PRIVACY

Supplement to CSH5 Chapter 69

“Security Audits, Standards and Inspections”

Notes by M. E. Kabay, PhD, CISSP-ISSMP
Assoc Prof Information Assurance
School of Business & Management
Norwich University

NOTE

- This lecture is a supplement to the material in CSH5 chapter 69, “Privacy in Cyberspace.”
- Theses slides do not follow the structure of the chapter; they also include additional material.

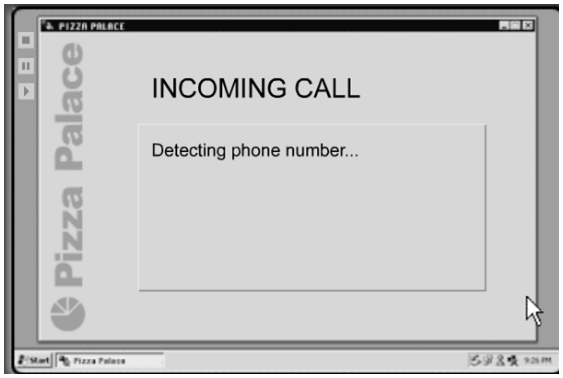
-- M. E. Kabay, PhD, CISSP-ISSMP

Topics

- Introduction: A Future Pizza Order
- Privacy in US Jurisprudence
- Effects of Information Technology on Privacy
- Fourth Amendment Issues
- Key US Laws Protecting Privacy
- Defending Privacy in Cyberspace
- Reading about Privacy

Introduction: A Future Pizza Order (2006)

- http://www.youtube.com/watch?v=RNJl9EEcsoE



INCOMING CALL

Detecting phone number...

Privacy in US Jurisprudence

- Privacy:
  - ❑Power to control truths about you that other people know
  - ❑Power to hide parts of the truth
    - ✓From *Cyberspace Law for Non-Lawyers*

http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html

Common Law Privacy

- *The makers of our Constitution. . . Sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the Government, the right to be let alone – the most comprehensive of the rights of man and the right most valued by civilized men.”*

Justice Louis D. Brandeis
Dissenting in the *Olmstead* decision

Common Law Privacy

Invasion of privacy under common law:

- Intrusion upon seclusion
- Appropriation of name or likeness
- Publicity given to private life
- Publicity placing person in false light

- US Constitution does not specifically mention privacy
  - ❑But 4th amendment usually applied when discussing government intrusion

Types of Privacy

- Informational privacy: Truths you have revealed to others but still want to control
  - ❑Public records
  - ❑Medical records
  - ❑But public behavior is not protected
- Truths you have kept private
  - ❑Books you read
  - ❑What you say in private letters or e-mail
  - ❑Used to protected by laws of *trespass*

Effects of Information Technology on Privacy

- Radical change in ease of acquiring data about individuals
  - ❑Electronic purchase records
  - ❑Telephone and e-mail records
  - ❑Surveillance technology redefines *public space*
  - ❑Identification technology reduces the anonymity of the crowd
  - ❑Public records online
- Radical change in ease of acquiring aggregate data about groups

Informational Privacy

- US law traditionally did not limit uses of observations about consumers
  - ❑What you buy / read / view / eat
  - ❑Data shared among credit agencies
  - ❑Names, addresses, preferences sold to advertisers
  - ❑Even medical data were not much protected
- European Privacy Directive much more stringent
  - ❑Caused problems for US firms – barred from doing business because of lax laws

Informational Privacy and the Internet

- Google bought DejaNews
  - ❑Archive of all USENET discussions
  - ❑Spans ~15 years
  - ❑Can provide interesting information about previous levels of professionalism
- Google caches Web pages
  - ❑Owner can remove an embarrassing page from Web site
  - ❑But cached copy persists for months

Controlling Electronic Information is Difficult

- E-mail messages often circulated without permission
  - ❑Theoretical violation of copyright
  - ❑In practice, impossible to stop once it starts
- Private message group discussions are often made public
  - ❑Can be embarrassing
  - ❑Has led to lawsuits

