)

Warner, Why Privacy Matters (selections)

B. Prospects for Privacy Norms

V. GENERAL INTRODUCTION TO INFORMATION SECURITY

Anderson, SECURITY ENGINEERING, Chapters 1, 22.1–22.2, and 22.5 (Chapters may be downloaded from http://www.cl.cam.ac.uk/~rja14/book.html or hard copy book can be purchased)

Solomon and Chapple, INFORMATION SECURITY ILLUMINATED, Chapters 1, 2.1, 3, 7.9 (hard copy)
A. Foundations of Information Security

1. Security goals: the confidentiality, integrity, availability triad
2. Security standards and policies
3. Security mindset
4. Defense in depth
5. Brief overview of threats
6. Security versus usability, time, and/or money tradeoffs

A. Very Brief Overview of Risk Assessment

VI. The Economics of Information Security

A. Information Security as a Negative Externality

Anderson, *The Economics of Information Security*

B. The Lemons Market in Security Products

Bruce Schneier, *A Security Market for Lemons*,
http://www.schneier.com/crypto-gram-0705.html

C. Prevention or Response?

1. Prevention technologies
2. Response and remediation

D. Market Solutions

1. Information markets

Sunstein, *INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE* (selections)

A. Insurance

Kalinich, *Network Risk Insurance: A Layman’s Overview*

AIG on network risk insurance,
http://www.aigexecutiveliability.com/executiveliability/productdetail/0,2128,448-13-2995,00.html
E. Legal Solutions

   A. The need for norms

VII. Software

   A. Why Software Vulnerabilities Are Inevitable

   Anderson, Chapter 22.3.
   1. Technological reasons
   2. Economic reasons

   B. The Problem of a Single Dominant Operating System

   C. A Role for Open Source Software

   D. Legal Responses

      1. Industry standards

         In re America Online Inc. Version 5.0 Software Litigation
         Kaczmarek v. Microsoft Corp. (recommended)
         In re Sony BMG DD Technologies Litigation (recommended)

      2. The large grey area

   E. Market responses

         Sunstein, INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE (selections)


   F. End User License Agreements

         Lemley, Terms of Use

         ProCd v. Zeidenberg
         Klocek v. Gateway

VIII. Information Security Technology

   A. Technology
1. Protocols
Anderson, Chapter 2, omitting 2.7

2. Authentication and Passwords
Solomon and Chapple, Sections 2.6, 2.8, and 10.6
Anderson, Chapter 3

3. Cryptography and Digital Systems
Solomon and Chapple, Chapter 5
Anderson, Chapter 5.1–5.3

4. Access Control
Solomon and Chapple, Chapter 10.5–10.6
Anderson, Chapter 4, skipping 4.3

B. Legal responses

1. Negligence liability
Guin v. Bazos
Forbes v. Wells Fargo Bank
Banknorth v. BJ's Wholesale Club
Sovereign Bank v. BJ's Wholesale Club

2. Disclosure statutes
California Civil Code Section 1798.82

XI. MALWARE, SPYWARE, ADWARE

A. Viruses, Worms, and Trojans

1. Legal responses
United States v. Morris
Entry of Verizon-Maine into the InterLATA Telephone Market

2. Market responses

B. Spyware and Adware

1. Legal responses
X. DENIAL OF SERVICE AND NETWORK ATTACKS

A. Network Infrastructure including security

Solomon and Chapple, Chapter 6.2–6.5
Anderson, Chapter 6.2

B. Botnets

C. Network Attacks, Technological Defense Measures

Solomon and Chapple, Chapters 7.8–71., 11.1–11.3, and 12
Anderson, Chapter 18

1. Spyware programs

2. Firewalls
   Solomon and Chapple, Chapter 8

3. Network intrusion detection
   Solomon and Chapple, Chapter 13

C. Market Responses

D. Legal Responses

XI. E-MAIL (if time allows)

A. What Is Spam?

CAN SPAM Act

B. Who Should Attempt to Regulate Spam?

Media3 Technologies, LLC v. Mail Abuse Prevention System
Hall v. Earthlink Network, Inc.