Privacy and Anonymity

Steven M Bellovin

Course Outline

- Legal framework (US and European)
- Data mining and databases
- Anonymous commerce (digital cash)
- Anonymous use of the Internet (onion routing, anonymous browsing, P3P)
- Traffic analysis
- Biometrics and authentication
- Policy and national security considerations
- Possible occasional interruptions to the schedule to read about and discuss privacy-related current events

Class Structure

- Student presentations of assigned reading material (50% of the grade)
- Class discussion of the reading material (25%)
- A 5–10 page paper (25%), plus
- In-class presentation (during one of the last two class meetings) of your paper.

Presentations

- Everyone should be prepared to present each paper
- Email me your presentation or notes by the start of each class. (Note: Postscript, PDF, HTML, or ASCII preferred; Powerpoint is sometimes problematic for me, especially if fancy, since I'm not a Windows user.)
- Presentations turned in up to one week late accepted at 50% credit
- You *don't* need to use slides, Powerpoint, etc. You do need to turn in something to me
- If you do, you can use either my laptop or your own. If you want to use mine, be certain to email the slides to me no later than 3:00pm, so that I can verify that I can display them

Presenting a Paper

- 15–20 minute summary of the work. Act as if your audience has not read the paper
- 5-10 minutes of your reaction, evaluation, lessons, etc.
- 5-10 minutes of class discussion

The Paper

Think of it as an take-home essay exam where you pick the question. This is not expected to be original research. It is intended to show me that you understand the material.

The easiest approach is to take one topic that I've covered, read the listed papers carefully *plus others you find yourself*, and produce a survey paper on that subject. Another approach is to do a detailed case study of some issue or implemented solution. Feel free to suggest your own topics, too, but please confirm the selection with me, either in person during my office hours or by email. I would expect the length to be about 5-10 pages.

The written paper is due when the final for this class would be held.

Presenting Your Own Paper

- 12-15 minute presentation of the work
- 5 minutes of class discussion
- Bonus credit for those who present in the first session, since they have one less week to work on it

Contacting Me

- Email is by far the best way to reach me outside of office hours
- I travel a fair amount, and rarely check voice mail when on the road
- If you need to see me and can't make it during my office hours, email me to set up an appointment
- Given the vagaries of NJ Transit's schedules, I am generally not available after class
- Exceptions to my office hours will be posted on my web page: `http://www.cs.columbia.edu/~smb`

Discussing Legal Works

- This is not a law class
- We are not interested in the legal minutae or in a critique of the legal reasoning
- We are interested in the broad foundations of legal decisions, their effects, and on how these decisions and laws interact with technology

Biases

Many of the assigned readings assume that privacy is a benefit, and should be protected to the extent possible.

"You have zero privacy anyway. Get over it".
—Scott McNealy
CEO, Sun Microsystems

I'm an unabashed privacy advocate. But the course is not about *promoting* privacy, and I don't expect you to agree with me. The course is about understanding privacy, its context, how to achieve it if you want it, and what the drivers are against privacy.

Other Issues?

Legal Research

- `http://www.findlaw.com` — statutes, cases, etc.
- `http://www.law.cornell.edu` — similar
- LexisNexis, via CU library — comprehensive, annotated, complex
- `http://www.lib.uchicago.edu/~llou/mpoctalk.html` — research guide
- `http://thomas.loc.gov` — good for bills currently before Congress
- Many, many more

Legal Notation: Court Cases

United States v Morris (1991, CA2 NY) 928 F2d 504

United States v Morris Common name; lists parties to the case

1991 Year of the decision

CA2 NY Court of Appeals, Second Circuit, New York

928 F.2d 504 Volume 928, page 504, of the Federal Reporter, Second Series (yes, cases are cited by page number!)

See `http://www.faqs.org/faqs/law/research/part1/` for more details

Similar formats are used even when referring to cases from other countries: Semayne's Case, 5 C. Rep. 91a, 77 Eng. Rep. 194 (K.B. 1603).