Data Collection on the Web

- Cookies store information about where you have been on a specific Web site
  - E.g., AMAZON uses cookies to track your identity and your book preferences
  - Unless badly formed, cookies are not supposed to be shared among Web sites
- Web bugs
  - 1-pixel images (invisible) that return information to specific advertisers
  - Allow tracking of how many people visit a Web page vs how many click on ads

Data Collection – cont'd

Spyware

- Software that covertly communicates with a Web address *(phones home)*
- Caught by firewalls
- Present in Comet Cursor – cartoon cursors favored by children
- Sends information about exactly what Web pages kids are looking at
- Covert market research
- *Some spyware does not remove itself via its uninstall function*

Spyware

- What is spyware?
- How does spyware enter a system?
- Examples of spyware
- Removing spyware
- Blocking spyware

What Is Spyware?

- Spyware: any *technology* that covertly gathers information
  - About person
  - About organization
  - About system
  - Without knowledge of victim
- Any *software* which
  - Employs user's Internet connection
  - In background ("backchannel")
  - Without their knowledge or explicit permission

How does Spyware Enter a System?

- Install freeware, shareware
  - Often those that are ad-supported
- Some browser plugins
  - Offer new functions,
  - New file format compatibility
- Viruses & worms
  - E-mail attachments

Early Examples of Spyware

- Aureate / Radiate
- Conducent / Timesink
- Comet Cursor
- Creative Labs
- GoHip
- Web3000

Aureate / Radiate

- Toolkit for information gathering
  - ❑ Used by programmers of other programs
  - ❑ Installed in > 30,000,000 computers
- Functions of toolkit
  - ❑ Send advertising to computers where Radiate code was installed
  - ❑ Exchange information between client and host computers
  - ❑ Collect *nonspecific* data about usage
  - ❑ Ask for answers to survey of preferences relating to products & services

Aureate / Radiate Problems

- Did not tell developers to include warning to users (end-user license agreement, EULA)
- Allowed programmers to defer or eliminate demographics survey
- Can download arbitrary code from any server
  - ❑ Uses browser process & permissions
  - ❑ Therefore passes firewalls
  - ❑ update-dll.exe already found in 3 different versions in the wild
- Demonstrated to cause browser & Windows crashes
  - ❑ Common knowledge in tech support: remove advert.dll to stop (main component of A/R)

Conducent / Timesink

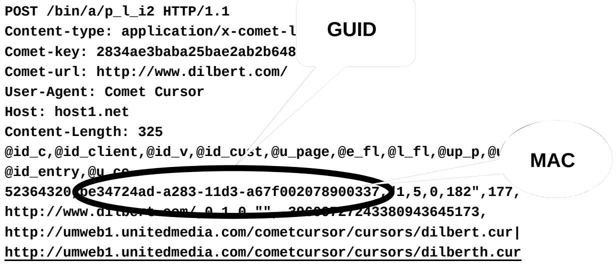
- Software Developers Kit
  - ❑ SoftClick Optimization Engine
  - ❑ Timesink = TSadbot.exe
- Delivers advertising to client computer
  - ❑ Retrieves user / campaign activity information
  - ❑ Maintains comprehensive system for campaign management & reporting
- Users include
  - ❑ CD-ROM distributors
  - ❑ eGames (large game publisher)

Comet Cursor

- Changes cursor to animated cartoon when visiting Comet Cursor enabled Web sites
  - ❑ Installed by > 90,000,000 users
- Installations (except of RealPlayer) install GUID (Globally Unique Identifier)
- Automatically updates code
- Counts how many times user changes cursor
  - ❑ Provides aggregated *anonymous* information to clients
  - ❑ Records URL where cursor changed
  - ❑ URL of next page viewed

