Data breaches and identity theft

Lorrie Faith Cranor

November 12, 2013

8-533 / 8-733 / 19-608 / 95-818: Privacy Policy, Law, and Technology

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

Writing a research paper

Organizing a research paper

- Decide up front what the point of your paper is and stay focused as you write
- Once you have decided on the main point, pick a title
- Start with an outline
- Use multiple levels of headings (usually 2 or 3)
- Don’t ramble!

Typical paper organization

- Abstract - Short summary of paper
- Introduction - Motivation (why this work is interesting/important, not your personal motivation)
- Background and related work - Sometimes part of introduction, sometimes two sections
- Methods - What you did; in a systems paper you may have system design and evaluation sections instead
- Results - What you found out
- Discussion/Conclusions - May include conclusions, future work, discussion of implications, etc.
- References
- Appendix - Stuff not essential to understanding the paper, but useful, especially to those trying to reproduce your results - data tables, proofs, survey forms, etc.

Road map

- Papers longer than a few pages should have a "road map" so readers know where you are going
- Road map usually comes at the end of the introduction
- Tell them what you are going to say, then say it, (and then tell them what you said)
- Examples
  - In the next section I introduce X and discuss related work. In Section 3 I describe my research methodology. In Section 4 I present results. In Section 5 I present conclusions and possible directions for future work.
  - Waldman et al, 2001: "This article presents an architecture for robust Web publishing systems. We describe nine design goals for such systems, review several existing systems, and take an in-depth look at Publius, a system that meets these design goals."

Use topic sentences

- (Almost) every paragraph should have a topic sentence
  - Usually the first sentence
  - Sometimes the last sentence
  - Topic sentence gives the main point of the paragraph
- First paragraph of each section and subsection should give the main point of that section
- Examples from Waldman et al, 2001
  - In this section we attempt to abstract the particular implementation details and describe the underlying components and architecture of a censorship-resistant system.
  - Anonymous publications have been used to help bring about change throughout history.

Avoid unsubstantiated claims

- Provide evidence for every claim you make
  - Related work
  - Results of your own experiments
- Conclusions should not come as a surprise
  - Analysis of related work, experimental results, etc. should support your conclusions
  - Conclusions should summarize, highlight, show relationships, raise questions for future work
  - Don’t introduce completely new ideas in discussion or conclusion section (other than ideas for future work)
  - Don’t reach conclusions not supported by the rest of your paper

Creating a research poster

December 4 Poster Fair

- During class in GHC 6115
- 32x40 inch foam core boards, 9x12 inch construction paper, glue sticks, and thumb tacks will be made available
  - You can get them from Tiffany Todd ttodd@cs.cmu.edu in Wean 4114
- Present your preliminary project results and get feedback you can use as you finish your paper

Creating a research poster

- Any word processor, drawing, or page design software will work
  - PowerPoint is well-suited for making posters
- Design poster as single panel or modular units
  - Single panel posters
    - Have a professional look (if well designed)
    - Should be printed on large format printers (SCS has one for student use, requires SCS account)
    - Other large printers on campus or local copy shops – some can also print on fabric
  - Modular units
    - Easier to design and transport
    - Print on letter paper (optionally, mounted on construction paper)

Research poster content

- Don’t try to present your whole paper
  - Convey the big picture
  - Don’t expect people to spend more than 3-5 minutes reading your poster
  - 500 words, maximum (can be a lot shorter!)
- Introduce problem, your approach, and results
- Provide necessary background or glossary
- A picture is worth 1000 words
  - Graphs, diagrams, etc.
- Use bullets and sentence fragments, similar to making slides
- Don’t forget to include title and author

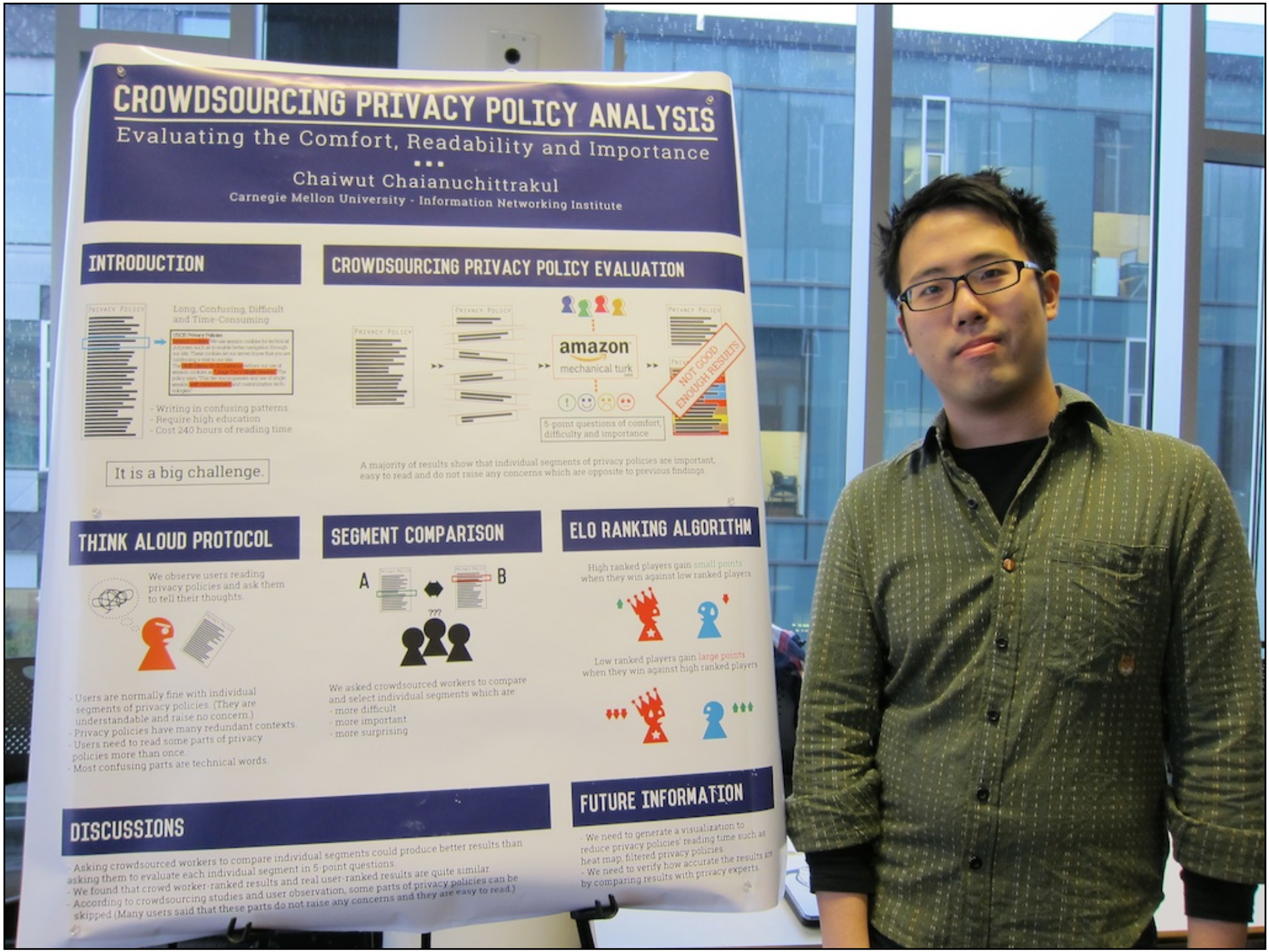
Research poster design

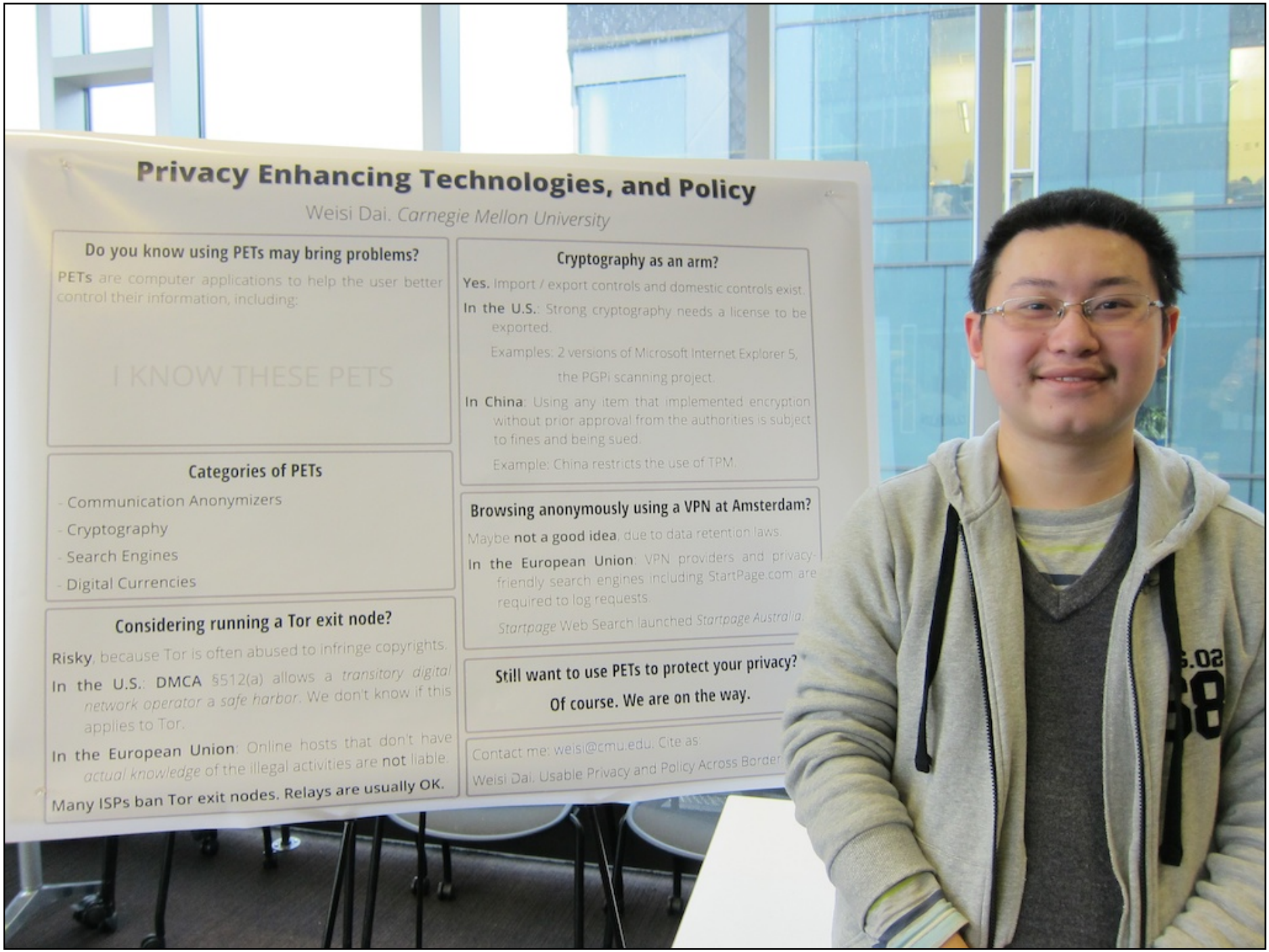
- Use a modular design
- Each section of your poster can go in a box
- Use a large, easy-to-read font
  - Most text should be at least 20 point font
  - No text less than 14 point font
  - Headings should be larger and in bold
- Use color consistently
- Arrange elements for a sensible visual flow

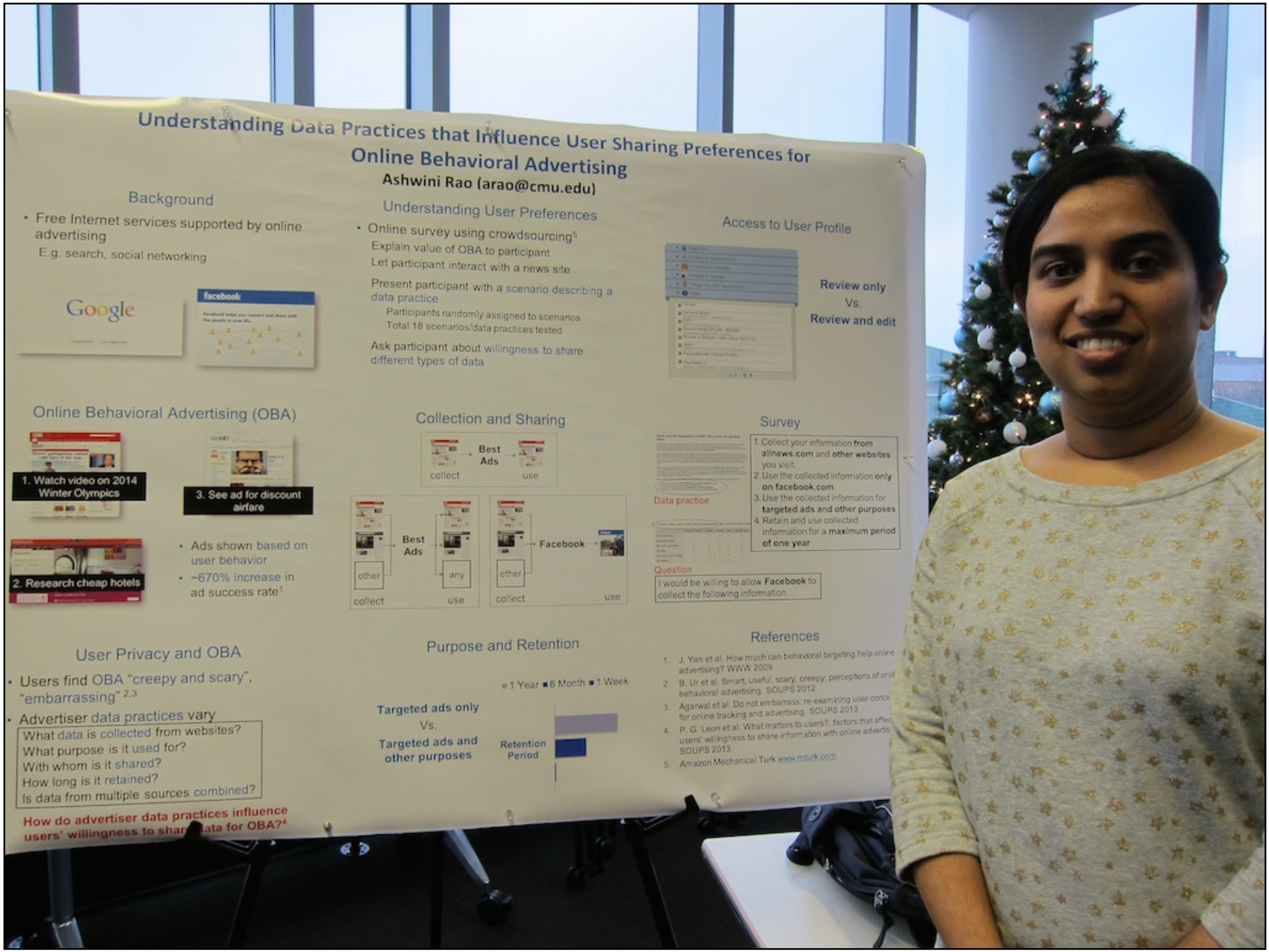
Presenting your research poster

- Be prepared to give a 1-minute overview of your poster and answer questions
- Let people read your poster without interrupting them
- Consider bringing a laptop if you have software to demo or a video to show
- Consider making handouts available with abstract, web URL for obtaining your paper, and your contact information


