Professional Ethics for Computer Science

Lecture 4: Privacy

Klaus Mueller

Computer Science Department

Stony Brook University

Privacy Protection And The Law

Ethical conundrum:

- IT technology allows businesses to gather information
- must balance the needs of those who use this information against the privacy rights of those people whose information may be used

Systems collect and store key data from every interaction with customers

- purchasing habits, contacts, search terms, etc.

Many people object to data-collection policies of government and business

- strips people of the power to control their own personal information
- but IT does it on a regular basis….

Privacy Protection And The Law (cont.)

Privacy

- key concern of Internet users
- top reason why non-users still avoid the Internet (according to US Census data)

Reasonable limits must be set

- information and communication technologies must be developed to protect privacy, rather than diminish it

Historical perspective on the right to privacy

- Fourth Amendment (1789) - reasonable expectation of privacy
  protection against unreasonable searches and seizures

Key Privacy And Anonymity Issues

Government electronic surveillance

Data encryption

Identity theft

Customer profiling

Need to treat customer data responsibly

Workplace monitoring

Spamming

Advanced surveillance techniques

Governmental Electronic Surveillance

USA Patriot Act of 2001:

"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"

- passed just after 9/11
  - although more than 340 pages and quite complex, passed into law just five weeks after being introduced
- gives sweeping new powers to
  - domestic law enforcement wiretaps without court order
  - international intelligence agencies
- critics argue it removes checks & balances that previously gave courts opportunity to ensure that law enforcement agencies did not abuse their powers
- contains several "sunset" provisions for increased searches & electronic surveillance (terminated on 12/31/05)
- ammendment to FISA: Foreign Intelligence Surveillance Act

Key Provisions of USA Patriot Act Subject to Sunset

primarily those that modified Title III and FISA (allow government to conduct wiretaps w/out court order)

Section	Issue addressed	Summary
201	Wiretapping in terrorism cases	Added several crimes for which federal courts may authorize wiretapping of people's communications
202	Wiretapping in computer fraud and abuse felony cases	Added computer fraud and abuse to the list of crimes the FBI may obtain a court order to investigate under Title III
203 b	Sharing wiretap information	Allows the FBI to disclose evidence obtained under Title III to other federal officials, including "law enforcement, intelligence, protective, immigration, national defense, [and] national security" officials
203 d	Sharing foreign intelligence information	Provides for disclosure of threat information obtained during criminal investigations to "appropriate" federal, state, local, or foreign government officials for the purpose of responding to the threat
204	FISA pen register/trap-and-trace exceptions	Exempts foreign intelligence surveillance from statutory prohibitions against the use of pen register or trap-and-trace devices, which capture "addressing" information about the sender and recipient of a communication. It also exempts the U.S. government from general prohibitions against intercepting electronic communications and allows stored voice-mail communication to be obtained by the government through a search warrant rather than more stringent wiretap orders.
206	FISA roving wiretaps	Expands FISA to permit "roving wiretap" authority, which allows the FBI to intercept any communications to or by an intelligence target without specifying the telephone line, computer, or other facility to be monitored
207	Duration of FISA surveillance of non-U.S. agents of a foreign power	Extends the duration of FISA wiretap orders relating to an agent of a foreign power from 90 days to 120 days, and allows an extension in 1-year intervals instead of 90-day increments

Terms Used

Pen register:

- collects the outgoing phone numbers placed from a specific telephone line,

Trap and trace device

- captures the incoming numbers placed to a specific phone line
- for example, a caller-id box is a trap and trace device

First Amendment

- freedom of speech, etc.

Fourth Amendment

- right to be protected from unreasonable search, etc.