Comet Cursor Analysis

- Richard M. Smith (well-respected author), 1999
  - ❑ Noticed attempts to contact server
  - ❑ Used sniffer to analyze what was being sent:



```
POST /bin/a/p_l_i2 HTTP/1.1
Content-type: application/x-comet-l
Comet-key: 2834ae3baba25bae2ab2b648
Comet-url: http://www.dilbert.com/
User-Agent: Comet Cursor
Host: host1.net
Content-Length: 325
@id_c,@id_client,@id_v,@id_cust,@u_page,@e_fl,@l_fl,@up_p,@u
@id_entry,@u_ce
52364320,be34724ad-a283-11d3-a67f002078900337,"1,5,0,182",177,
http://www.dilbert.com/,0,1,0,"",-39600727243380943645173,
http://umweb1.unitedmedia.com/cometcursor/cursors/dilbert.cur|
http://umweb1.unitedmedia.com/cometcursor/cursors/dilberth.cur
```

Creative Labs

- Makers of popular sound cards, music players
- Include *newsupd.exe* file in installations
  - ❑ Automatically checks for driver updates
  - ❑ But also sends information about user program usage to Creative Labs server
- Problems
  - ❑ Not documented
  - ❑ No way of turning off in early versions
- Outcry has resulted in improvements

GoHip

- Describes itself as “metasearch engine”
- Accused of covert installations
  - Installs “Windows Startup” program into Start Menu
  - Reconfigures browser to visit GoHip site every time browser is launched
  - Redefines search default to GoHip
  - Changes autosignature files to attach advertisement to every e-mail message recommending visit to GoHip
- Privacy policy now details all of this information

Web3000

- Web3000 Ad Network
- Toolkit for software developers
- Automatically supplies
  - Browser headlines
  - Splash screens
  - Status-bar messages
  - Opt-in e-mail newsletters
  - Installation offers
- Automatically tries to connect to its server even when user is not using browser

Removing Spyware

- Problems with uninstalling spyware
  - Some products do not (or did not) include uninstall function
  - Uninstall function failed in several cases
  - Some products reinstall themselves
- Tools available for removal; e.g.,
  - AdAware http://www.lavasoftusa.com/
  - Aureate/Radiate DLL remover http://www.spychecker.com/radiateremover.html
  - PestPatrol http://www.pestpatrol.com/

Blocking Spyware

- Can prevent messages from reaching “mother ship”
- Silencer http://www.spychecker.com/silencer.html
  - Points all connections to adware sites to null address (127.0.0.1) in Windows hosts file
- Personal firewalls; e.g.,
  - BlackIce http://www.blackice.com
  - Norton Personal Firewall 2002 http://www.symantec.com/sabu/nis/npf/
  - ZoneAlarm http://www.zonelabs.com

Preventing Spyware Infestations

- Read the fine print before installing software
  - Especially *adware* = freeware supported by advertising
- Run appropriate scanners (removal tools) periodically
- Firewalls help identify infestations as well as blocking transmissions
  - Choose firewall capable of trapping unexpected *outbound* connections
  - Set parameters to alert user to unauthorized connections

Arguments Defending Data Collection

- Doesn’t hurt anyone
- No names collected
- Helps to improve effectiveness of advertising
- Improves market mechanisms by providing statistical information about consumer preferences

Attacks on Data Collection

- Issue is control
- Covert data collection is unacceptable
- Data subject must be informed
  - ❑Who is collecting what info
  - ❑For what purpose
  - ❑How to stop collection
  - ❑Who has used information

Fourth Amendment Issues

- Fourth Amendment to the US Constitution passed in 1791
  - ❑Forbids unreasonable search and seizure by government and law enforcement agents
- Did not apply to new technological means of information gathering
  - ❑1928 SCOTUS decision excluded telephone wiretaps from 4th Amendment protection
  - ❑Brandeis dissented, arguing that interpretation must be updated to include new technologies

New Interpretations of 4th Amendment

- 1968 Katz vs US
  - ❑Constitution protects “people, not places”
  - ❑Invasion of property not the issue
  - ❑Key is whether person has “reasonable expectation of privacy”

