Bynum ethical analysis – EMAILFUNDER

- E_researcher
- E_profiler
- E-writer

Analysis

- Participants and their actions:
  - Joe Biggheart
  - Recipients of messages
  - Software engineers
  - Training leaders
  - Prosecutors/ suitors
- Agents
  - E_RESEARCHER, E-PROFILER, E-WRITER

Ethical questions

- Joe created an email who caused harm to people. Who is to blame? Was harm intentional or unintentional?
- If harm unintended, was anyone negligent or irresponsible? Or was this unpreventable accident?

- Precedents and similarities – blackmail?
- Objectors?
  - Email recipients, Fund workers, children with cancer, JoeCharityBot.com staff members and owners
- Interim conclusions
  - Joe did not intend to harm anyone, but should have been more persistent with his worries
  - CharityBot.com did not take risks of using softbots seriously. Not enough quality control (“lust”), not enough attention to problems brought up by customers

- Policy gaps – softbot responsibility/ethics
- Professional standards analysis
- Roles and responsibilities analysis
  - Joe Biggheart
  - Training leaders
  - non-human agents
- stakeholders analysis: email recipients, children

- Conclusions
  - Primary cause
  - Contributing factors
  - Privacy
  - Agent ethics
  - Jurisdiction of ethics?

Another example – Fosbakk $100K case

- Read the article ”losing $100K”
- Analyze it using the Bynum methodology
  - First the 6 point analysis
  - Then the extended analysis
  - Make use of the research described in the article

Privacy

We will cover:

- General discussion
- Technology to protect privacy
- Canadian Internet privacy context

Privacy - What We Will Cover

- Privacy and Computer Technology
- “Big Brother is Watching You”
- Privacy Topics
- Protecting Privacy
- Communications

Privacy and Computer Technology

Key Aspects of Privacy:

- Freedom from intrusion (being left alone)
- Control of information about oneself
- Freedom from surveillance (being tracked, followed, watched)

Privacy and Computer Technology (cont.)

New Technology, New Risks:

- Government and private databases
- Sophisticated tools for surveillance and data analysis
- Vulnerability of data

Privacy and Computer Technology (cont.)

Terminology:

- Invisible information gathering - collection of personal information about someone without the person's knowledge
- Secondary use - use of personal information for a purpose other than the one it was provided for

Privacy and Computer Technology (cont.)

Terminology (cont.):

- Data mining - searching and analyzing masses of data to find patterns and develop new information or knowledge
- Computer matching - combining and comparing information from different databases (using social security number, for example, to match records)

Privacy and Computer Technology (cont.)

Terminology (cont.):

- Computer profiling - analyzing data in computer files to determine characteristics of people most likely to engage in certain behavior

Privacy and Computer Technology (cont.)

Principles for Data Collection and Use:

- Informed consent
- Opt-in and opt-out policies
- Fair Information Principles (or Practices)
- Data retention

Privacy and Computer Technology Discussion Questions

- Have you seen opt-in and opt-out choices? Where? How were they worded?
- Were any of them deceptive?
- What are some common elements of privacy policies you have read?

"Big Brother is Watching You"

Databases:

- In Canada, Privacy Commissioners (federal - Jennifer Stoddard - and provincial – Ann Cavoukian in Ontario) - monitor government's privacy policies and privacy violations

"Big Brother is Watching You" (cont.)

Video Surveillance:

- Security cameras
  - Increased security
  - Decreased privacy

"Big Brother is Watching You" (cont.)
Discussion Questions

- What data does the government have about you?
- Who has access to the data?
- How is your data protected?

Diverse Privacy Topics

Marketing, Personalization and Consumer Dossiers:

- Targeted marketing
  - Data mining
  - Paying for consumer information
  - Data firms and consumer profiles
- Credit records

Diverse Privacy Topics (cont.)

Location Tracking:

- Global Positioning Systems (GPS) - computer or communication services that know exactly where a person is at a particular time
- Cell phones and other devices are used for location tracking
- Pros and cons

Diverse Privacy Topics (cont.)