Conundrum

- puzzling question

Key Provisions of the USA Patriot Act Subject to Sunset (continued)

Section	Issue addressed	Summary
209	Seizure of voice-mail messages pursuant to warrants	Enables the government to obtain voice-mail messages under Title III using just a search warrant rather than a wiretap order, which is more difficult to obtain. Messages stored on an answering machine tape, however, remain outside the scope of this section.
212	Emergency disclosure of electronic surveillance	Permits providers of communication services (such as telephone companies and Internet service providers) to disclose consumer records to the FBI if they believe immediate danger of serious physical injury is involved. Communication providers cannot be sued for such disclosure.
214	FISA pen register/trap-and-trace authority	Allows the government to obtain a pen register/trap-and-trace device "for any investigation to gather foreign intelligence information." It prohibits the use of FISA pen register/trap-and-trace surveillance against a U.S. citizen when the investigation is conducted "solely on the basis of activities protected by the First Amendment."
215	FISA access to tangible items	Permits the FBI to compel production of any record or item without showing probable cause. People served with a search warrant issued under FISA rules may not disclose, under penalty of law, the existence of the warrant or the fact that records were provided to the government. It prohibits investigation of a U.S. citizen when it is conducted solely on the basis of activities protected by the First Amendment.
217	Interception of computer trespasser communications	Creates a new exception to Title III that permits the government to intercept the "communications of a computer trespasser" if the owner or operator of a "protected computer" authorizes it. It defines a protected computer as any computer "used in interstate or foreign commerce or communication" (because of the Internet, this effectively includes almost every computer).
220	Nationwide service of search warrants for electronic evidence	Expands the geographic scope where the FBI can obtain search warrants or court orders for electronic communications and customer records
223	Civil liability and discipline for privacy violations	Provides that people can sue the government for unauthorized disclosure of information obtained through surveillance
225	Provider immunity for FISA wiretap assistance	Provides immunity from lawsuits for people who disclose information to the government pursuant to a FISA wiretap order, physical search order, or an emergency wiretap or search

Data Encryption

Cryptography

- science of *encoding* messages
- only sender and intended receiver can understand the messages
- key tool for ensuring confidentiality, integrity, authenticity of electronic messages and online business transactions

Encryption

- process of converting electronic messages into a form understood only by the intended recipients

Data Encryption (continued)

Encryption key

- a (large random) value applied using an algorithm to encrypt or decrypt text
- length of key determines strength of encryption algorithm

Public key encryption system uses two keys: public and private key

- message recipient's *public* key
  - readily available and used for encryption
- message recipient's *private* key
  - mathematically related to public key
  - kept secret and used for decryption