Research Questions
Metadata on Privacy Policies (.5)
Analysis of Privacy Policies (.5)


CROWDSOURCING PRIVACY POLICY ANALYSIS
Evaluating the Comfort, Readability and Importance
Chaiwut Chaianuchittrakul
Carnegie Mellon University - Information Networking Institute
INTRODUCTION
Privacy Policy
Long, Confusing, Difficult and Time-Consuming
- Writing in confusing patterns
- Require high education
- Cost 240 hours of reading time
It is a big challenge.
CROWDSOURCING PRIVACY POLICY EVALUATION
Privacy Policy
amazon mechanical turk
5-point questions of comfort, difficulty and importance
NOT GOOD ENOUGH RESULTS
A majority of results show that individual segments of privacy policies are important, easy to read and do not raise any concerns which are opposite to previous findings.
THINK ALOUD PROTOCOL
We observe users reading privacy policies and ask them to tell their thoughts.
- Users are normally fine with individual segments of privacy policies. (They are understandable and raise no concern.)
- Privacy policies have many redundant contexts.
- Users need to read some parts of privacy policies more than once.
- Most confusing parts are technical words.
SEGMENT COMPARISON
A
B
We asked crowdsourced workers to compare and select individual segments which are:
- more difficult
- more important
- more surprising
ELO RANKING ALGORITHM
High ranked players gain small points when they win against low ranked players
Low ranked players gain large points when they win against high ranked players
DISCUSSIONS
- Asking crowdsourced workers to compare individual segments could produce better results than asking them to evaluate each individual segment in 5-point questions.
- We found that crowd worker-ranked results and real user-ranked results are quite similar.
- According to crowdsourcing studies and user observation, some parts of privacy policies can be skipped (Many users said that these parts do not raise any concerns and they are easy to read.)
FUTURE INFORMATION
- We need to generate a visualization to reduce privacy policies' reading time such as heat map, filtered privacy policies
- We need to verify how accurate the results are by comparing results with privacy experts


Privacy Enhancing Technologies, and Policy
Weisi Dai. Carnegie Mellon University
Do you know using PETs may bring problems?
PETs are computer applications to help the user better control their information, including:
I KNOW THESE PETS
Categories of PETs
- Communication Anonymizers
- Cryptography
- Search Engines
- Digital Currencies
Considering running a Tor exit node?
Risky, because Tor is often abused to infringe copyrights.
In the U.S.: DMCA §512(a) allows a transitory digital network operator a safe harbor. We don't know if this applies to Tor.
In the European Union: Online hosts that don't have actual knowledge of the illegal activities are not liable.
Many ISPs ban Tor exit nodes. Relays are usually OK.
Cryptography as an arm?
Yes. Import / export controls and domestic controls exist.
In the U.S.: Strong cryptography needs a license to be exported.
Examples: 2 versions of Microsoft Internet Explorer 5, the PGPi scanning project.
In China: Using any item that implemented encryption without prior approval from the authorities is subject to fines and being sued.
Example: China restricts the use of TPM.
Browsing anonymously using a VPN at Amsterdam?
Maybe not a good idea, due to data retention laws.
In the European Union: VPN providers and privacy-friendly search engines including StartPage.com are required to log requests.
Startpage Web Search launched Startpage Australia.
Still want to use PETs to protect your privacy?
Of course. We are on the way.
Contact me: weisi@cmu.edu. Cite as:
Weisi Dai. Usable Privacy and Policy Across Border


Understanding Data Practices that Influence User Sharing Preferences for Online Behavioral Advertising
Ashwini Rao (arao@cmu.edu)
Background
• Free Internet services supported by online advertising
E.g. search, social networking
Google
facebook
Understanding User Preferences
• Online survey using crowdsourcing[5]
Explain value of OBA to participant
Let participant interact with a news site
Present participant with a scenario describing a data practice
Participants randomly assigned to scenarios
Total 18 scenarios/data practices tested
Ask participant about willingness to share different types of data
Access to User Profile
Review only
Vs.
Review and edit
Online Behavioral Advertising (OBA)
1. Watch video on 2014 Winter Olympics
3. See ad for discount airfare
2. Research cheap hotels
• Ads shown based on user behavior
• ~670% increase in ad success rate[1]
Collection and Sharing
Best Ads
collect
use
other
any
Facebook
Survey
Data practice
1. Collect your information from allnews.com and other websites you visit.
2. Use the collected information only on facebook.com.
3. Use the collected information for targeted ads and other purposes
4. Retain and use collected information for a maximum period of one year
Question
I would be willing to allow Facebook to collect the following information...
User Privacy and OBA
• Users find OBA "creepy and scary", "embarrassing" [2,3]
• Advertiser data practices vary
What data is collected from websites?
What purpose is it used for?
With whom is it shared?
How long is it retained?
Is data from multiple sources combined?
How do advertiser data practices influence users' willingness to share data for OBA?[4]
Purpose and Retention
1 Year
6 Month
1 Week
Targeted ads only
Vs.
Targeted ads and other purposes
Retention Period
References
1. J. Yan et al. How much can behavioral targeting help online advertising? WWW 2009
2. B. Ur et al. Smart, useful, scary, creepy: perceptions of online behavioral advertising. SOUPS 2012
3. Agarwal et al. Do not embarrass: re-examining user concerns for online tracking and advertising. SOUPS 2013
4. P. G. Leon et al. What matters to users?: factors that affect users' willingness to share information with online advertisers. SOUPS 2013
5. Amazon Mechanical Turk www.mturk.com

Do Teens Have a Right to Privacy? Parents' and Teens' Perspectives

Adam Durity, Abigail Marsh, Blase Ur

Motivation

- Legally, teens have few rights to privacy from their parents
  - FERPA protects education records, but mandates sharing with parents/guardians
  - COPPA protects children under age 13 from online third-party tracking
  - No omnibus protections beyond age 12
- **Hypothesis:** Families believe teens have a de facto right to privacy from their parents
  - Teens and parents have differing expectations of the boundaries
  - Boundaries expand with age
- What do parents feel they have a right to know? Not to know? What is acceptable and ethical in their view?
- What do teens feel parents have a right to know? Does this differ from parents' opinions?

Methodology

- Semi-structured interviews with teens in high school and parents of teens in high school
  - 2 participants (Eventually 20 participants)
- Recruited participants from Pittsburgh, PA using Craigslist and flyers
- Selected only one participant per family
- In participant's eyes, to what extent do teens have a right to privacy from their parents?

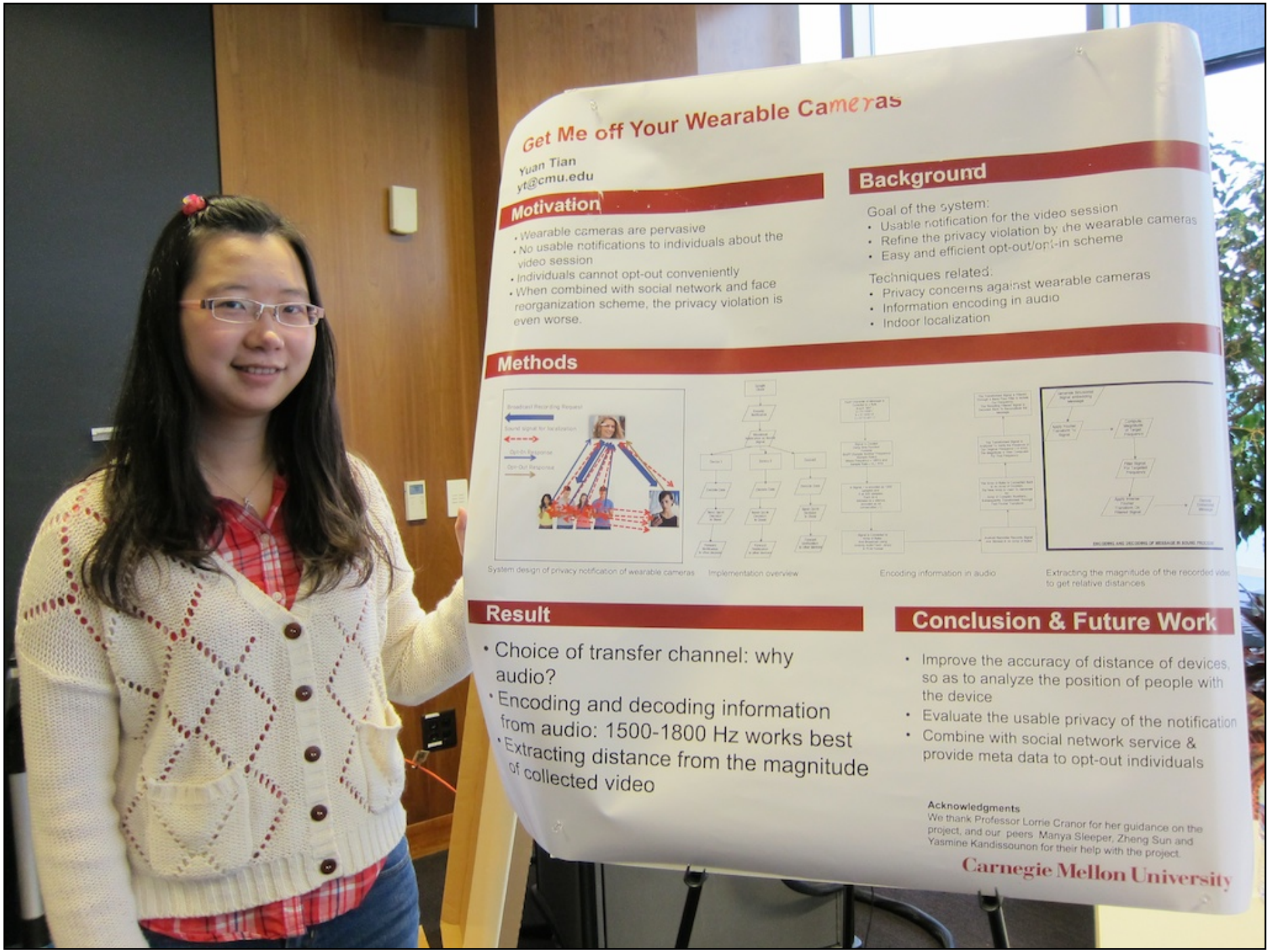
Area of inquiry	Examples
Privacy at home	Closing bedroom doors, areas that are off-limits, knocking
Social privacy	Knowing their friends, always knowing where they are
Monitoring	Reading texts, monitoring computer, parental controls

Preliminary Results

Theme	Participants
Respect for teen ➔ Privacy	P0, P1
A parent's concerns override a teen's right to privacy	P0, P1
Privacy as parent-teen negotiation	P0, P1

- Teens' bedrooms are generally private
  - P0: "If they are actually in there and don't want me in there . . . I respect their wishes."
  - P1: "It's his private [area], it's his domain."
  - However, P1 examines son's room when he is not at home "just to make sure…he's not doing nothing he shouldn't be doing."
- Some privacy attitudes varied
  - P0 tried to use parental controls, whereas P1 never tried to monitor technology usage
  - P1 knows most of son's friends, whereas P0 knows only a handful
- Teens' right to privacy is not absolute
  - P0: "[they] have a right to privacy to some extent ... but not overriding a parent's need to know some things."
  - P1: "It's my house and I'm gonna go in that room whenever I want to."
- Responsibility for teens' actions vs. privacy
  - P0's nephew was arrested for downloading child porn on grandparent's computer and nearly liable
  - P1: "Hell, there could be a mad man living in the room, how would I know? I could see Dr. Phil, 'Well, you never went in your son's room, huh?'"
- Teen years are a privacy transition
  - P0: "By the time you're done with it you have a right to privacy; when you start it you don't."