Stolen and Lost Data:

- Hackers
- Physical theft (laptops, thumb-drives, etc.)
- Requesting information under false pretenses
- Bribery of employees who have access

Diverse Privacy Topics (cont.)

What We Do Ourselves:

- Personal information in blogs and online profiles
- Pictures of ourselves and our families
- File sharing and storing
- Is privacy old-fashioned?
  - Young people put less value on privacy than previous generations
  - May not understand the risks

Diverse Privacy Topics (cont.)

Public Records: Access vs. Privacy:

- Public Records - records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)
- Identity theft can arise when public records are accessed
- How should we control access to sensitive public records?

Diverse Privacy Topics (cont.)

National ID System:

- Social Security Numbers
  - Too widely used
  - Easy to falsify

Diverse Privacy Topics (cont.)

National ID System (Cont.):

- A new national ID system - Pros
  - would require the card
  - harder to forge
  - have to carry only one card
- A new national ID system - Cons
  - Threat to freedom and privacy
  - Increased potential for abuse

Diverse Privacy Topics (cont.)

Children:

- The Internet
  - Not able to make decisions on when to provide information
  - Vulnerable to online predators
- Parental monitoring
  - Software to monitor Web usage
  - Web cams to monitor children while parents are at work
  - GPS tracking via cell phones or RFID

Diverse Privacy Topics Discussion Questions

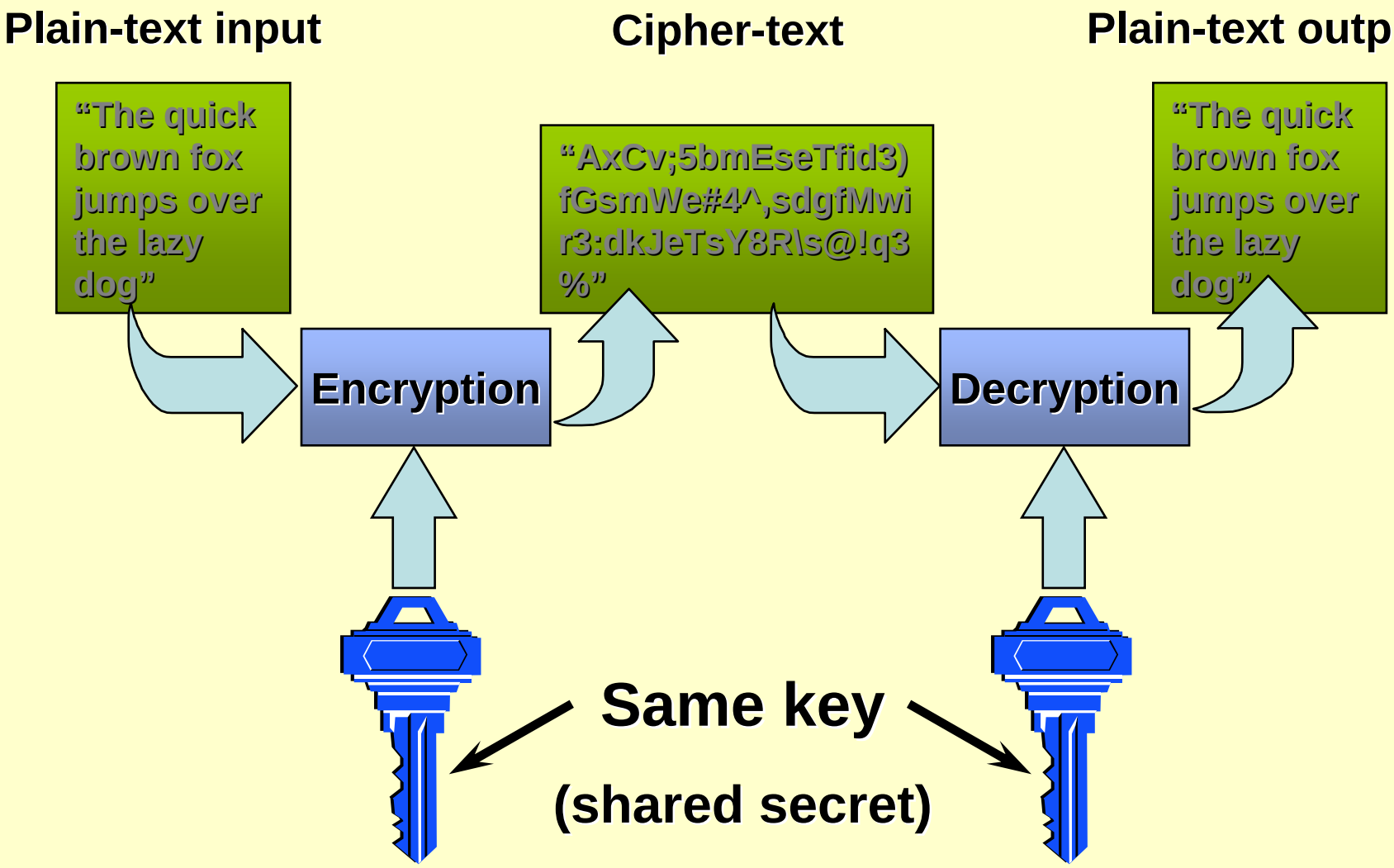
- Is there information that you have posted to the Web that you later removed? Why did you remove it? Were there consequences to posting the information?
- Have you seen information that others have posted about themselves that you would not reveal about yourself?