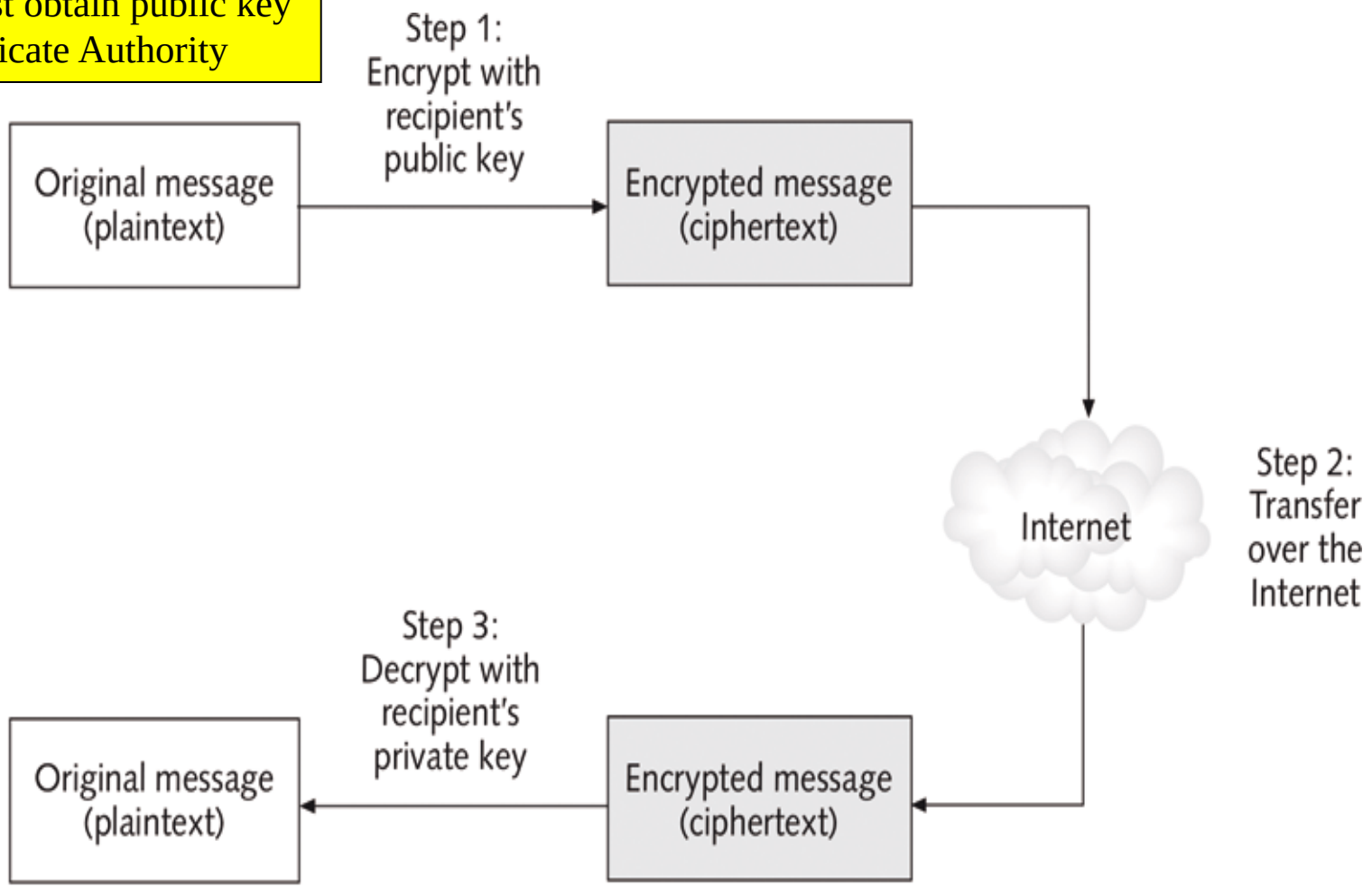
RSA - a public-key encryption algorithm (RSA keys typically 1024–2048 bits long)

Private key encryption system

- single key to encode and decode messages
- issue of secretly distributing private key to sender/receiver paramount

Public Key Encryption

Sender must obtain public key from Certificate Authority



Public key encryption

Only recipient can read message

Data Encryption (continued)

Despite potential management and administration headaches most people agree encryption eventually must be built into

- networks
- file servers
- tape backup systems

Seagate Technology hard drive

- automatically encrypts all data
- must know password to access data

U.S. Arms Export Control Act controls the export of encryption technology, hardware, and software

- violators face 10-year jail term and $1M fine

Identity Theft

Theft of key pieces of personal information to gain access to a person's financial accounts

- using this info, ID thief may apply for new credit or financial accounts, register for college courses, etc—all in someone else's name

Information includes:

- name
- address
- date of birth
- Social Security number
- passport number
- driver's license number
- mother's maiden name

Identity Theft (continued)

Fastest growing form of fraud in the United States

- victims spend >600 hours over several years recovering from ID theft

Lack of initiative by companies in informing people whose data was stolen

"*The personal information of 90,000 people in a Stony Brook University database was accidentally posted to Google & left there until it was discovered almost two weeks later*."