Legal Notation: U.S. Code

18 USC 1030 (Computer Fraud and Abuse Act)

18 Title 18 of the U.S. Code (Crimes and Criminal Procedure)

USC U.S. Code or other body of laws or regulations ("CFR" is the Code of Federal Regulations)

1030 Section 1030

Computer Fraud and Abuse Act The common name. Strictly speaking, it applies to the *Public Law* that created that section (or made major amendments to it)

The U.S. Code is the orderly compilation; sections are created and amended by Public Laws: P.L. 98-473, Title II, Ch XXI, §2102(a), 98 Stat. 2190.

Late-breaking news…

- http://www.boston.com/business/technology/articles/2005/01/17/gps_spying_may_prove_irresistible_to_police/
- http://www.vnunet.com/news/1160618

Privacy Challenges in Authentication Systems

Context

- National Research Council report
- Committe composed of computer scientists (including me), lawyers, human factors experts, biometrics experts
- Report is *not* the result of original research by the commitee
- This chapter provides a legal and societal framework for privacy

Privacy Impact of the Decision to Authenticate

- Registration may require disclosure of personal facts or information
- Authenticating may cause creation of records
- Details of an event can augement these records
- Even without personally identifiable information, a dossier can be compiled
- Others may have access to this information

Access Control Systems

- What sort of access is mediated, and when? Are people aware of the borders or the access control? Differs in physical and online worlds.
- Computer technology reduces cost of record keeping
- Computer technology facilitates linkage
- Computer technology enables covert identification on a large scale (think red light cameras)

Legal Foundations of Privacy

- Common law: “[T]he house of every one is to him as his castle and fortress.” Semaynes Case, 5 C. Rep. 91a, 77 Eng. Rep. 194 (K.B. 1603)
- Doesn’t work as well in today’s interconnected world
- Types of privacy:
  - Bodily integrity
  - Decisional privacy
  - Information privacy
  - Communications privacy

Constitutional Roots

- Limits on government actions; does not apply to private behavior
- The word “privacy” is not mentioned in the U.S. Constitution
- A right to privacy is inferred from other provisions
- First Amendment: anonymous speech has a long history; right to receive information also protected
- Fourth Amendment: warrants and probable cause required for searches. Held in 1967 to encompass wiretaps
- Fifth Amendment: note distinction between testimonial evidence and physical evidence
- Ninth Amendment: states that other rights exist

Common Law Roots

- Tort law provides (some) recourse for private misbehavior
- Prosser (1960) defined four separate privacy torts:
  - Intrusion upon seclusion (including private affairs)
  - Public disclosure of private facts
  - Publishing objectionable, false information
  - Misappropriation of name or likeness
- Useful (in this report) as a reminder of what people expect to be protected

Statutory Protections

- Federal Trade Commission has the power to enforce voluntary privacy statements
- Piecemeal statutes protect some privacy, often in response to market failure or narrow court rulings.
- Often regulate private sector behavior; sometimes constrain government
- 11 different federal laws contrain private sector; much personal information is freely available for sale, including to the government
- Personal information voluntarily given to businesses not protected by the Fourth Amendment

Fair Information Practices

- First “code of fair information practices” developed in 1973 at HEW
- Basic rules for minimizing information collection, ensuring due process, protection against secret collection, provide security, ensure accountability
- Emphasize individual knowledge and consent
- Principles are broadly accepted, but individual principles not implemented uniformly

Fair Information Principles and Practices

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security
- Openness/notice
- Individual participation
- Accountability

Privacy of Communications

- Law recognizes need for privacy in new forms of communication
- Need is both value-driven and pragmatic
- Balance between privacy and law enforcement needs
- Protection for new communication mechanisms not as strong as for voice

Conclusions

- Authentication can affect all forms of privacy
- Authentication systems should not infringe on autonomy and legal rights. They should recognize the need for multiple identities
- Fair information practices should be followed