Protecting Privacy

Technology and Markets:

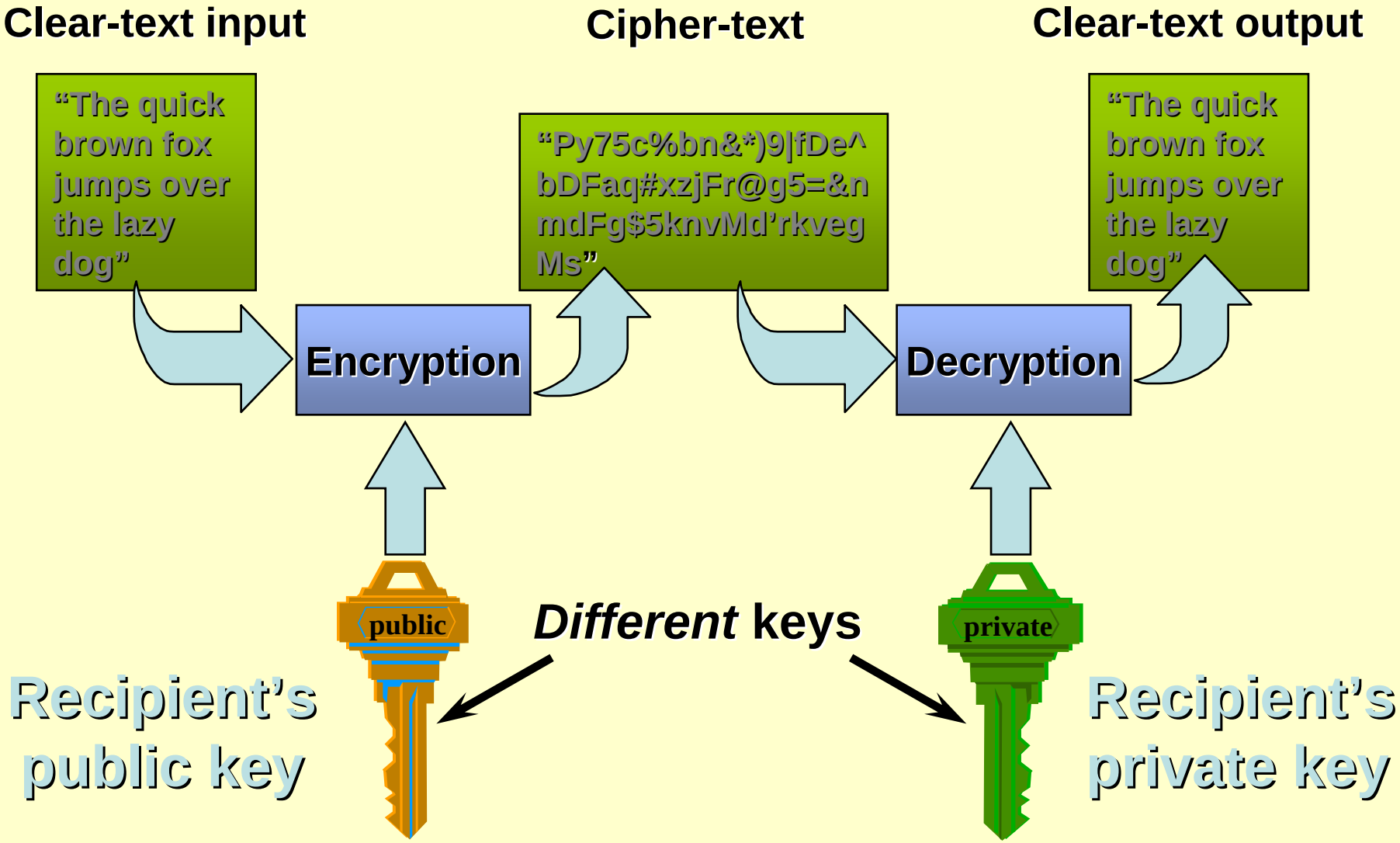
- Privacy enhancing-technologies for consumers
- Encryption
  - Public-key cryptography
- Relationship between privacy and security
- Business tools and policies for protecting data