Phishing

- attempt to steal personal identity data
- by tricking users into entering information on a counterfeit Web site (spoof emails)
- spear-phishing - a variation in which employees are sent phony e-mails that look like they came from high-level executives within their organization

Identity Theft (continued)

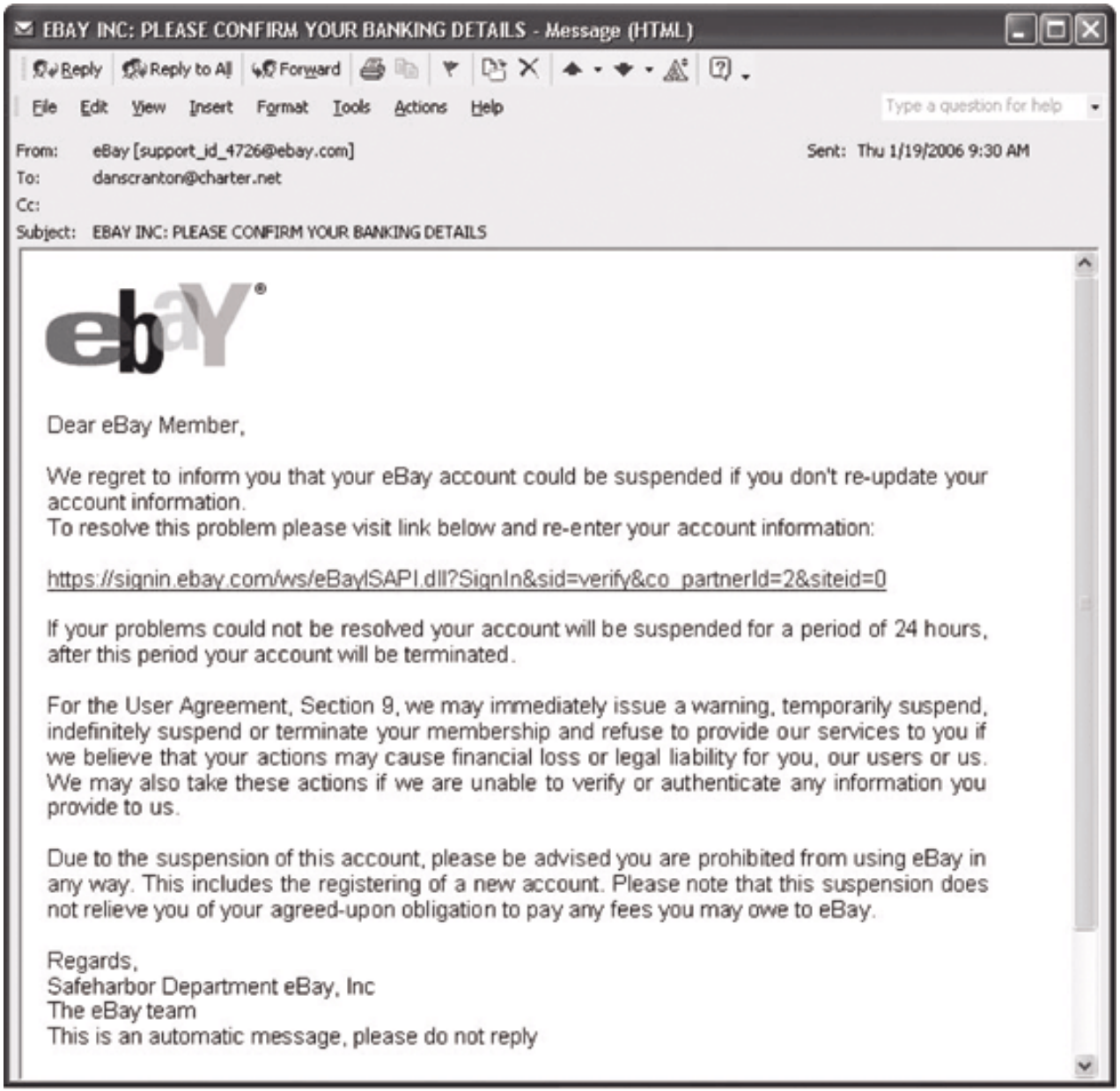
Spyware

- keystroke-logging software downloaded to user's computer without consent
- enables the capture of:
  - account usernames
  - passwords
  - credit card numbers
  - other sensitive information
- operates even if an infected computer is not connected to the Internet
- records keystrokes until users reconnects; data collected then emailed to spy or posted to a web site