Carnegie Mellon University
CyLab


Get Me off Your Wearable Cameras
Yuan Tian
yt@cmu.edu
Motivation
• Wearable cameras are pervasive
• No usable notifications to individuals about the video session
• Individuals cannot opt-out conveniently
• When combined with social network and face reorganization scheme, the privacy violation is even worse.
Background
Goal of the system:
• Usable notification for the video session
• Refine the privacy violation by the wearable cameras
• Easy and efficient opt-out/opt-in scheme
Techniques related:
• Privacy concerns against wearable cameras
• Information encoding in audio
• Indoor localization
Methods
System design of privacy notification of wearable cameras
Implementation overview
Encoding information in audio
Extracting the magnitude of the recorded video to get relative distances
Result
• Choice of transfer channel: why audio?
• Encoding and decoding information from audio: 1500-1800 Hz works best
• Extracting distance from the magnitude of collected video
Conclusion & Future Work
• Improve the accuracy of distance of devices, so as to analyze the position of people with the device
• Evaluate the usable privacy of the notification
• Combine with social network service & provide meta data to opt-out individuals
Acknowledgments
We thank Professor Lorrie Cranor for her guidance on the project, and our peers Manya Sleeper, Zheng Sun and Yasmine Kandissounon for their help with the project.
Carnegie Mellon University

Towards Information Extraction From Natural Language Privacy Policies In Retail & News Sectors

Aditya Marella
Dilek Yuksel Civelek

Poster Fair – December 5, 2013

Goals

- Facilitating Usable Privacy Policy Project (usableprivacy.org) affiliated by:

Carnegie Mellon University | Fordham University | Stanford University

- Identifying key policy features from Retail and News Entertainment sectors
- Extracting different types of information collected and their sharing targets for each sector

News Entertainment

14 News Websites:

- 4 from top ten broadcast media
- 3 political websites
- 3 business websites
- 4 personal finance websites

Retail Sector

15 Retail Websites

- 4 popular online stores
- 3 not so popular stores
- 2 each Health foods & Kid stores
- 2 each Electronic & Home goods

Methodology

- Identify key features in each sector
- Build questionnaire to reflect key features
- Determine what each privacy policy says about each feature
- Collect terms used for information types, categories & sources; usage types; sharing targets
- Identify any patterns or anomalies in the privacy policies

Key Features

- News Entertainment
  - Services other just offering news?
  - Share behavioral data with other third parties?
  - Collection and usage of Social media data incase the user connects to the website using social media services
- Online Retail
  - Collection & Sharing of sensitive information (credit card, credit history)
  - Restrictions on sharing target's privacy policies
  - Use of SSL while transferring sensitive information
  - Opt-out choices w.r.t advertising and promotional emails

Questionnaire

- 22 Questions for News Entertainment Sector
- 18 Questions for Retail Sector
- The questions are designed to be answered as:
  - a) Yes
  - b) No
  - c) Not clear from the policy
  - d) Policy does not answer the question

Results: News Entertainment

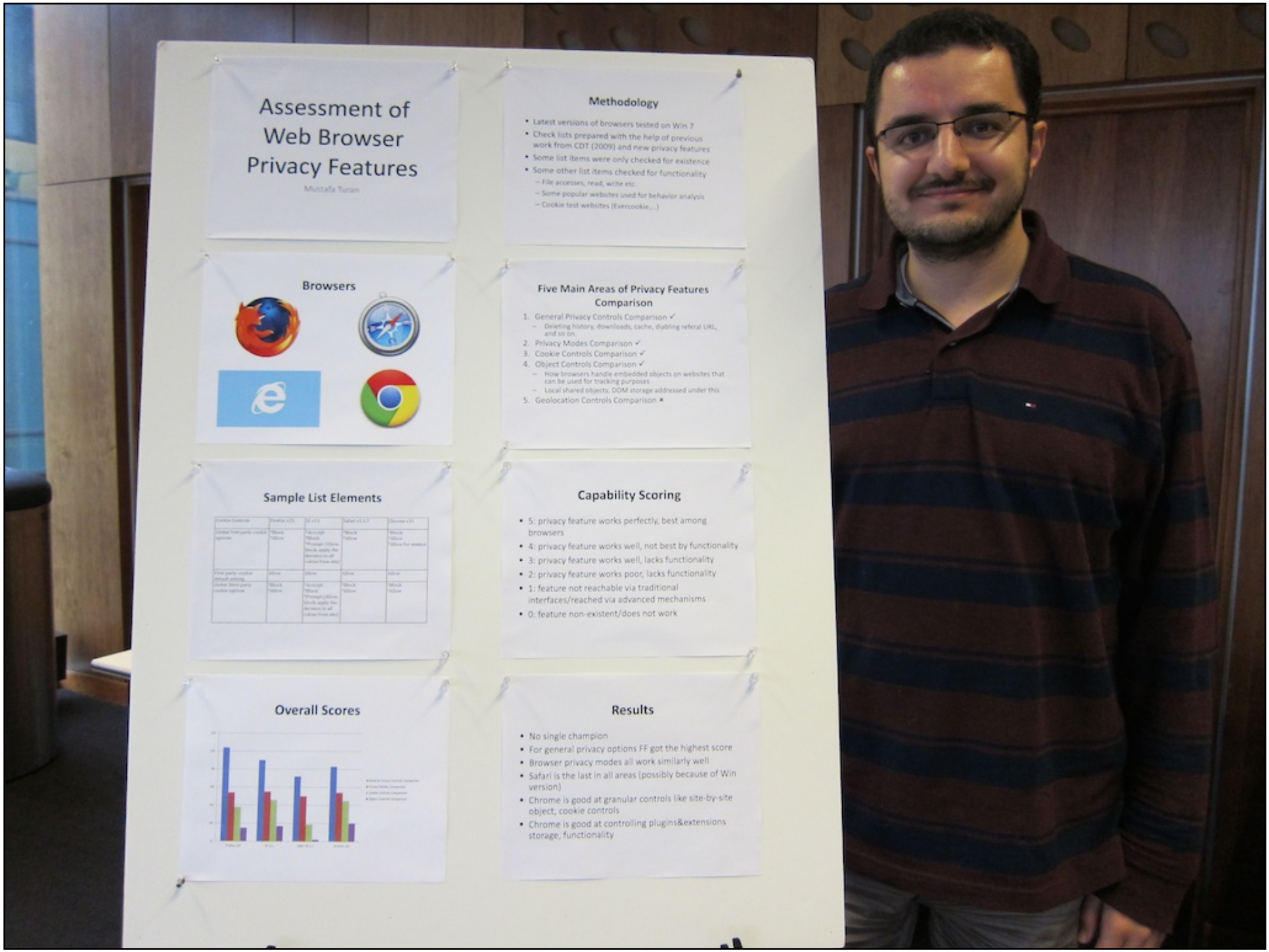
- News websites not limited to "news", 100% of the samples sell product and services, offer interactive services…
- If registered, all of them collect contact information
- 72.8 % collect current location of a user
- 92% use cookies, beacons or other tracking technologies
- 78% use (OBA) to deliver targeted advertising

Results: Online Retail

- Contact Information
  - all of them collect contact information and
  - 70% share for purposes other than provisioning core services,
- Financial Information
  - all of them collect credit card information and
  - 20% collect credit history information
- SSL 50% protect personal information; 30% protect only sensitive information; 20% do not mention SSL

Results: collection of terms

- Personal Information: name, address, phone, email, age, dob, credit card information, social security number, personal description, photograph, location, device-identifier, purchase-information, redemption-information, etc
- Behavioral Information: purchase-history, products viewed, products searched, session-information, page-response-times, download-errors, viewing-duration, clicks, scrolls, mouse-overs, page-view-information, search-term, search-result, paid-listings, etc
- Technical Information: IP, computer, browser, version, timezone, plugin-types, plugin-versions, OS, platform, etc
- Full spreadsheet is available on request


Assessment of Web Browser Privacy Features
Mustafa Turan
Methodology
• Latest versions of browsers tested on Win 7
• Check lists prepared with the help of previous work from CDT (2009) and new privacy features
• Some list items were only checked for existence
• Some other list items checked for functionality
– File accesses, read, write etc.
– Some popular websites used for behavior analysis
– Cookie test websites (Evercookie,...)
Browsers
Five Main Areas of Privacy Features Comparison
1. General Privacy Controls Comparison ✓
– Deleting history, downloads, cache, disabling referal URL, and so on
2. Privacy Modes Comparison ✓
3. Cookie Controls Comparison ✓
4. Object Controls Comparison ✓
– How browsers handle embedded objects on websites that can be used for tracking purposes
– Local shared objects, DOM storage addressed under this
5. Geolocation Controls Comparison ✗
Sample List Elements
Capability Scoring
• 5: privacy feature works perfectly, best among browsers
• 4: privacy feature works well, not best by functionality
• 3: privacy feature works well, lacks functionality
• 2: privacy feature works poor, lacks functionality
• 1: feature not reachable via traditional interfaces/reached via advanced mechanisms
• 0: feature non-existent/does not work
Overall Scores
Results
• No single champion
• For general privacy options FF got the highest score
• Browser privacy modes all work similarly well
• Safari is the last in all areas (possibly because of Win version)
• Chrome is good at granular controls like site-by-site object, cookie controls
• Chrome is good at controlling plugins&extensions storage, functionality


OBA Tools Collect Digital Data
From a specific computer browser or device
Over time & across multiple unrelated web pages
Purposes
Develop profiles of online activity of specific users-consumers
Generate predictions of preferences and interests which enable
Targeted online advertising to consumers
Aggregate data for marketing trend forecasts.
Fund "free" web services, e.g., search engines & web browsers.
Value
Over $20 billion advertising industry annual revenues based on OBA
18% annual growth rate
Is Privacy Self-Regulation Working
within the
Online Behavioral Advertising Industry?
A Privacy Policy Analysis
Candice Hoke
Privacy Policy, Law & Technology
Carnegie Mellon ◇ Professor Lorrie F. Cranor ◇ Fall 2013
"Self-Regulatory" Trade Associations
iab.
SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING FACTSHEET
2013 NAI Code of Conduct
NAI
Empirical Study Results
Ghostery
Privacy Information
Privacy Policy
Data Collection
Data Sharing
Conclusion
No, the OBA industry "self-regulatory" regime is not working.
Preliminary data suggests little difference between firms affiliated & non-affiliated with the regime.
Lightbeam
Weekly
Self-Regulatory Governance Decisions
1. Voluntary choice whether to join & comply
2. What consumer protection rules
3. Face-to-no compliance assessments
4. What penalties for non-compliance
5. Usability testing input to monetization
6. Failure to correct for verbose & confusing privacy policies.
7. Deceptive & misleading presentation of tracking "anonymous" IP data permitted.
Privacy Policy

Is Facebook Morally Obligated to Protect Privacy?

A teleological and deontological analysis of corporate social responsibility and privacy protection

Mia Wang
MSISPM
miawang@cmu.edu
95-815F13

I
Introduction

As **privacy violations** by **social media services** become more publicized, businesses are faced with the **ethical and strategic dilemma** of if, and to what extent, they should improve privacy controls. Social media providers must consider **business ethics** to determine how to protect their users and the petabytes of data they generate.

Existing **corporate social responsibility** (CSR) research does not address the increasingly controversial issue of social media services' privacy practices.

This project seeks to evaluate **whether social networking providers are bound by CSR to protect user privacy beyond the minimum legal requirements.**

II
Overview

Goal	to develop a Privacy Decision-Making Framework for social media services to evaluate CSR obligations.
Method	Evaluate privacy-related CSR through 2 classic normative philosophical approaches (teleology, deontology) to CSR and a case study to understand the philosophies in practice.

III
Philosophical Approaches to CSR

Teleological	Deontological
• *Telos* (τέλος) = end • Focus on outcome • "greatest good for the greatest number" • Consequentialism, Egoism, welfarism • Difficult to forecast outcome • Often avoided in modern science except in evolutionary biology • John Stuart Mill, Jeremy Bentham	• *Deon* (δέον) = duty • Focus on adherence to duty, rules, obligations • Inherent rightness • Categorical Imperative, Natural rights theory, contractualism, divine command theory • Flexibility and terms of duty are difficult to define • Immanuel Kant, Thomas Nagel, Thomas Scanlon

IV
Case Study - Facebook

A 2012 Wall Street Journal article titled "When the Most Personal Secrets Get Outed on Facebook" documented two University of Texas students' (Bobbi Duncan, Taylor McCormick) experiences after Facebook (FB) inadvertently "outed" them to their fathers.

The two students' fathers received notifications that their children became members an Open "Queer Chorus" Facebook group after the group's owner added them. Membership and public notification did not require consent from the students.

Facebook statistics:

a. Monthly active users: 1.26B
b. Daily active users in the United States: 128M
c. Avg. time spent on Facebook: 20B minutes per day
d. FB's share of "total Internet minutes spent": 15.8%
e. Market capitalization: $121.39B

Is Facebook morally obligated to improve privacy controls for their Group feature?

Teleological Approach (excerpt of analysis)

Argument	Explanation	Impact
***Claim A**: Corporate social responsibility dictates that Facebook is morally obligated to improve privacy controls and mechanisms.*		
Facebook's market value may increase	Improved image, user satisfaction, and a reduction in fines could increase Facebook's profits which could all increase the value of Facebook's stocks. While this potential outcome is hypothetical, improved performance overall and less negative attention could increase investor interests and overall value of the company.	With a market cap of $120B+, Facebook is a large, profitable organization whose value could increase based on appreciation in share price.
***Claim B**: Corporate social responsibility dictates that Facebook is not morally obligated to improve privacy controls and mechanisms.*		
Positive impact is not guaranteed	Facebook could potentially not see any improvements in image, user activity, or market value. There does not exist silver bullet privacy enhancements so the effort invested into the improvement could result in negative impact if the benefits do not outweigh the investment.	0/negative – The cost of this incident to Facebook's bottom line is unclear and may not have had any direct impact.

Deontological Approach (excerpt of analysis)

Stakeholder	Rationale
***Claim A**: Corporate social responsibility dictates that Facebook is morally obligated to improve privacy controls and mechanisms.*	
Duty to Shareholders	If the duty of a business, as per Milton Friedman, is to increase profits, Facebook would be bound by CSR to implement additional privacy protections if they improve its P&L. Privacy improvements may improve Facebook's financial performance which in turn, increases returns to its shareholders and allows the company to continue growing. Deciding to take measures to protect privacy in response to the Duncan and McCormick incident would be the socially responsible action as it benefits its shareholders.
***Claim B**: Corporate social responsibility dictates that Facebook is not morally obligated to improve privacy controls and mechanisms.*	
Duty to Shareholders	If Facebook's duty is to maximize ROI for its shareholders, implementing additional privacy enhancements increases operational costs without the guarantee of better financial performance in the long run. The company may not face significant enough backlash to justify improving privacy controls. As such, P&L and ability to increase returns to shareholders are not positively impacted. This would indicate that Facebook should not improve privacy out of duty to increasing returns for its shareholders.

V
Privacy Decision-Making Framework

Company S is considering whether or not to implement additional user privacy protections. Consider:

Teleological		Deontological	
Impact	**Score (-1, 0, +1)**	**Adherence to Duty**	**Score (-1, 0, +1)**
to Users		to Users	
to Shareholders		to Shareholders	
to Employees		to Employees	

Note: if Company S does not have Shareholders, consider Impact/Duty to the Company

Total:

If Total ≥3, Company S should consider implementing additional user privacy protections.