Later Judgements

Would you expect privacy in

- Bank records (no: US vs Miller)
- Car travel tracked by LoJack (no: US vs Knotts)
- Material stored in open field (no: Oliver vs US)
- Garbage on curbside (no: CA vs Greenwood)
- Material visible from plane (no: Dow Chemical v US)
- Marijuana farming Gro-Lights seen via Infrared cameras (yes: US vs Robinson)

Key US Laws Protecting Privacy

- Fair Credit Reporting Act of 1970
- Privacy Act of 1974
- Right to Financial Privacy Act of 1978
- Privacy Protection Act (PPA), 1980
- Electronic Communications Privacy Act (ECPA), 1986
- Telephone Consumer Protection Act, 1991
- Health Insurance Portability and Accountability Act (HIPAA), 1996
- Gramm-Leach-Bliley Act (GLB), 1999

Fair Credit Reporting Act of 1970

- Credit reports limited to
  - ❑Credit application
  - ❑Insurance
  - ❑Employment
  - ❑Government benefits
  - ❑Business transactions justifying such reports
- Credit bureaus are data sinks
  - ❑Share information via clients (banks etc.)
  - ❑Refusals can be mislabeled, sent on
  - ❑Wrong data can circulate endlessly
  - ❑FCRA requires due care to remove / correct bad info
- See http://www.ftc.gov/os/statutes/fcra.htm

Privacy Act of 1974
5 USC §552a

- Government agencies may not conceal data gathering about individuals and data repositories
- Also restrictions on distribution
- Publish notice giving details including
  - ❑Name, location
  - ❑Types of people covered
  - ❑Purposes of routine uses of the data
  - ❑Responsible persons
  - ❑Means for *data subjects* to check correctness of record about themselves

http://www4.law.cornell.edu/uscode/5/552a.html

http://www.usdoj.gov/04foia/privstat.htm

Right to Financial Privacy Act of 1978 (amended 1987)

- Limits *government* access to financial records
- Allows reports to government agencies for
  - ❑Establishing collateral or security for loan
  - ❑Bankruptcy proceedings
  - ❑Application for government loans
- Banks (etc.) may notify government agencies of suspected wrongdoing
- Customers may authorize any disclosure
  - ❑Permission extends max. 3 months
  - ❑Permission can be revoked any time

http://www.dol.gov/dol/allcfr/SOL/Title_29/Part_19/toc.htm

Privacy Protection Act (PPA) of 1980 42 USC §2000aa

- Protects journalists' and writers' materials and sources
- Require probable cause for search or seizure
  - ❑Except if crime is in process or has already occurred
  - ❑To prevent immediate injury to a victim
- Steve Jackson Games case
  - ❑Secret Service raided game company
  - ❑Seized computers, refused to return them
  - ❑See http://www.eff.org/Legal/Cases/SJG/

http://www4.law.cornell.edu/uscode/42/2000aa.html

Steve Jackson Games vs Secret Service

- March 1, 1990
  - ❑ Chris Goggans "Erik Bloodaxe" arrested, computer gear confiscated
  - ❑ JG small SciFi computer-game maker in Austin TX
  - ❑ LEO raided HQ, confiscated computers
  - ❑ Seized gaming manual called *G.U.R.P.S. Cyberpunk* thinking it was a terrorism manual
- Police misinterpreted Cyberpunk game
  - ❑ Loyd Blankenship – SJG employee
  - ❑ Simulated cyberspace conflicts
- Operation Sundevil – May 8, 1990
  - ❑ Crackdown on phone fraud and credit-card fraud bulletin boards around USA