Symmetric Key Encryption



Following [Kalakota]

Public Key Encryption



Protecting Privacy (cont.)

Rights and laws: Contrasting Viewpoints:

- Free Market View
  - Freedom of consumers to make voluntary agreements
  - Diversity of individual tastes and values
  - Response of the market to consumer preferences
  - Usefulness of contracts
  - Flaws of regulatory solutions

Protecting Privacy (cont.)

Rights and laws: Contrasting Viewpoints (cont.):

- Consumer Protection View
  - Uses of personal information; opt-in *vs* opt-out
  - Costly and disruptive results of errors in databases
  - Ease with which personal information leaks out
  - Consumers need protection from their own lack of knowledge, judgment, or interest

Protecting Privacy (cont.)

Privacy Regulations in the European Union (EU):

- Data Protection Directive
  - More strict than U.S. regulations
  - Abuses still occur
  - Puts requirements on businesses outside the EU

Protecting Privacy
Discussion Question

- How would the free-market view and the consumer protection view differ on errors in Credit Bureau databases?
- Who is the consumer in this situation?

Communication
Discussion Questions

- What types of communication exist today that did not exist in 1968 when wiretapping was finally approved for law-enforcement agencies?
- What type of electronic communications do you use on a regular basis?

Moor's privacy paper

- "greased" data – pizza example

http://www.youtube.com/watch?v=-zh9fibMaEk

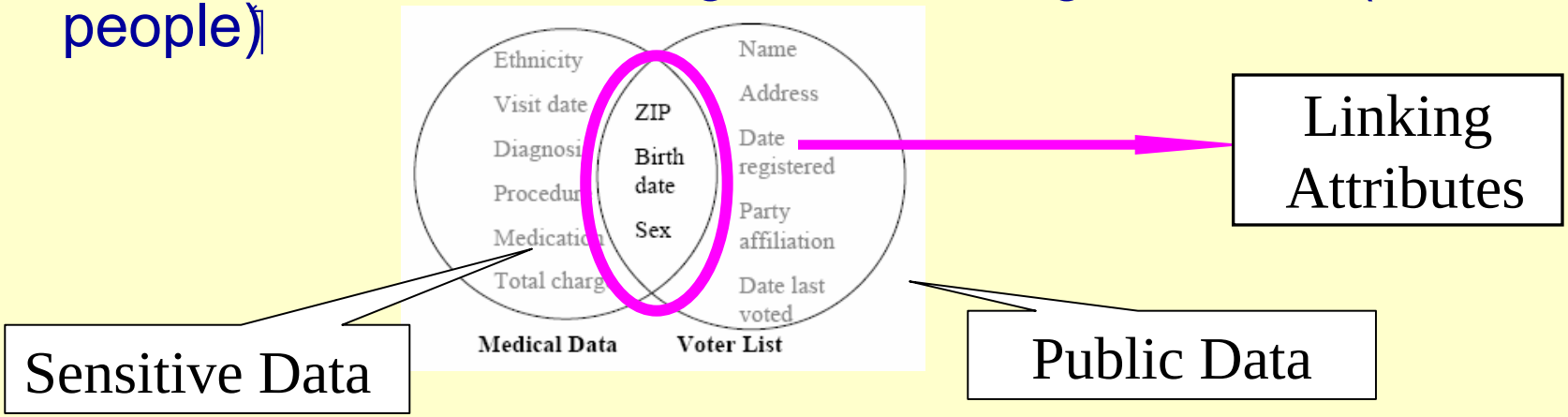
- Privacy justification – instrumental, intrinsic, core values
  - Life, happiness, freedom, knowledge, ability, resources, security