VI
Conclusion

There are not definitive standards and perceptions of corporate social responsibility, so implementation will depend on an organization's leadership. If a privacy enhancing improvement is being considered, a social media service has the responsibility to reconcile strategic and ethical benefits, which may not be mutually exclusive, to implementing the privacy control. Given the volume and scale at which social media services are collecting data, privacy decisions impact billions of users on a global level.

The framework developed in this project serves to help a service organize their priorities and responsibilities to assess whether or not they are ethically bound to enacting a certain privacy control.

References

[illegible]

Anonymous Dislike:

Users' Reaction to Anonymous Peer Reviews in Social Networks

Pranshu Kalvani
pok@andrew.cmu.edu

Chao Pan
chaop@andrew.cmu.edu

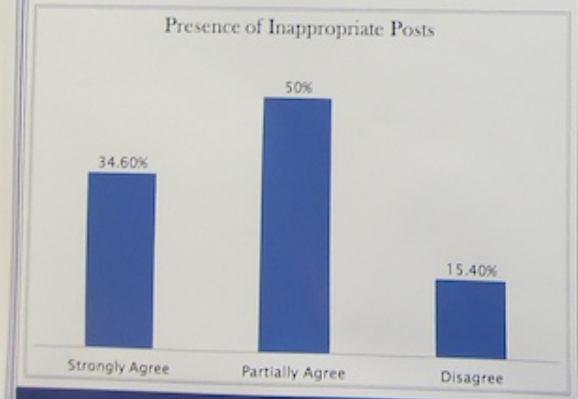
Introduction

This study explores the effects of anonymity on users behavior and also tries to find out their response to anonymous comments. Its primary objective is to provide feedback, so people can realize the error of their ways and thus make them more conscious with future posts.

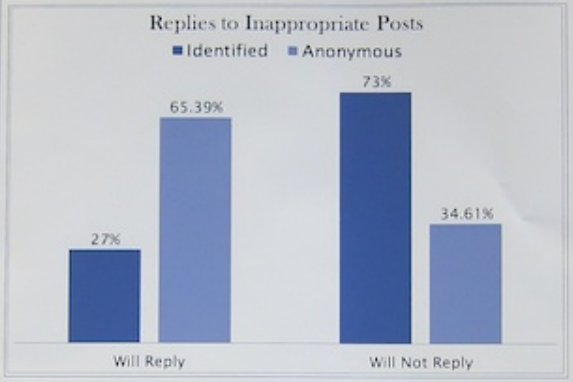
Methodology

We have performed two surveys on Amazon's MTurk. Based on these surveys we have created an anonymous commenting system. It is a Google Chrome add-on for Facebook and we are currently conducting a user study to test the efficacy of our system.

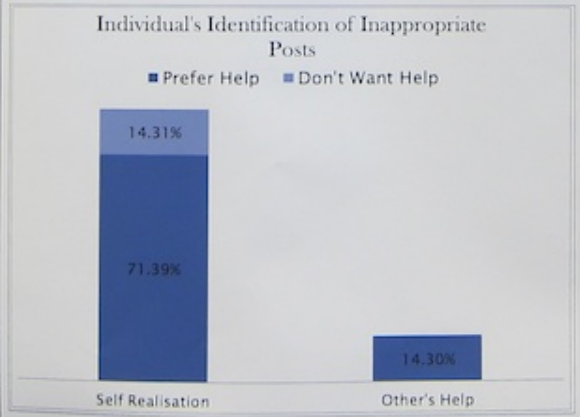
Results



Results (contd.)



These were the important results from the first survey. However, we wanted to see if after receiving these comments if any steps to improve privacy were taken.



System Architecture

Challenges & Future Work

- Due to Facebook changing its source code and DOM regularly our extension stops functioning. This leads to difficulties in conducting a user study.
- Getting large groups that provide meaningful data is one of the other sizeable challenge we face.
- We intend on adding more features to our system to make it more informative. A report dashboard is at the top of this list.
- Delimiting the anonymous post content via peer review or natural language processing is another feature we intend on adding.
- There is still a lot more work possible, in this area.

Carnegie Mellon University | Master of Science in Information Technology | privacy ENGINEERING

Web Application for Searching and Comparing Financial Companies' Privacy Practices

Gabriel Moreno
gabrielm@cs.cmu.edu

Overview

- Comparing the privacy policies of financial institutions is a time-consuming task for consumers.
  - No centralized place to find the policies
- This web application allows users to:
  - Look at policies
  - Search for institutions with specific privacy practices and other criteria
  - Compare privacy practices of multiple institutions side-by-side

Motivation

- The Federal Trade Commission (FTC) envisioned that privacy notices would enable competition in a market where privacy practices would be part of the consumer's decision.
- Consumers are expected to *comparison shop on privacy policies* to protect their privacy.
- Doing this comparison puts too much burden on consumers
  - It is time-consuming task

Limitations of Existing Tools

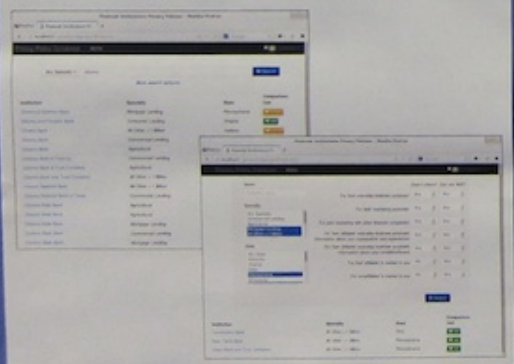
- Compare things other than privacy policies
  - consumer products
    - Examples: pricegrabber.com, shopper.com
  - for banks: offered services, financial strength indicators, user reviews
    - Example: findthebest.com
  - insurance policies (health, auto, homeowner's)
    - Example: ehealthinsurance.com
- Focus on the online practices of organizations
  - Example: privacyscore.com

Standard Privacy Notice for Financial Institutions

- Most financial institutions use the model privacy notice to comply with the requirements of federal regulations.
- Standardized privacy notices are easier to compare, but still it involves a manual process for the consumer.
  - Find the privacy notices
  - Compare them

Current Burden on Consumers

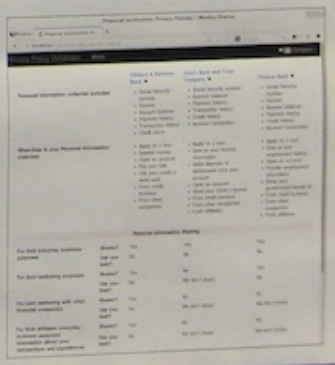
- Consumers must first obtain privacy notices from the different financial institutions and then compare them.
- What if a consumer wants to find a financial institution with specific privacy practices?
  - The consumer must first **obtain all the privacy notices**.
  - **Go one by one to select** those that satisfy the specific criteria.



Use Cases Supported by this Web Application

- Search for and view the privacy practices of a financial institution
  - no need to request it or find were it is on the web
- Compare two or more selected institutions side-by-side
- Search for financial institutions whose privacy policies match some specified characteristic
  - For example, institutions in Pennsylvania that do not share personal information for marketing purposes

L. F. Cranor, K. Idouchi, P. G. Leon, M. Sleeper, and B. Ur. "Are they actually any different? comparing thousands of financial institutions privacy practices." In workshop on the Economics of Information Security (WEIS 2013), 2013.



Demonstration of financial companies' privacy practices

Privacy Bank

Jie Chen, Ziwei Hu, Zhipeng Tian
5000 Fobres Ave, Pittsburgh, PA
Carnegie Mellon

WHY?

Have you ever wonder how your banks deal with your personal info?

Do they sell your personal info?

Do they share your personal info? with whom? for what?

OR do they keep your info secure and protected?

Traditional privacy policies have been difficult to read and understand. It also takes lots of time to read.

More importantly, it does not allow users compare privacy practices across different financial organization.

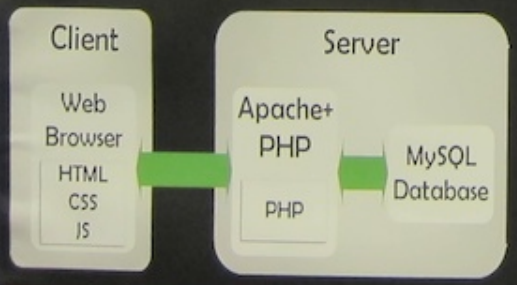
WHAT?

The Project is to design a website that allows users to search , compare, and review financial companies privacy policy..

Our Focus is not noly on the main features, but also on communication and presentation.

HOW?

PRIVACYBANK=
User-friendly Interface
+
Comprehensive and detailed data



System Architecture Graph

User Study

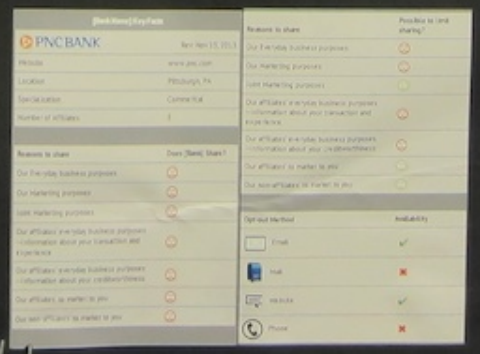
Interviewed with 10 people and ask them what they care about the most in the search results.

a) Does my bank share?
b) Can I opt out?
c) How to opt out?
d) Number of affiliates

MAIN FEATURES:

Search

Our database includes 729 financial companies info across the United States.



Rate, Review, and Share

You can rate and review a bank after you search it. You can also share the search results on Facebook.

Are your banks selling your info?

Scan and Check out our website!

Research Questions

- What are the similarities or differences between the privacy policies of top US and Turkish wireless communications companies?
- Can these similarities or differences be attributed to the country wide or sector specific privacy laws or regulations in place in each country?

Privacy Policy Analysis in the Electronic Communications Sector

Ayse Gul MIRZAOGLU

December 5, 2013

Primary Motivation

"to generate valuable input to the Usable Privacy Policy Project*"

*Aims to "semi-automatically extract key privacy policy features from natural language website privacy policies and present these features to users in an easy-to-digest format that enables them to make more informed privacy decisions as they interact with different websites" (usableprivacy.org)

Metada on Privacy Policies (US)

	Title	Version	Certification?	Accreditation?	Summary?	Page[1]
Verizon Wireless	Privacy Policy	English, Spanish	TRUSTe	BBBOnline	+	13
AT&T Wireless	Privacy Policy	English, Spanish	TRUSTe	-	+	15
Sprint Nextel	Privacy Policy	English, Spanish	-	-	FAQ	3
T-Mobile (DT)	Privacy Policy	English, German	-	-	-	2+11[2]
Leap Wireless	Online Privacy Stmt	English	-	-	-	2

[1] Times New Roman, 12 pt, single spacing
[2] 11 pages of Code of Conduct for the Protection of the Individual's Right to Privacy in the Handling of Personal Data within the Deutsche Telekom Group (worldwide)

Why the Electronic Communications Sector?

- 220,000 subscribers in US[1]
  69,000 subscribers in Turkey[2]
- Sectoral business operations are highly data intensive; collect, process and store huge amounts of personal data
- Sector-specific privacy regulations are in place in both countries

[1] IBISWorld, Wireless Telecommunications Carriers in the US Report, Estimated 2013 Revenues
[2] ICTA, Quarterly Market Data Report, 2013 Q3 Number of Subscribers

Metada on Privacy Policies (TR)

	Title	Version	Certification?	Accreditation?	Summary?	Page[1]
Turkcell	Security and Privacy	Turkish	-	-	-	6[2]
Vodafone	Privacy Policy	Turkish, customized for each country in which Vodafone operates	-	-	-	1
Avea	Security and Privacy	Turkish, English	-	-	-	1

[1] Times New Roman, 12 pt, single spacing
[2] Privacy policy mainly consists of the "Turkcell Online Subscriber Transactions Contract"

Analysis of Privacy Policies (US)

Fair Information Practices Implementation	Verizon	AT&T	Sprint Nextel	T-Mobile (DT)	Leap
Collection Limitation	Strong	Strong	Strong	Strong	Medium
Use Limitation	Strong	Strong	Strong	Strong	Medium
Data Quality	Medium	Medium	Medium	Medium	Weak
Purpose Specification	Strong	Strong	Strong	Strong	Medium
Security Safeguards	Strong	Strong	Strong	Medium	Weak
Openness	Strong	Strong	Medium	Strong	Medium
Individual Participation	Strong	Strong	Medium	Strong	Medium
Accountability	Strong	Strong	Strong	Strong	Weak

Strong | Medium | Weak

Top Wireless Communication Companies

US Market Shares (%)[1]

TR Market Shares (%)[2]

[1] IBISWorld, Wireless Telecommunications Carriers in the US Report, Estimated 2013 Revenues
[2] ICTA, Quarterly Market Data Report, 2013 Q3 Number of Subscribers

Analysis of Privacy Policies (TR)

Fair Information Practices Implementation	Turkcell	Vodafone	Avea
Collection Limitation	Medium	Strong	Weak
Use Limitation	Medium	Strong	Weak
Data Quality	Weak	Strong	Weak
Purpose Specification	Weak	Strong	Weak
Security Safeguards	Medium	Strong	Strong
Openness	Medium	Strong	Medium
Individual Participation	Medium	Medium	Medium
Accountability	Strong	Strong	Weak

Strong | Medium | Weak

Revisiting Private E-mail

A review of anonymous remailers and similar technologies

Michael Kahn

Background

- Much of the discussion today surrounding online privacy concerns the collection of surfing habits and personal information.
- Many users have more specialized privacy needs. Among these is being able to send e-mail anonymously – specifically, to send an e-mail such that neither a recipient nor an attacker can identify the sender.
- Such technologies are important for whistleblowers and others who risk repercussions if their actions are revealed.
- The problem of anonymous e-mail has solutions that do not function effectively in the general case with all web traffic.
- Even members of the public who are reasonably well informed about privacy may not be aware of ways to effectively send anonymous e-mail.