Identity Theft and Assumption Deterrence Act of 1998 was passed to fight Identity fraud

- makes it a Federal felony (3-25 yrs in prison)

E-mail Used by Phishers



EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS - Message (HTML)

Reply | Reply to All | Forward

File Edit View Insert Format Tools Actions Help

Type a question for help

From: eBay [support_id_4726@ebay.com]
Sent: Thu 1/19/2006 9:30 AM
To: danscranton@charter.net
Cc:
Subject: EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Consumer Profiling

Companies can collect info about consumers without their explicit permission!

Companies openly collect personal information about Internet users

- when they register at web sites, complete surveys, fill out forms or enter contests online

Cookies

- text files a web site places on user's hard drive so that it can remember info
- examples: site preferences, contents of electronic shopping cart
- cookie are sent back to server unchanged by browser each time it accesses that server

Tracking software

- identify visitors to your web site from e.g. pay-per-click accounts

Consumer Profiling (continued)

Similar methods used outside the Web environment

- marketing firms warehouse consumer data
- foer example, credit card purchases, frequent flier points, mail-order catalogue purchases, phone surveys

Databases contain a huge amount of consumer behavioral data

Affiliated Web sites:

- group of web sites served by single advertising network
- DoubleClick tracks ad clicks and web purchases: useful for marketers and sellers

Customized service for each consumer

- marketers use cookies to recognize return visitors and store useful info about them

Consumer Profiling (continued)

Types of data collected while surfing the Web

- GET data: affiliated web sites visited and info requested
- POST data: form data
- Click-stream data: monitoring of consumer surfing activity

Four ways to limit or even stop the deposit of cookies on hard drives

- set the browser to limit or stop cookies
- manually delete them from the hard drive
- download and install a cookie-management program
- use anonymous browsing programs that don’t accept cookies
    - e.g. anonymizer.com allows you to hide your identity while browsing

Consumer Profiling (continued)

Personalization software used by marketers to optimize number, frequency, and mixture of their ad placements

- ***Rules-based:***

  uses business rules tied to customer-provided preferences or online behavior to determine most appropriate page views
- ***Collaborative filtering:***

  consumer recommendations based on products purchased by customers with similar buying habits
- ***Demographic filtering:***

  considers user zip codes, age, sex when making product suggestions
- ***Contextual commerce:***

  associates product promotions/ads with content user is currently viewing

Platform for Privacy Preferences (P3P)

- shields users from sites that don't provide desired level of privacy protection
- P3P software in a browser will download privacy policy for each site visited and notify users if policy does not match their preferences

Treating Consumer Data Responsibly

Strong measures are required to avoid customer relationship problems

Code of Fair Information Practices and 1980 OECD privacy guidelines

- companies collect only personal info necessary to deliver its products/services
- protects this info
- informs customers if it intends to use this info for research or marketing
- provides a means for customers to opt out

Chief privacy officer (CPO)

- executive to oversee data privacy policies and initiatives
- avoids violating government regulations and assures customers that their privacy will be protected

Manager's Checklist for Treating Consumer Data Responsibly

Questions	Yes	No
Do you have a written data privacy policy that is followed?	___	___
Can consumers easily view your data privacy policy?	___	___
Are consumers given an opportunity to opt in or opt out of your data policy?	___	___
Do you collect only the personal information needed to deliver your product or service?	___	___
Do you ensure that the information is carefully protected and accessible only by those with a need to know?	___	___
Do you provide a process for consumers to review their own data and make corrections?	___	___
Do you inform your customers if you intend to use their information for research or marketing and provide a means for them to opt out?	___	___
Have you identified a person who has full responsibility for implementing your data policy and dealing with consumer data issues?	___	___