Electronic Communications Privacy Act (ECPA), 1986

- 17 USC §1367 et al.
- Governs interception and disclosure of electronic communications
  - ❑Telephone
  - ❑E-mail
  - ❑Fax
  - ❑Pager
- Employers are not subject to ECPA restrictions on their own employees' communications
  - ❑Except if they have allowed a reasonable expectation of privacy to develop

http://www.cpsr.org/cpsr/privacy/wiretap/ecpa86.html

Telephone Consumer Protection Act, 1991

- 47 USC §227
- Bars automated calling systems that charge consumers
- Makes unsolicited commercial fax illegal
  - ❑Need pre-existing business relation *or*
  - ❑Agreement of recipient
- Some attempts to extend this law to junk e-mail
  - ❑UCE = unsolicited commercial e-mail
  - ❑aka *SPAM*
- http://www.fcc.gov/ccb/consumer_news/tcpa.html

Health Insurance Portability and Accountability Act (HIPAA), 1996

- 42 USC 1297ii
- Protects employees who change jobs but want to keep their health insurance
- Mandates administrative simplification
- Privacy provisions affect everyone who collects, keeps and transmits medical information
- Patients must have full access to their medical files
- Standards for protecting *individually identifiable health information*
- http://www4.law.cornell.edu/cgi-bin/htm_hl?DB=uscode&STEMMER=en&WORDS=hipaa+&COLOUR=Red&STYLE=s&URL=/uscode/42/1397ii.html
- Also overview at http://www.hcfa.gov/hipaa/hipaahm.htm

Gramm-Leach-Bliley Act (GLB), 1999

- Financial Services Modernization Act
- Many sections dealing with structure of banks, securities firm
- Title V – Privacy
  - Clear disclosure of privacy policies
  - Notice to consumers
  - Opt-out of sharing consumer info
  - Enforced by FTC, federal banking agencies, SEC, National Credit Union Administration
- http://www.senate.gov/~banking/conf/grmleach.htm

Recent US Laws Affecting Privacy

- U.S.A.P.A.T.R.I.O.T. Act
  - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
  - Called the "US *Patriot* Act" to sway public opinion in its favor
  - Passed by a Congress whose members did not read the text of the Act
- TIA System
  - Total Information Awareness

U.S.A.P.A.T.R.I.O.T. Act

- http://w2.eff.org/patriot/
- Signed 2001-10-26
- Based on premise that civil liberties prevented discovery of 9/11 plot

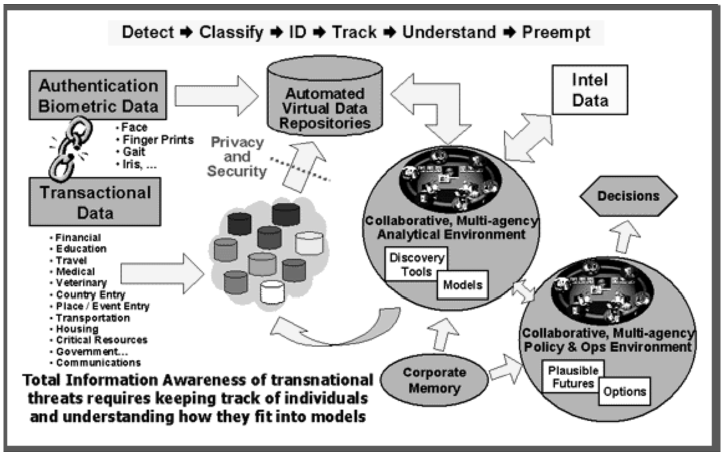
U.S.A.P.A.T.R.I.O.T. Act

- Warrant can be obtained *without providing evidence* to justify request
  - Inform any judge that surveillance is "*relevant*" to an investigation
  - Target need not be subject of investigation
  - No requirement to report findings to judge or to subject
  - Judge has only 2 choices under Act:
    - ✓Grant permission
    - ✓Accuse law enforcement of lying
- Easier surveillance in cases of suspected computer crime – some without court order

U.S.A.P.A.T.R.I.O.T. Act (cont'd)