Goals

- Design criteria to test different types of e-mail anonymizing methods
- Examine a variety of existing solutions and choose a test group
- Evaluate solutions, and determine which options would be best for different user groups
- Suggest improvements for existing tools

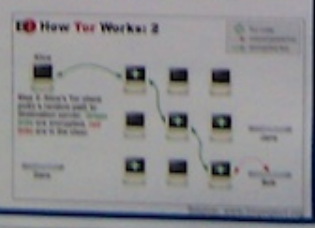
Anonymity Services

Mail-specific services

- anon.penet.fi (Type 0)
  - First large-scale pseudonymous remailer (1993)
- Cypherpunk (Type I)
  - Strips sender information before forwarding messages
  - Requires only PGP and a cypherpunk server
- Mixmaster (Type II)
  - Sends messages in equal-sized chunks in random order
  - Requires client software
- Mixminion (Type III)
  - Adds security improvements to Mixmaster
  - Uses single-use reply blocks to allow replies

General anonymity services

- Tor
  - Uses onion routing to send IP traffic
- JonDonym (Java Anonymous Proxy)
  - Uses mix networks composed of known relays
- I2P
  - Anonymity layer available to other applications



Evaluation Criteria

- **Effectiveness**
  How effective is the system at protecting senders from identification by third parties?
  - Is the system backed by a mathematical model? If so, what are the probabilities of identifying the sender?
  - How secure is the theory's implementation? Can an attacker use indirect attacks to identify the sender?
  - Does the system allow governments to expose users?
- **Accessibility**
  How accessible is the system?
  - What system or technical requirements does it have for an end-user?
  - What technical skill set is required to use the system?
  - What kind of support is available for users?
- **Openness**
  Is the system able to be examined by experts? Is it open-source?
- **Restrictiveness**
  How restrictive is the system?
  - Does it create a delay before the message can be received? If so, how long?
  - Does it restrict the kind of traffic?
  - Can attachments or other rich content be sent?

Results

	Remailers				General solutions		
	Penet	Cypherpunk	Mixmaster	Mixminion	Tor	JonDonym	I2P
Effectiveness	Very Low	Low	Moderate	High	High	Moderate	Moderate
Accessibility	High	Moderate	Low	Moderate	High	High	High
Openness	Moderate	High	High	High	High	Moderate	High
Restrictiveness*	High	Moderate	High	Moderate	Low	Moderate	Low

* I2P is often used by bind-using programs, which have their own interfaces.
* Restrictiveness is an undesirable quality, and so the color-coding is reversed.

Conclusion

- General anonymity services are consistently easier to use than currently available remailers. These remailers are typically used and maintained by a small group of researchers or enthusiasts, whereas Tor is widely used and has a large base of developers and support.
- For the majority of users, a general solution such as Tor or JonDonym provides ease of use and broader applications than are offered even by advanced remailer implementations like Mixminion. However, these general, low latency services are more vulnerable to timing attacks than the higher latency remailers, and mixminion offers greater anonymity.
- Anonymous remailers still have a place in the privacy landscape, but in order to remain feasible, they must provide the accessibility users expect from other, more popular services.

Enhanced P3P-Enabled Search Engine

Damon Smith

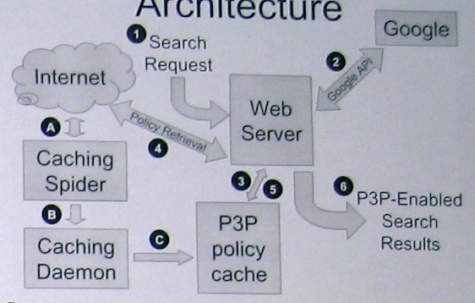
15508 Privacy Policy, Law, and Technology

Motivation

- First P3P Search Engine by Byers, et al.*
- Dual purpose engine:
  - Provide P3P-enabled search
  - Facilitate P3P deployment research
- Goals:
  - Improve scalability and usability
  - Add research functionality

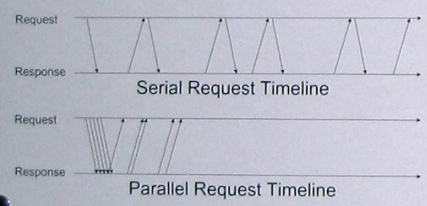
*Byers, S., Cranor, L. F., Kormann, D., and McDaniel, P. Searching for privacy: Design and implementation of a P3P-enabled search engine. In *Proceedings of the 2004 Workshop on Privacy Enhancing Technologies*, pp. 26-28.

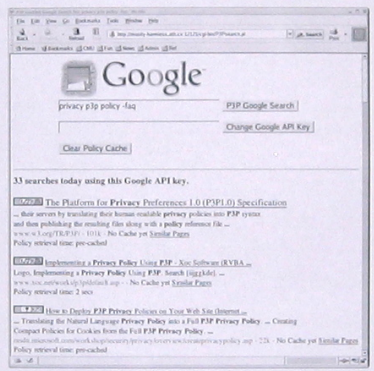
Architecture



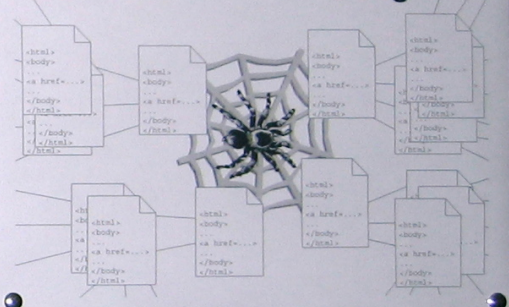
Policy Retrieval

- Problem: performance bottleneck
- Solution: parallel policy requests





Proactive Caching



Presentation

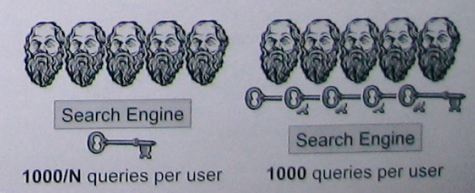
- Custom APPEL rule sets in addition to predefined low, medium, high rule sets
- Save rule set choice in cookie
- Privacy Bird Icons
  - Green: policy passes rule set
  - Yellow: no policy
  - Red: policy fails rule set

Cache Query

- P3P policy cache as a research tool
- Use special queries:
  - p3p:<website> *display cached policy*
  - p3pstat: *stats about policies in cache*
    - Total policy count
    - Percent deployment
    - Multiple policies/site count
  - appel:<ruleset> *test policies against rule set*
    - Percent matching policy

Scalability

- Google API allows 1000 queries per day
- Let users input their own Google API key



Instant Messenger Privacy Concerns & Remedies

Ryan Mahon
rmahon@andrew.cmu.edu

1

Concerns

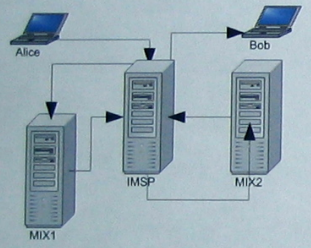
- Exposed Information
  - Conversations
  - Social Networks
  - Internet Presences
- Exposed To
  - IMSP
  - ISP
  - Snoopers

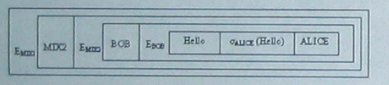
2

Private Conversations With Existing Architecture

- Chaum's Mix Nets [1981]
- Onion Routing via other IM Clients
- Advantages: Interoperability, Privacy
- IMSP, ISP, snoopers
  - Cannot tell what is being said
  - Cannot tell who is being spoken to
- Disadvantages: Latency, Centralization

3



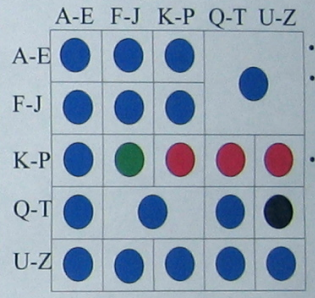


4

Private Conversations With Peer-To-Peer Infrastructure

- Content-Addressable Networks: Overlay network by Ratnasamy et al. [2001]
- Crowds: Anonymity tool by Reiter and Rubin [1999]
- Advantages: Decentralized, Better Latency-Privacy Tradeoff
- Disadvantages: Interoperability, Misbehavior-Detection

5



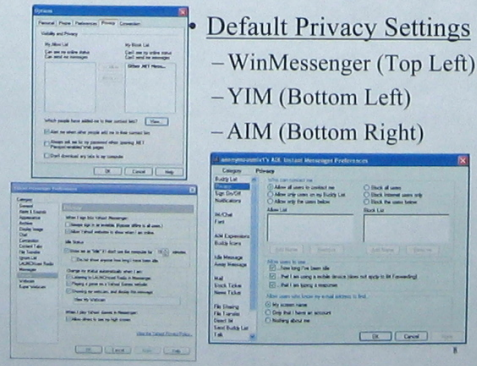
- 2-D CAN
- "UTAH" contacting "ILLINOIS"
- No intermediary can tell where message started

6

Preventing Presence Exposure

- Focus: AIM, YIM, & WinMessenger
- Three Main Problems (all solvable):
  - Poor Default Privacy Settings
  - Lack of Granularity in Configurations
  - No Notice of Presence Viewing

7



- Default Privacy Settings
  - WinMessenger (Top Left)
  - YIM (Bottom Left)
  - AIM (Bottom Right)

8

Conclusions

- Future Work
  - Implementation of Architectures
  - Evaluation: Fault Tolerance, Latency
  - Examination of Legal and Ethical Issues
- Privacy in Current Popular Instant Message Systems is Poor, But Fixable!

9


Discovering Information Leaks
Peripheral Privacy Notification for Wireless Networks
Motivation
Wireless Networks
Designing for Privacy
User's Dilemma
Models of Privacy
Social Translucence in Digital Systems
Surveillance / Capture Model
later
understanding
speaker
friday
Boundary Regulation Process
Peripheral Display
Balance Between Privacy and Utility
Implementation
Experimental Trial
Google
Braden Kowitz
Carnegie Mellon University

Analyzing Software Architectures for Privacy

Jeff Barnes (jmbarnes@cs.cmu.edu)

08-733 Privacy Policy, Law, and Technology
Carnegie Mellon University

1. Background

Organizations use privacy policies for many reasons:

- To demonstrate their privacy commitment to consumers, regulators, and industry groups
- To protect against litigation
- To assess their own compliance with relevant law
- To engender trust

But what happens when the privacy policy is wrong?

- **2000:** Chase Manhattan Bank violated its own privacy policy by selling personal information about 18 million customers to marketers. Chase agreed to correct its privacy practices and pay the New York attorney general $101,500.
- **2000:** Due to a software error, a subsidiary of Sony Music transmitted personal e-mail addresses to marketers in violation of its privacy policy. The company agreed to take measures including hiring an independent auditor and paid $75,000.
- **2004:** The FTC fined Gateway Learning Corp. for renting the personal information of users of its flagship product, Hooked on Phonics.
- **2006:** New York sued Gratis Internet for selling personal information to a marketer in violation of its own privacy policy. A $1.1M settlement was reached.

Companies misunderstand their own privacy practices and consequently misrepresent themselves, underestimate their legal culpability, and damage their reputations.

Why is this a hard problem?

Part of the problem is human misunderstanding or ignorance of organization privacy policies.

But another problem is the complexity of the software systems that manage and store personal information.

Even the developers of a software system may find it difficult to make statements about its privacy characteristics, because its complexity makes it difficult to infer how privacy-sensitive information travels through the system as a whole.

My approach is to use software architecture to confront this problem directly.

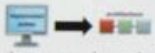
2. Software Architecture

Software architecture views software systems as comprising, at a high level, software components that communicate with each other through connectors.

Primary uses of software architecture include:

- Engineering a new system

- Reverse-engineering an existing system



Analysis techniques can be applied to both uses: analyzing the properties of proposed designs for a new system and analyzing the properties of an existing system.

Such properties include performance, security, etc. Privacy can be analyzed in this way too.

3. Conceptual Overview

Key idea: Rather than trying to determine the privacy properties of a software system holistically, evaluate the privacy behaviors of its constituent elements and model the flow of privacy-sensitive data through the system.

Why does this make sense?

Figuring out the privacy properties of an entire system is hard. But figuring out those of a small software component should be easy for the software engineers responsible for a project.

Then, we can apply our analysis to infer the global privacy properties of the system from those of the constituent elements.

4. Theoretical Framework

Graph theory provides a mathematical model of our approach.

We can view a software architecture as a directed graph where the vertices are components and the edges are connectors.

Model the set of privacy-sensitive information as a set of labels, like `contact` for contact information.

Annotate each vertex with a set of labels indicating the privacy-sensitive information that enters the system at that component.

Annotate each edge with a set of labels indicating the privacy-sensitive information that may pass through that connector.

Finally, use these annotations to model how different types of data flow through the system.

5. Example

Consider a company that collects sensitive user information (name, contact information, Social Security Number) through a Web interface. All of this information is stored in a secure database of user information. Individuals' names and contact information are periodically extracted from this database and sent to a marketing database to be shared with marketing partners, in accordance with the privacy policy. SSNs are not supposed to be sent to the marketing database.

This architecture violates the policy, because SSNs can flow through the DataManager to the MarketingDatabase, even though they cannot flow directly from the UserDatabase to the MarketingDatabase.

6. Implementation

An **architecture description language (ADL)** is used to describe software architectures in a clear and unambiguous way. A typical ADL:

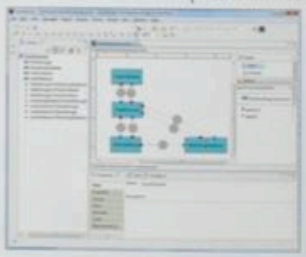
- Provides a way to describe components and connectors and how they are hooked up
- Allows elements of an architecture (components and connectors) to be annotated with user-defined properties such as performance attributes
- Allows definition of **architectural styles**—classes of software architectures. An architectural style is characterized by a vocabulary of architectural elements and a set of constraints on how they may be assembled.

Acme is an ADL developed at CMU. I picked it in part because of its GUI, **AcmeStudio**, which allows easy usage of Acme, provides graphical representation of architectures and supports extensions for analyses.

I implemented my privacy analysis in Acme by:

1. Developing a style to accommodate the expression of privacy-relevant information
2. Developing an external privacy analysis for systems of that style

This is a screen shot of our example in AcmeStudio:



7. Future Work

- Basic improvements: better UI, more sophisticated definition of data types
- Sophisticated description and analysis of where and how data exit the system
- Model information that is anonymous or pseudonymous but privacy-sensitive.
- Check conformance between an implemented system and its described privacy characteristics
- Check conformance with a privacy statement

Porting Privacy Bird to Firefox

William Haines
Guillermo Marinero
Steven Novick

Why Port Privacy Bird?