  - Privacy as *an expression* of security (peeping Tom example)
- Moor's "control/restricted access" definition of privacy: a person can decide who knows what and when about that person

- Database definition of privacy
  - We are a database of facts about oursevkles, we own that databse
  - Privacy is the ability to define **views** of that database for different recipients
- Privacy is necessary to enter into meaningful social relationships with people and organizations

…more precisely

- Privacy preservation: what does that mean?
- Given a table of instances (rows), we cannot associate any instance with a given person
- Naive anonymization…
- …is not sufficient, due to pseudo-identifiers

- L. Sweeney published this « attack » in 2001:
- **anoymized** (*de-linked*) health records of all 135,000 employees+families of the state of Massachussetts was placed on-line
- Electoral list of Cambridge, MA – bought for $20 (54 805 people)



- 69% records are unique wrt birthdate, ZIP; 87% are unique wrt to bday, ZIP, sex…
- Governor's health records were identified
- …naive anonymization is not sufficient

Other privacy fiascos

- AOL search engine queries published

  2006
- Netflix publicly released a data set containing movie ratings of 500,000 Netflix subscribers *between December* 1999 and December 2005.
- By matching no more than 8 movie ratings and approximate dates, 96% of subscribers can be uniquely identified.

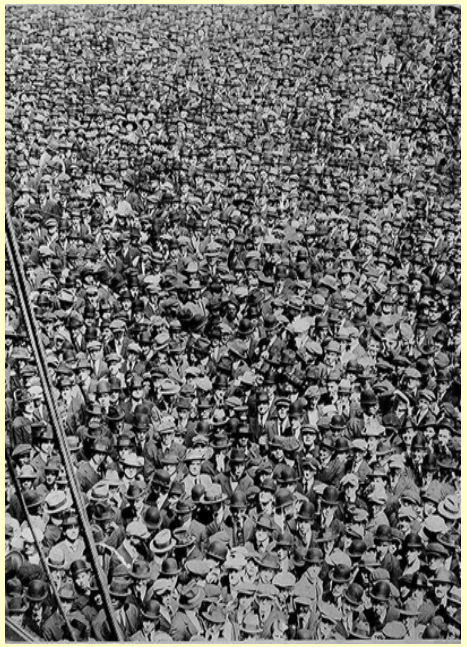
PET-PPDM

- Privacy-enhancing technologies (PET)
- Privacy-preserving Data Mining (PPDM)

camouflage

Data modification/ perturbation

hiding in the crowd



k-anonymization