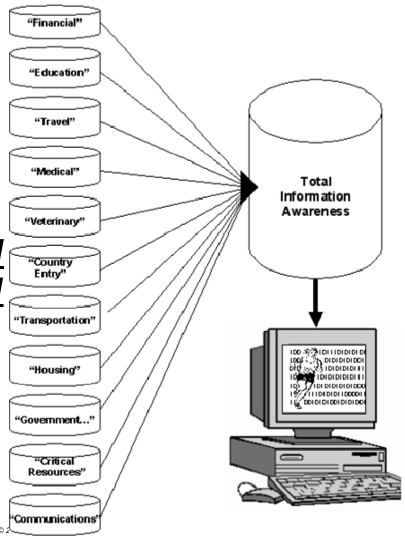
- Extension of Foreign Intelligence Surveillance Act (FISA)
  - Allows surveillance of US citizens and residents by CIA & NSA
- Information sharing between intelligence agencies and law enforcement
  - Had been separated after abuses in 1950s & 1960s
- Increased authority to Attorney General to circumvent restrictions on domestic surveillance limitations

Total Information Awareness (TIA) System http://www.darpa.mil/iao/TIASystems.htm


Detect ➡ Classify ➡ ID ➡ Track ➡ Understand ➡ Preempt
Authentication Biometric Data
• Face
• Finger Prints
• Gait
• Iris, ...
Transactional Data
• Financial
• Education
• Travel
• Medical
• Veterinary
• Country Entry
• Place / Event Entry
• Transportation
• Housing
• Critical Resources
• Government...
• Communications
Automated Virtual Data Repositories
Privacy and Security
Intel Data
Collaborative, Multi-agency Analytical Environment
Discovery Tools
Models
Decisions
Collaborative, Multi-agency Policy & Ops Environment
Plausible Futures
Options
Corporate Memory
Total Information Awareness of transnational threats requires keeping track of individuals and understanding how they fit into models

TIA (cont'd)

http://www.epic.org/privacy/profiling/tia/



TIA (cont'd)

- **Project funding shut down by Congress in September 2003**
- **Closed Pentagon's Information Awareness Office**
- **Student profiling continues under other programs**
  - ❑**See http://www.epic.org/privacy/student/**

Defending Privacy in Cyberspace

- **Technology**
  - ❑**Encryption**
  - ❑**Steganography**
  - ❑**Anonymizers**
- **Organizations**
  - ❑**Privacy International**
  http://www.privacyinternational.org
  - ❑**Electronic Privacy Information Center (EPIC) http://www.epic.org**
  - ❑**Center for Democracy and Technology http://www.cdt.org**
  - ❑**Electronic Frontier Foundation http://www.eff.org**

Reading about Privacy

- **Diffie, W. & S. Landau (1998). *Privacy on the Line - The Politics of Wiretapping and Encryption.* MIT Press (Cambridge, MA). ISBN 0-262-04167-7. 342 pp.**
- **Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century.* O'Reilly (Sebastopol, CA). ISBN 1-565-92653-6. vii + 312. Index.**
- **Nissenbaum, H. F. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford Law Books (Stanford, CA). ISBN 0-804-75237-0. 304 pp.**

Review Questions (1)

1. **Define different kinds of privacy (4)**
2. **What did Justice Louis Brandeis famously say about privacy? (1)**
3. **Does the US Constitution explicitly use the word "privacy"? (1)**
4. **Does the US Constitution protect privacy rights? Where? (4)**
5. **Explain how modern information technology has encroached upon privacy (10)**
6. **Contrast the US and European legal constraints on information about consumer behavior (4)**

Review Questions (2)

7. What is a “Web bug” and how does it affect privacy? (4)
8. What is “spyware?” Why do many people object to spyware? (4)
9. How has the U.S.A.P.A.T.R.I.O.T. Act changed US law concerning privacy rights? (10)
10. What is a “cookie” in information technology? Do cookies necessarily infringe privacy? Explain. (5)
11. Be prepared to give the names of key US laws protecting privacy given a brief description of the laws.

DISCUSSION