Privacy Bird: A continuous P3P user agent developed by AT&T and maintained at Carnegie Mellon

"The most complete P3P tool currently available"

Currently, it **only works with Internet Explorer**

Can we create a port of Privacy Bird that:

- Allows greater user access
- Maintains Privacy Bird's core functionality

But Everyone Uses IE...

Estimated Browser Usage Share

A sizeable proportion of users do not use IE or even Windows!

An ideal port would be browser and OS independent

Our Proposal

In our port of Privacy Bird to Firefox we sought to:

- Engineer a core P3P evaluation process based on XSLT transformations, a cross-platform specification
  - The core should transfer directly to any future ports
- Use standard technologies and APIs supported by Firefox: Javascript, XML, XSLT, XUL
  - This architecture is extensible and cross-platform friendly
- Maintain the feel of the original Privacy Bird
  - Allow users to select between three levels of privacy
  - Update the user interface for Firefox
  - Future work will include customized privacy levels

Technological Resources

We rebuilt Privacy Bird from scratch using:

- XML (Extensible Markup Language)
  - P3P is a subset of XML, a general purpose markup language
  - Since Privacy Bird was first implemented, XML parsing has become a commodity task
- XSLT (Extensible Stylesheet Language Transformations)
  - A cross-platform method to transform one XML format into another
  - We used it as a cross platform P3P parser!
- XUL (XML User Interface Language)
  - Firefox's cross platform, XML-based language for UI design
- Javascript
  - Lightweight, semi object-oriented, cross-platform scripting language
  - The glue that holds it all together

Privacy Bird's Architecture

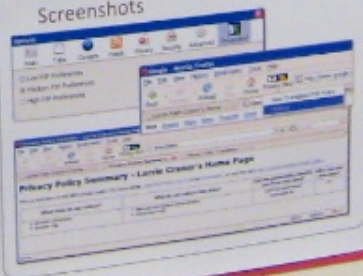
- Browser Request: The user navigates to a website
- Retrieval of User Preferences: The browser fetches the user's stored privacy preferences
- P3P processing: A P3P policy is retrieved from the website and transformed into a easy to parse format
- Notification: The browser UI notifies the user whether his or her privacy preferences match the policy of the site being visited

Privacy Bird's Implementation

P3P Discovery → P3P Retrieval → P3P Transformation → Interpretation → Notification

- P3P Discovery: This module detects if the web site contains a P3P policy
- P3P Retrieval: The P3P is retrieved from the website
- P3P Transformation: The retrieved P3P is transformed into an easy to parse format using XSLT
- Interpretation: This module checks the transformation result for its consistency with the user's privacy preferences
- Notification: Alerts the user whether or not a match occurred

Screenshots



Conclusions and Future Work

- We validated the utility of re-architecting Privacy Bird, making it:
  - Modular
  - Reusable
  - Cross-platform friendly
- We laid the groundwork for future development
  - Hopefully ports to Safari and Opera
- Future work
  - Support for P3P 1.1
  - Enable users to define their own preferences
  - Various UI improvements like sound and notification location options

What is Spyware?

- Wikipedia says: a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user
- Unwanted for obvious reasons, but can also slow your system

Spyware: Are You Really Protected?

Jackie Milhans
17-801

Results

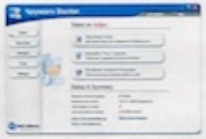
Brand and Model	Price	Files Detected	User Friendliness	Scheduled scans	Auto Updates	Protect Browser	Breakdown of Types	Shows Threat Level	Justifies	Time	Speed Level
McFunda Spyware Scanner	$20	1,1	High	+	+	+	+	+	High	4h	1,4
Spybot Search and Destroy	Free	1,1	High	+	+	+	+	+	High	4h	1,4
Lavasoft Ad-Aware SE Personal Edi	Free (upgrade $20)	1,1	High	+	+	+	+	+	High	4h	1,4
Microsoft Anti-Spyware Beta1	Free	1,1	High	+	+	+	+	+	High	4h	1,4
Webroot spy sweeper	Free 30d upgrade	1,1	High	+	+	+	+	+	High	4h	1,4
PCTools Spyware Doctor	Free	1,1	High	+	+	+	+	+	High	4h	1,4
Max Secure Spyware Detector	Free	1,1	High	+	+	+	+	+	High	4h	1,4
NoAdware	$30	1,1	High	+	+	+	+	+	High	4h	1,4
Spyware Doctor	$30	1,1	Med	+	+	+	+	+	Med	4h	1,4
Spyware Eliminator	$30	1,1	High	+	+	+	+	+	High	4h	1,4

Examples of Spyware

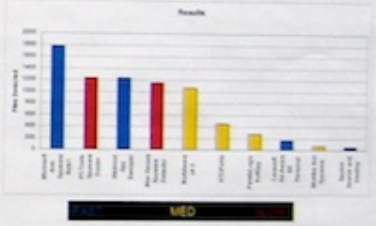
- Pop-ups
- Activity trackers
- Information Theft
- Routing HTTP requests
- Recording Key-logging
- Dialers

Anti-Spyware Tools

- Which One Is Best?
- How to Choose?



Which Should You Use?



How Does it Get On My Computer?

- Bundled Software
- Drive-by Downloads
- Promotes itself as useful
  - GAIN
  - Bonzi Buddy
- Pop-up Offers disguised Windows dialog

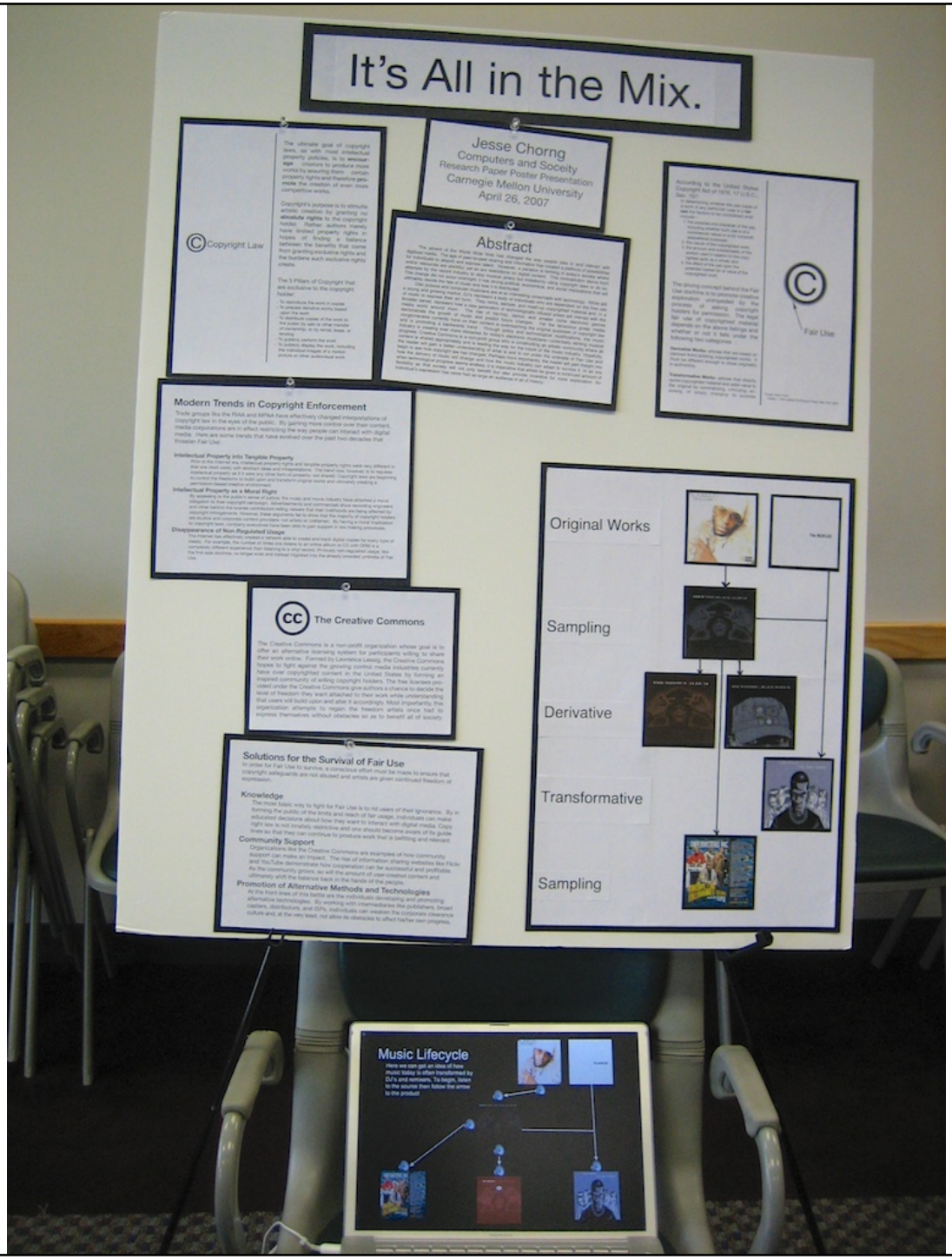
Procedure for Testing

1. Start with a Clean Drive
2. Download KaZaa
3. Download a Anti-Spyware Tool
4. Run Spyware Scan

Windows Users Best Bets Are:

1. Microsoft Anti-Spyware Beta
2. Webroot Spyware Sweeper
3. PCTools Spyware Doctor
4. Max Secure Spyware Detector
5. NoAdware

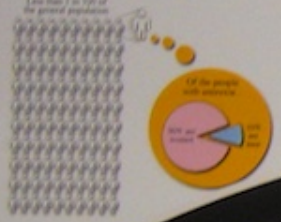

1
How Technology Drives Vehicular Privacy
Presented by A. McDonald
Legal Background
2
Fourth Amendment
Protects against "unreasonable search and seizure."
Requires probable cause and particular description of what will be searched.
Courts limited applicability to cars
Car can be moved to new jurisdiction while law enforcement seeks warrant.
Public thoroughfare - plain sight - expectation to privacy limited.
Because limited expectation to privacy in cars, therefore no expectation in glove compartment.
Black Boxes
3
What they are
Similar in concept to airplane black boxes.
What they do
Record and store crash data: seat belt use, airbag deployment, speed at impact.
Initial use
Car companies improved air bags.
New uses
Understanding causes of accidents.
Court cases: determining fault, especially fatalities.
Monitoring teens, real time feedback & logging.
Insurance companies: blame & rates.
Traffic Cameras
4
What they are
Multiple types: red light, traffic patterns, automated speed traps, interactions with police in squad cars.
What they do
Infra-red. Record make model, color of cars. Drivers, passengers. Time of image, speed of car. Software for license plate & facial recognition.
Initial uses
Make us safer. Deter running red lights by fines.
Optimize post-game traffic, ambulance routes.
New uses
Profit: DC: $18M red light cameras, 1999-02. Speed traps: $9M in first 7 months. Oakland police: avoid lawsuits.
Problem: increase accidents. Solution: timing.
GPS transponders
5
What they are
Determines location and elevation of transponder.
What they do
Transponder sends signal to satellites, triangulate location. Precision: 65 ft. Can be 4 inches with error correction software. Depends on (and stores) time.
Initial use
Department of Defense. Detect missile launches.
New uses
Map systems in cars.
Placed on cars to track them. FBI does not need a warrant in some jurisdictions, does in others.
OnStar
6
What it is
Commercial system for safety. All GM cars, 2007.
What it does
Mobile phone + GPS + black box.
Initial use
Prevent theft, open doors, voice activated phone, reports accidents.
New uses
FBI uses OnStar to listen to drug dealers' conversations & track movement. No way to turn it off.
OnStar reports all accidents to police, even when requested not to.
EZPass and Related Systems
7
What they are
RFID passes for toll collection.
What they do
Pass sends ID to reader. Looks up ID to debit account. Records where it was read.
Initial use
Speed toll traffic, decrease pollution.
New uses
FBI cited using EZPass data without judicial oversight for PATRIOT re-authorization.
Highway Use Tax Proposals
8
What they are
Electronically collected mileage fee.
What they do
Either GPS or cameras to determine road use, calculates fee, debits car owner's account.
Initial use
Replace lost revenues from gas taxes (presumption: move to hybrids.)
New uses
War on terror, war on drugs.
Insurance companies can calculate mileage, speed - and change fees.
Automatic speeding & HOV fines.
Potential Privacy Invasions
9
Black boxes | Traffic Cameras | On Star | GPS | EZPass | Highway Use Tax
Legal risk: accidents: ✓ ✓ ✓
Legal risk: divorce: ✓ ✓ ✓ ✓ ✓
Traffic fines: ✓ ✓ ✓
Insurance company: ✓ ✓ ✓ ✓ ✓ ✓
Family surveillance: ✓ ✓ ✓
Government surveillance: ✓ ✓ ✓ ✓ ✓ ✓


It's All in the Mix.
Jesse Chorng
Computers and Soceity
Research Paper Poster Presentation
Carnegie Mellon University
April 26, 2007
Copyright Law
Abstract
Fair Use
Modern Trends in Copyright Enforcement
The Creative Commons
Solutions for the Survival of Fair Use
Knowledge
Community Support
Promotion of Alternative Methods and Technologies
Original Works
Sampling
Derivative
Transformative
Sampling
Music Lifecycle

Digital Enhancement of the Female Figure: Harmful Fallacy of Perfection or Fair Marketing Tool?

Background

What happens when women of society are highly enhanced images of women and perceive them as real-life beauties? Reuters Health, a world-wide leader in medical news, stated in an article about eating disorders, "…advertisers heavily market weight-reduction programs and present anorexic young models as the paradigm of sexual desirability…. One study reported that teenage boys and girls who made strong efforts to look like celebrities of the same sex were more likely to be constant dieters." [4]. Although anorexia afflicts only about one out of one-hundred people, it is a growing disease that's nine times more likely to affect women. Additionally, the United States holds the largest annual mortality rate of anorexics (31.8 per year in January 2004) than any other country, and has been rising. It is followed by Japan (18.6), then Germany, then Brazil and Canada [5]. It is possible that digital enhancement technology helps promote this disease.