Workplace Monitoring

Ethical conundrum

- ensure worker productivity without violating privacy rights of employees

Employers monitor workers

- record email, surfing activity, files, even videotaping employees on the job
- ensures that corporate IT usage policy is followed

Fourth Amendment cannot be used to limit how a private employer treats its employees

- public-sector employees have far greater privacy rights:

  "reasonable expectation of privacy" *Katz v. U.S.* 1998 Supreme Court ruling

Privacy advocates want federal legislation

- to keep employers from infringing upon privacy rights of employees
- inform employees of electronic monitoring devices; restrict type of info collected

Spamming

Transmission of same e-mail message to *large* number of people

Extremely inexpensive method of marketing

- $1K vs. $10K for direct-mail campaign
- 3 weeks to develop vs. 3 months
- 48hrs for feedback vs. 3 weeks

Used by many *legitimate* organizations

- example: product announcements

Can contain *unwanted and objectionable* materials

Last 2 bullets point to the ***ethical conundrum***!

Email considered Spam: 40% of all email; **Daily Spam emails sent**: 12.4 billion; **Daily Spam received per person**: 6; **Annual Spam received per person**: 2,200; **Spam cost to all non-corp Internet users**: $255 million; **Spam cost to all U.S. Corporations in 2002**: $8.9 billion: **States with Anti-Spam Laws**: 26

Spamming (continued)

The ***Controlling the Assault of Non-Solicited Pornography and Marketing*** (CAN-SPAM) Act 2004

- says it is legal to spam but
  - spammers cannot disguise their identity
  - there must be a label in the message specifying that the e-mail is an ad or solicitation
  - they must include a way for recipients to indicate they do not want future mass mailings (i.e. opt out)
- may have actually *increased* the flow of spam as it legalizes the sending of unsolicited e-mail

Advanced Surveillance Technology

Provides exciting new data-gathering capabilities vs. personal-privacy issues

- **advocates**: people have no legitimate expectation of privacy in public places
- **critics**: creates potential for abuse – intimidation of political dissenters, blackmail of people caught with "wrong" person or in "wrong" place

Camera surveillance

- U.S. cities plan to expand surveillance systems

  London has one of world's largest public surveillance systems
- "Smart surveillance system"

  singles out people acting suspiciously

Facial recognition software

- identifies criminal suspects and other undesirable characters
- yields mixed results

  at Boston's Logan airport: 96 failures, 153 successes

Advanced Surveillance Technology (continued)

Global Positioning System (GPS) chips

- Placed in many devices to precisely locate users
    - cars, cellphones, etc.
- **Good**: accurately respond to 911 callers; real-time location-aware marketing
- **Bad**: wireless spamming from local restaurants etc, your whereabouts always known

Summary

Legal concept of right to privacy has four aspects

- web-surfing private, ID theft, HIPPA, false info about someone on web

Number of laws have been enacted over past 40 years that affect a person's privacy

- FISA 1978 (wiretapping aliens)
- ECPA 1986 (set standards access to stored email & other electronic communication
- US PATRIOT Act 2001
- these (and other) laws authorize electronic surveillance by the government

Data encryption

- public key encryption system
- private key encryption system

Identity theft

Summary (continued)

Consumer behavior data is collected both online and offline

- recall: consumer profiling

Code of Fair Information Practices and 1980 OECD privacy guidelines

- protect consumer data orgs only collect personal info necessary to deliver product or service

Employers record and review employee communications and activities on the job

- recall: workplace monitoring

Advances in information technology for Surveillance

- surveillance cameras
- facial recognition software
- GPS systems