Overview of Online Privacy Policies

CYBR 4400/5400: Principles of Internet Policy, Lecture 5-1

Dr. David Reed, Technology, Cybersecurity, and Policy Program, CU Boulder

Today's Lecture

- Unit 4 Wrap-up
- Unit 5 Roadmap
- Online Privacy Policies Lecture

Spectrum Unit Wrap-up: Learning Outcomes

1. Explain the need for regulation of spectrum and how it is has been regulated in the past.

- Spectrum is a scarce resource, owned by the public
- Need to prevent harmful interference
- Regulate access to spectrum under “public interest, convenience, and necessity” standard

2. Understand how modern spectrum management practices are applied to support mobile wireless applications and how technologies have required these practices to change over time

- Categories: Allocation, Service Rules, Assignment, Enforcement

- Spectrum usage models: Exclusive Use (licensed), Commons (unlicensed), and Command & Control

  - Circumstances (spectrum scarcity, transactions costs, public interest) favoring each model

- Technologies permitting more spectrum sharing via time, space, and location (white spaces)

3. Explain the economics of spectrum scarcity, and how this impacts the market for mobile services and how they are regulated

- Economics applied to spectrum auctions (promote competition, policy instruments)
- Coase's Law applied to interference
- Internalizing opportunity costs

Unit 5: Privacy on the Internet — Tracking the Policy Solution

- Learning outcomes
  - Explain modern practices recommended by the FTC for protecting consumer information consistent with Fair Information Practice Principles (FIPPS)
  - Explain the new European Union's General Data Protection Regulations (GDPR)
  - Explain the economics of privacy, and how this impacts measurement of consumer online usage patterns and behaviors
  - Develop policy position on whether the FTC should pass new regulations governing the collection and use of consumer information through the application of the interdisciplinary policy framework

Defining Privacy

Defining Privacy

- Privacy (rough definition)

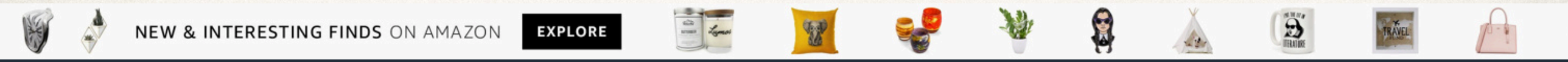
  Ability (or maybe the 'right') of an individual to control their exposure to the rest of the world, and to be able to hide information about themselves

- Impact of new Information Technologies such as digital storage, processing, retrieval, and distribution
  - Enormous cost reductions and massive adoption
  - Combine, re-use, re-purpose data (data mining)
  - Ability to process data using artificial intelligence (analytics)
- Raises concerns over use of Personally Identifiable Information (PII)
- Society's needs sometimes trump individual privacy

Privacy and Law

- No constitutional right to privacy
  - The word “privacy” is not in the Federal Constitution
  - Congress has passed numerous laws
    - Effectiveness under constant debate
    - Problems due to growth of ad-based business models on Internet, trends in data analytics and artificial intelligence
- Privacy is a function of culture, means different things in different countries
  - Major differences hold implications for global Internet

Amazon's Privacy Notice



Help & Customer Service

Search H | Go

‹ All Help Topics

Legal Policies

- Conditions of Use
- EU-US Privacy Shield
- Amazon.com Privacy Notice
- Amazon Group Companies
- Supported Browsers
- About Identifying Whether an E-mail is from Amazon
- Report a Security Issue
- Supply Chain Standards
- Public PGP Key
- Non-Exhaustive List of Applicable Amazon Patents and Applicable Licensed Patents
- Non-Exhaustive List of Amazon Trademarks
- Guidelines: Uploading Your Own Content to an electronic Amazon.com Gift Card or Other Electronic Message

Quick solutions

Your Orders
Track or cancel orders

Security & Privacy › Legal Policies ›

Amazon Privacy Notice

Last updated: August 29, 2017. To see what has changed, click here.

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

What Personal Information About Customers Does Amazon.com Gather?

The information we learn from customers helps us personalize and continually improve your Amazon experience. Here are the types of information we gather.

Collecting Personal Information

- Often voluntary
  - Filling out a registration form
  - Registering for a prize
  - Supermarket “Rewards” programs
- Legal, involuntary sources
  - Demographics
  - Change of address
  - Various directories
  - Government records

Complications

- Lots of information floating about online
  - How should we handle concerns over use of this information?
    - Who should have access to PII? Who should know?
- Consumers can benefit from sharing information
- Consumers may be harmed from sharing information
- How much should be shared and who should decide?
  - Some laws exist that try to draw this line

Flash Drill for Discussion on Wednesday!