Before Retouching [1]

The picture to the right has been digitally enhanced such that the model has undergone so-called digital rhinoplasty and hair implants. Also, her face has been reconstructed to look thinner, her eyes and teeth appear to be whiter; her skin tone is lighter and brighter; and her hair has richer color and contrast in the enhanced photo.

After Retouching [1]

Issue

Supermodel Tyra Banks commented on E! 101 Best Kept Hollywood Secrets that while modeling for Victoria's Secret, a popular lingerie store, her buttocks and thighs looked like someone had squeezed it and it had stayed, "but no one would know that." No one would know that because Hollywood's Best Kept Secret Number 66 is that actresses, actors, and models have their photos digitally retouched [6].

While airbrushing photos has been a photographer's tool for years, software programs such as Adobe, MakeUp Pilot™, AKVIS Stamp, and Adobe Photoshop have raised photo retouching to a new level. While manual airbrushing was commonly used to overlay wrinkles or other skin disorderations; now, software programs actually change a model's face and body structure, overall skin tone, eye color, muscle tone, lack of bone protrusion, and any other attributes seen as flaws.

Combined with women in Hollywood's efforts to be wait-like to fit the fashions, this software produces images of women who have unnatural eye sockets; tan porcelain skin; perfectly symmetrical faces; and elongated, thin bodies; and enlarged breasts. Yet, these images are published in advertisements to portray real Hollywood stars, not cartoon images, to society. this study will examine the use of photo enhancement software and the possible effects it has on society, including phenomena such Western culture's sales of diet products, Kodak's new slimming camera [7], and the trendy Korean shrangs who alter each own photos of themselves.

Digital Enhancement Programs

There are many programs that marketers can use to enhance photos. A few such programs include: Adobe® Photoshop®, Corel Paint Shop, Adesiga, and AKVIS Stamp. The pictures on the right are screen shots of photo editing within a free trial of MakeUp Pilot™. One can see that there are significant differences in the photos, including skin tone evenness, clarity of complexion, size and color of lips, whiteness of teeth and eyes, number of lines on face, and size of body frame. It is important to note that these photos are not professionally enhanced, which projects how much more believable a professional artists' photo manipulation can be. In addition, MakeUp Pilot® is a very simple program with blurring and color burning capabilities. With more intricate tools, an artist can fully alter the appearance of a model, as seen in the photo of the hair model above, where the photo enhancement has provided digital rhinoplasty and hair extensions.

The most intricate and popular photo editing program for professional photo editors is Adobe® Photoshop® CS3. This software package is equipped with Smart Filters, which are "non-destructive" in that they allow the artist to "visualize changes without offering pixel data" it also contains a Quick Selection tool that allows one to briskly outline the edges that he wants to enhance, and the software will then guess what the artist is intending to define and allow him to choose from many functions such as blur or sharpen to create the effect that he wants. CS3 also offers "enhanced 32-bit high dynamic range (HDR) support," which allows one to work on 32-bit (very large) photos with the fullest available photo contrast. CS3 supports this high quality image processing via new algorithms [14].

Screen shot of a photograph of my friend Sarah (Right) and me (Left) before digital enhancement.

Screen shot of the same photo, enhanced using a program called Makeup Pilot(R). A trial version of thesoftware can be found at: http://www.color-pilot.com/makeup.html.

Experiments Concerning Women and Advertising

Body dissatisfaction can be defined as one's unhappiness with her appearance or one's distorted view of her appearance; and, it is more frequently diagnosed in women than in men [8]. As body dissatisfaction can culminate into dangerous eating disorders and other behaviors, there have been many studies in the past that attempt to answer how women in become unhappy with their body. Although the actual body enhancing software was not directly addressed, a study at Kenyon College found that an extensive meta-analysis "supports the sociocultural perspective that mass media such as fashion magazines and television products promote, if not establish, a standard of slender beauty that leads many females to feel badly about their weight and shape," [8]. This conclusion stemmed out of the compilation of several studies where women were surveyed about their self perception while viewing pictures of models.

Similarly, a study at the University of Toronto "examined the changes in women's mood states resulting from their viewing pictures in fashion magazines of women who represent the thin ideal," [9]. This study surveyed 118 female college students (mean age of 21) about their own body image. After one week, half of the women, the control group, were shown slides of images that contained no women. The other half were shown images of fashion models from current magazines. Both groups then filled out the survey again. The study found that "women were more depressed ($R^2 = 0.745$, $p < .05$) and more angry ($R^2 = 0.73$, $p < .01$) following exposure to slides of female fashion models," [9]. Therefore, the study concluded that the ideal female, as advertised in fashion models today, has a negative effect on women's moods, and probably does aid in causing body dissatisfaction.

While neither of these analyses directly address photo enhancement technologies as an independent variable, their findings suggest that photo enhancement technologies help produce idealistic images of women that negatively affect their mood and self perception. Still, this statement could be further supported by testing women's self perception and mood as in the previous studies while assigning photo enhancement to be the independent variable. That is, one could display several raw photos of models to a control group of females and ask them questions regarding their self perception and mood. Then, one could display the same photos, but enhanced, to a test group of females and ask them the same questions. Considering a large enough sample size, if the test group of females show more body dissatisfaction and negative moods, the study could conclude that photo enhancement software is a technology that has made an impact on the psychology of women in society. (Note: Although this study has not been conducted, a suggested survey for further work is appended to the report supplementing this poster.)

Vogue cover [11]

Ethics

Before, after, and the changes made during the image enhancement [12]

In a 2004 Computing and Philosophy Conference, Canberra paper, Aaron Quigley distinguishes between original photo manipulation, while taking a picture, and secondary photo manipulation, changing elements of the photo for the photographer's gain. "The former type of manipulation can be a matter of routine colour correction - changing colour in an image to correct unintended technical flaws - the pejorative form - changes reality for the sake of news and sensationalism or aesthetics," [16]. Quigley goes on to mention journalistic values by Fred Mann, which involve establishing fairness, credibility, accuracy, and news judgment in the photographs. Whether or not these will be applicable to photographic advertisements will be evaluated within ethical frameworks in the supplementary paper.

When making a moral judgement on whether photo enhancement is ethical, one should subject the topic to ethical frameworks to gain a broad outlook. The frameworks that will be analyzed are the following:

1. *Kantianism*, which employs the categorical imperative (no man should be used as a "means to an end" and all actions should be universally sound.
2. *Utilitarianism*, a form of consequentialism that aligns an action with good if it benefits someone (act utilitarianism) or society (rule utilitarianism)
3. *Subjective Relativism*, which allows an individual to be right if he is doing what he considers right.
4. *Social Contract Theory*, "where morality is the result of an implicit agreement among rational beings who understand that there is a tension between self-interest and the common good," [15].

Graffe Picture (Airbrushed of Katie Couric soon after the broadcasted show she was on here. Right) The same picture of Couric, obviously edited, released four months later in a magazine cover by GQ [17].

Conclusion

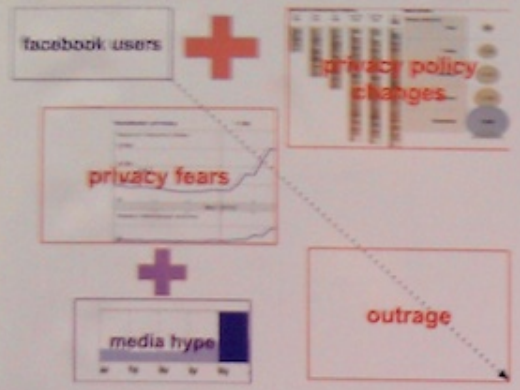
It is difficult to absolutely answer whether digital enhancement of the female figure is a harmful fallacy of perfection or fair marketing tool. Because previous studies reveal that women are adversely affected by images of the thin ideal woman, it can be reasonably conjectured that digital enhancement of the female figure is a harmful fallacy of perfection to all women. Yet, because marketers are not quite photojournalists, their images are not held to the same truthful standards; thus, digital enhancement could be considered to be a fair marketing tool. Expanding upon these viewpoints in ethical frameworks, the supplementary paper concludes that further research should be conducted to determine whether society as a whole benefits from this technology. This research should digital enhancement as the only independent variable to answer the following questions: Do women have negative effects on their mood and their self image when viewing digitally enhanced photos? By how much are women more persuaded to buy a product when it is endorsed using women who have been digitally enhanced? And, does society value the right to market a product with digital enhancement more or less than the possible effect it may have on women? An evaluation of the answers to these questions will determine whether society deems digital enhancement of the female figure as ethical. Finally, this analysis would lead to what kind of policy, if any, should be placed on digital enhancement of the female figure.

Before/After Retouching [1]

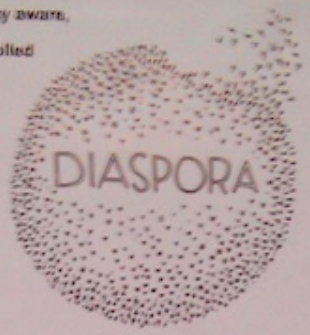
Sources

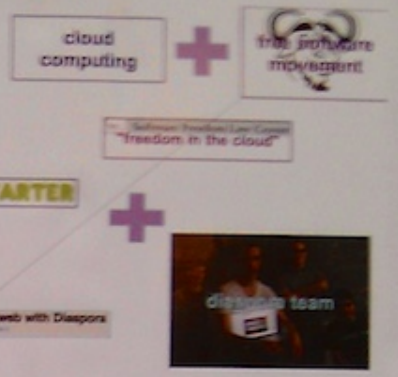
[1] Hypnotic.com [2] http://newsearch.com/newsarchives/search-kid.bk1019.html [3] AMAN, M.G. (2001). The eating disorders, in DE Dale, BD Federman, eds., Scientific American Medicine, vol. 3, chap. 15, pp. 1-7. New York: Scientific American. [4] 6.5.2.4 MC, 2001. Eating disorders. Reuters Health. http://www.medscape.com/viewarticle/408.2004 [5] WATCHMAKER.COM. 2004. Eating disorders by country. Mortality Statistics. http://www.watchmaker.com/gp/ref=nav_sdd_dk/002-8789-4409 [6] E! ENTERTAINMENT TELEVISION, INC. 2007. 101 Best Kept Hollywood Secrets. E! Entertainment Television. [7] COMBADIS, LUDOVIC. 2006. Digital camera focus on carried reality. DMT News.com. http://news.cnet.com/Digital-camera-focus-on-carried-reality/2100-1041_3-6130377.html. [8] T. GROSZ, L.M., LEVINE, M.P. AND MURNEN, S.K. 2001. The effect of experimental presentation of thin media images on body satisfaction: A meta-analytic review. International Journal of Eating Disorders, 31, 1, 1-16. [9] FRIMER, L., TORER, R. AND ROSENBERG, F. AND H. TYCHOLIZ. 1999. The effects of the ideal of female beauty on mood and body satisfaction. International Journal of Eating Disorders, 25, 3, 323-328. [10] http://www.saddleback.edu/fac/3270/3270f1.jpg [11] http://newsweek.org/images/newsweek.jpg [12] http://www.photoshop.com/products/photoshop/photoshop-family/photoshop_overview.pdf [13] QUIGLEY, A. 2003. Accepting manipulation or manipulating what's acceptable? In Selected Papers From Conference on Computers and Philosophy - Volume 37 J. Weckert and Y. Al-Saggaf, Eds. ACM International Conference Proceeding Series, vol. 101. Australian Computer Society, Darlinghurst, Australia, 59-64.

Nicole Hayward April 26, 2007



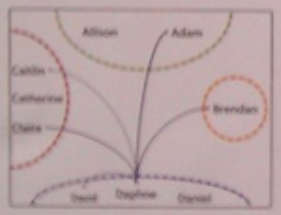
Diaspora, "The privacy aware, personally controlled do-it-all open source social network."





OpenSocialWeb Stack

- User authentication with OpenID
- API authorization with Oauth
- Distribution of updates and federation with OStatus
- Syndication of activity to and from other networks with Activity Streams
- User metadata querying with WebFinger
- Realtime-ification with PubSubHubbub
- Widgets with OpenSocial



Top 6 Privacy Goals

- All network data is held by the data's contributor
- Information sharing between two nodes in the network is not intermediated by a third party
- Users have real effective control over what is shared with whom and when
- The network's social graph is decentralized, not known or discernible to any particular party
- Users can revoke from the network any data which they have contributed to it
- No transmissions can be read by intercepting third parties

Alpha Release

"pushed back more technical features like plugins and APIs in favor of simple and high value features"

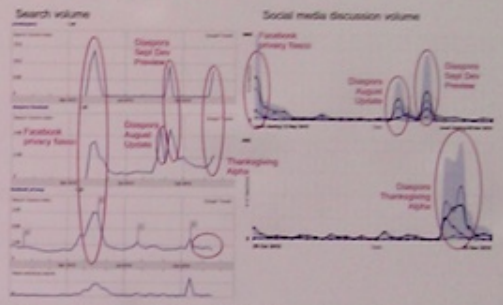
- November 23rd
- Invite only pod hosted by the team

Future Goals

- Continuing focus on security
- More extensibility and third-party client APIs
- Better documentation
- Easier upgrade path
- Cleaner code

Features	Alpha Status
Internationalization	Yes, problems with gender
Data Portability	Yes, not standards based
Facebook Integration	Yes
Seed Migration	Delayed
People Search	No, desired

The Future: An End or Simply a Means?



Most of the public is, for now, satisfied with the incumbent market leader – when there are no fascia.

Though no ongoing rabid demand, there is significant general interest in the potential of a privacy-focused alternative.

The free software movement is developing high hopes for Diaspora.

Significant investment has begun in projects counting on the continued development and eventual success of Diaspora as a product.

The Diaspora Team has significantly upgraded their commitment to the project. It is no longer just a Summer's exercise.