- Download your Facebook, Amazon, or Google data
  - Just search web for instructions
- Examine the data that is provided to you
- Next class, come prepared to discuss the following:
  - Easy to understand?
  - Biggest surprises that you want to share

Some U.S. Privacy Laws

Year	Title	Intent
1970	Fair Credit Reporting Act	Limits the distribution of credit reports to those who need to know.
1974	Privacy Act	Establishes right to be informed of personal information on government databases.
1978	Right to Financial Privacy Act	Prohibits federal government from examining personal financial accounts without due cause.
1986	Electronic Communications Privacy Act	Prohibits federal government from monitoring personal e-mail without a subpoena.
1988	Video Privacy Protection Act	Prohibits disclosing video rental records without customer consent or a court order.
1994	Communications Assistance for Law	Enhance lawful interception by requiring built-in capabilities in telecom equip. for targeted surveillance
2001	Patriot Act	Streamlines federal surveillance guidelines to simplify tracking possible terrorists.

Children's Online Privacy Protection Act (COPPA) of 1998

- Enforcement and regulations by Federal Trade Commission
- What responsibilities operator has to protect children's privacy and safety online
- Post clear and comprehensive privacy policy of information practices for PII
- Provide direct notice to parents and obtain verifiable parental consent before collection
- Give parents choice of consenting to collection and internal use of PII, but prohibiting disclosing data to third parties
- Provide parents access to their child's PII to review and/or have data deleted

Children's Online Privacy Protection Act (COPPA) of 1998 (cont'd)

- Give parents opportunity to prevent further use or online collection of child's PII
- Maintain confidentiality and security of PII, including taking reasonable steps to release PII only to parties capable of maintaining its confidentiality and security
- Retain PII for only as long as necessary to fulfill purpose for which it was collected, delete using reasonable measures to protect against unauthorized access or use
- FTC revised rules in 2012 to require parental consent for use of:
  - Geolocation data, photos or videos containing a child's image, audio files with a child's voice, screen or online user name
  - Persistent identifier that collects information about a child's activities on its website or online service

FTC Proposal: Do Not Track

- Universal, persistent opt-out across all web sites
- Easy for consumers to find, understand and use
- Enforceable: reduces technical loopholes, compliance can be measured
- The Battle Over Do Not Track

User-Centric Privacy

- More complex “subscription” mechanism (risks alienation)
- Ideal would be software-negotiation, based on user-preferences and machine-readable statement of privacy policies
- Does assume that the consumer can make an informed decision
- P3P (Platform for Privacy Preferences Project in W3C)
  - Language for defining privacy policies (and for expressing private information and privacy statements)
  - Failed effort to date
- Inrupt/Solid (decentralized web where consumers own their data)

Federal Trade Commission: Protecting Consumer Privacy in an Era of Rapid Change

FTC Objectives and Focus

- Section 5 of FTC Act prohibits deceptive practices affecting commerce resulting in focus upon:
  - Transparency
  - Honoring consumers' expectations about the use of their PII
  - Choices by consumers about sharing PII
  - Obligation of companies that collect PII to adopt reasonable data security practices

FTC Privacy Framework

- Privacy by design — build in privacy at every stage of product development

- Simplified choice for consumers — Give consumers ability to make decisions about their data at a relevant time and context, including by Do Not Track mechanism

- Greater transparency — Make information collection and use practices transparent

Fair Information Practice Principles (FIPPS)

- Created in 1974 as part of the Privacy Act, although not in themselves law, form backbone of privacy law in the United States

Transparency
- There shall be no personal-record systems whose existence is secret.

Choice
- Individuals have rights of access, inspection, review, and amendment to systems containing information about them.

Information Protection
- There must be a way for individuals to prevent information about themselves gathered for one purpose from being used for another purpose without their consent.

Data Protection
- Organizations and managers of systems are responsible for the reliability and security of their systems and for the damage done by them.

Accountability
- Governments have the right to intervene in the information relationships among private parties.

FTC Privacy Framework

Factor	Description
Scope	All commercial entities that collect or use consumer data reasonably linked to a specific consumer or device
Privacy By Design	Companies should promote consumer privacy at every stage of the development of their products and services
Substantive Principles	Companies incorporate privacy protections into their practices, such as data security, reasonable collection limits, sound retention & disposal practices, and data accuracy

FTC Privacy Framework

Factor	Description
Simplified Consumer Choice	Companies should simplify consumer choice
Practices That Do Not Require Choice	Those practices consistent with context of transaction or company's relationship with consumer or specifically authorized by law
Companies Should Provide Consumer Choice for Other Practices	Offer choice at a time and context in which consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes

FTC Privacy Framework

Factor	Description
Transparency	Companies should increase the transparency of their data practices
Privacy Notices	Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices
Access	Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use
Consumer Education	All stakeholders should expand their efforts to educate consumers about commercial data privacy practices