Developer Preview Release

"pushed back more technical features like plugins and APIs in favor of simple and high value features"

Highlights

- September 15th
- Source code released under AGPL License
- Code stored at GitHub

Aspects

- Separate faces you show the world
- Groups used as a basis for access control
- Separate statuses, messages, and photos

End to End Encryption

- Protects the contents of messages in transit
- Only intended recipients can view content

Features	September 15th Status
End to End Encryption	Yes, including photos
Third Party API	Delayed
Sharing Messages and Photos	Yes
External Service Integration	Delayed
Standards Compliance	Delayed
OpenID Provider	Yes, no longer planned

Privacy Evaluation

"pushed back more technical features like plugins and APIs in favor of simple and high value features"

Feature	Implication
Encryption	Communications are private between individuals
Signed Messages	Authentication of individuals
Open Source	All practices are transparent, privacy issues may be addressed by the community directly
Data Portability	Users are not bound to their pod or even to Diaspora
Aspects	Users can present completely different information to others
Local Data Retention	All user data is retained on the user's pod and can be deleted from the network at will
Direct Relationships	Users must explicitly add another user before any information is shared

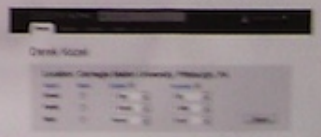
Location User Interface

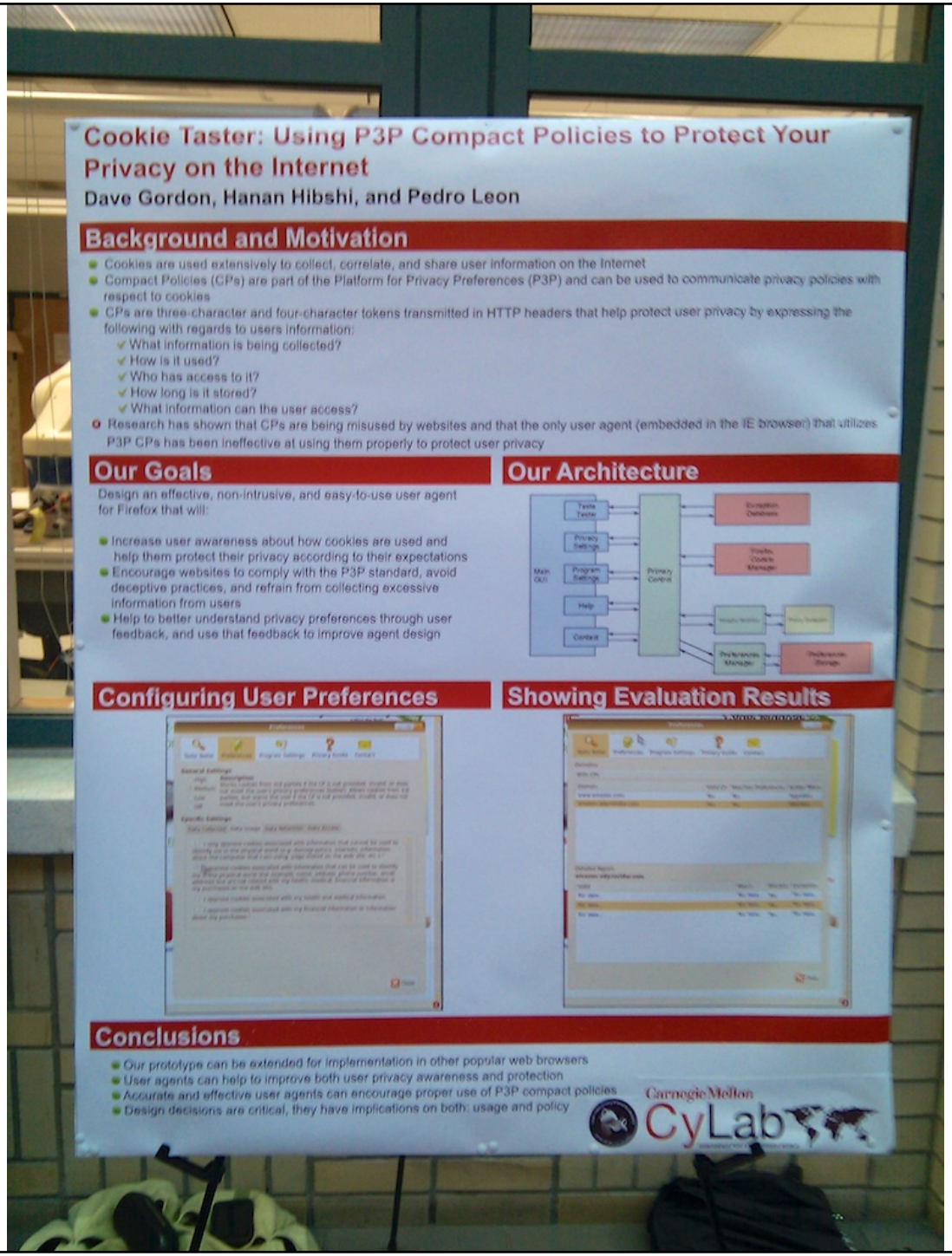
Design Goals

- Simple, Understandable Controls
- Natural access controls
- Intuitive variable precision of location
- Option to expire old location data

Future Considerations

- Ability to falsify location
- Warning before sending conflicting locations to individuals in multiple aspects
- Location based customization without leaking information to third parties




Cookie Taster: Using P3P Compact Policies to Protect Your Privacy on the Internet
Dave Gordon, Hanan Hibshi, and Pedro Leon
Background and Motivation
Cookies are used extensively to collect, correlate, and share user information on the Internet
Compact Policies (CPs) are part of the Platform for Privacy Preferences (P3P) and can be used to communicate privacy policies with respect to cookies
CPs are three-character and four-character tokens transmitted in HTTP headers that help protect user privacy by expressing the following with regards to users information:
What information is being collected?
How is it used?
Who has access to it?
How long is it stored?
What information can the user access?
Research has shown that CPs are being misused by websites and that the only user agent (embedded in the IE browser) that utilizes P3P CPs has been ineffective at using them properly to protect user privacy
Our Goals
Design an effective, non-intrusive, and easy-to-use user agent for Firefox that will:
Increase user awareness about how cookies are used and help them protect their privacy according to their expectations
Encourage websites to comply with the P3P standard, avoid deceptive practices, and refrain from collecting excessive information from users
Help to better understand privacy preferences through user feedback, and use that feedback to improve agent design
Our Architecture
Configuring User Preferences
Showing Evaluation Results
Conclusions
Our prototype can be extended for implementation in other popular web browsers
User agents can help to improve both user privacy awareness and protection
Accurate and effective user agents can encourage proper use of P3P compact policies
Design decisions are critical, they have implications on both: usage and policy
Carnegie Mellon
CyLab

A Survey and Review of Privacy-Related Extensions for Mozilla Firefox

Aaron J. Couch
Carnegie Mellon University
Heinz College
aaroncouch@cmu.edu

Introduction

"Privacy software" is available to users to address the concerns and problems associated with the distribution of personal information online.

Fears of ***identity theft***, the annoyance of ***unwanted marketing***, and the general ***desire to be left alone*** are the greatest drivers of the market for privacy software.

This project is intended to survey and review **extensions** for Mozilla Firefox that offer ***privacy-related functionality***.

Firefox extensions offer a means of altering the web-browsing experience to protect personal and private data. With some extensions, users can regain control over their online interactions and privacy.

Background

Firefox has seen growing adoption, now the second-most used browser at ***31.5% marketshare***.[1]

Users can be tracked and individually identified through a browser's **fingerprint**, which may include:

Cookies, IP addresses, user agent strings, system fonts installed, LSO's/SuperCookies, etc.

Companies specialize in ***aggregating browsing data*** to amass significant knowledge about **users' online activities** and **personal interests**.[2]

The most popular Firefox extension, Adblock Plus, has over ***12 million*** daily users.[4]

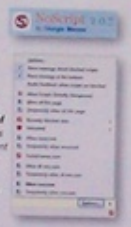
Evaluation

Various ***privacy-related extensions*** will be addressed in their implementation, usability, their adoption and reception by consumers, and their potential to serve as effective safeguards in the largely unregulated realm of online privacy.

- the ***installation process*** is carefully logged for each extension
- sequences of websites are browsed for ***usability*** and ***protection*** checking
- extensions' various ***configuration options*** are explored
- privacy-related ***functionalities*** are assessed using suitable analyses
- more ***objective measures*** of privacy-protection, such as counting cookies, are used where relevant

NoScript

- ***74 million*** downloads
- *"The best security you can get in a web browser! Allow active content to run only from sites you trust, and protect yourself against XSS and Clickjacking attacks"*



Advantages

- ***Successfully blocks all cross-site scripting attempts***
- Provides much ***customization*** and ***advanced features***, including an Application Boundaries Enforcer (ABE) module and HTTPS enforcement
- ***Large user base*** and ***dedicated developers***

Shortcomings

- Initially cripples media and social networking sites such as YouTube and Facebook
- Requires a high learning curve and much patience in initial configuration

Ghostery

- ***1.8 million*** downloads
- *"Providing transparent information and choices about internet-based advertising"*

Advantages

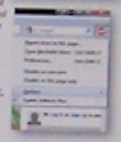
- Uses frequently updated filters to ***block known web-bugs*** (ensures that there are few false-positives)
- Provides helpful ***notifications***
- Provides a significant ***database*** of web-bug information to the user

Shortcomings

- Won't dynamically block new web-bugs

Adblock Plus

- ***100 million*** downloads
- *"Annoyed by adverts? Troubled by tracking? Bothered by banners? Install Adblock Plus now to regain control of the Internet and change the way that you view the web"*



Advantages

- Highly effective ***subscription-based block-lists***
- Can ***customize blocking*** to be privacy-centric, advertising-centric, or both
- Impressive cookie-blocking ***ability***

Shortcomings

- Without careful investigation of subscription settings, users may not be aware of the privacy-protections afforded

TrackMeNot

- Only ***451,000*** downloads
- *"A lightweight browser extension that helps protect web searchers from surveillance and data-profiling by search engines"*

Advantages

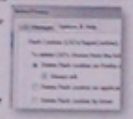
- ***Obfuscation of search terms*** over time enables search anonymization
- Effectively ***prevents*** Google and other search engines from producing a profile that reflects actual search patterns
- No negative ***usability*** impacts

Shortcomings

- Search engines may still know "who you are" based on an IP address (or, if logged into the provider's account, a "real" identity)

BetterPrivacy

- ***3.4 million*** downloads
- *"Ever wondered why you are still tracked though you tried everything to prevent it? BetterPrivacy is a safeguard which protects from usually not deletable LSO's on Google, YouTube and eBay"*



Advantages

- Removes so-called **SuperCookies** (Flash-based tracking files) upon exiting Firefox
- Can also set a timer for deleting these
- Doesn't alter the ***web-browsing experience***

Shortcomings

- Doesn't delete the Flash-player default cookie in the standard configuration (may allow for significant tracking)

RequestPolicy

- Only ***141,000*** downloads
- *"Be in control of which cross-site requests are allowed. Improve the privacy of your browsing by not letting other sites know your browsing habits"*

Advantages

- Simple configuration through regional ***cross-site scripting "white-lists"***
- ***Request-log feature*** which shows all cross-site requests in real-time

Shortcomings

- Some sites (like the *Wall Street Journal*) are completely crippled by initial configuration
- To regain access to content, especially multimedia, you must add entire domains to your white-list – true protection is lost

WOT – Safe Browsing Tool

- ***12 million*** downloads
- *"Would you like to know which websites you can trust? The WOT ("Web-of-Trust") add-on is a safe surfing tool for your browser. Traffic-light rating symbols show which websites you can trust"*

Advantages

- Simplistic nature of a ***traffic-light privacy-focused rating system***
- Shows full-page warnings when visiting some of the Internet's most hazardous sites (i.e., Wares)

Shortcomings

- Ratings seem to have little correlation to real internet privacy concerns
- The extension is overly-nagging with self-marketing

HTTPS Enforcing Extensions

- *Enforce secure connections to protect users from* ***data-interception & session hijacking***
- *Important for privacy-assurance*

HTTPS Everywhere

- Simple interface and straightforward configuration

Force-TLS

- More configuration needed to manually enter HTTPS-enabled domains

NoScript

- Includes more fine-grain functionality for HTTPS enforcement – suitable for a power user

Conclusions

Empowering users with the ***ability to control their online privacy*** is crucial in a political and legal landscape which offers negligible safeguards or reparations for privacy-intrusive practices.

Extensions frequently serve as ***front-line defenses*** against new or previously unexploited privacy threats, like *session hijacking*.

As web developers get trickier with *obscuring tracking activities*, extension developers do their best to fight back.

Increasing awareness of extension options is critical for all users to protect their privacy.

Top Recommendations:

Adblock Plus
Ghostery
BetterPrivacy
TrackMeNot
any of the HTTPS enforcing extensions

A note on *proxy-enabling extensions*

A variety of extensions are available for Firefox to enable anonymized web browsing via proxies. Proxy servers can act as intermediaries for Internet requests, effectively anonymizing users. While these extensions are not specifically explored here, users may want to investigate popular proxy extensions such as *Torbutton*, *FoxyProxy*, *AutoProxy*, and *QuickProxy*.

Works referenced

1. Kingsbury, Kevin. "Internet Explorer Market Share Falls Below 50% – Dot Crunches." The WSJ Digits Blog. Wall Street Journal, October 5, 2010. http://online.wsj.com/article/BT-CO-20101005-706575.html.
2. Eckersley, Peter. "How Unique Is Your Web Browser?" Proceedings of the Privacy Enhancing Technologies Symposium (PETS). Berlin, Germany: 2010. http://www.eff.org/files/browser-uniqueness.pdf.
3. Krishnamurthy, Balachander, Delfina Malandrino, and Craig E. Wills. "Measuring Privacy Loss and the Impact of Privacy Protection in Web Browsing." Symposium On Usable Privacy and Security (SOUPS). Pittsburgh, PA, 2007. 52-62. http://portal.acm.org.
4. "Adblock Plus – Statistics Dashboard." Add-ons for Firefox. n.d. https://addons.mozilla.org/en-US/firefox/addon/1865/ (accessed October 26, 2010).

For more info

Look at my draft paper!
Contact me at aaroncouch@cmu.edu

What is P3P anyway?

The **Platform for Privacy Preferences**

A **machine readable** description of website privacy practices in XML format

A snippet of a P3P description from Capital One...

Privacy Label Editor

A simple, graphical, web-based tool for creating P3P policies

Yoonhana Mahindhara
Taylor Rusck
Jeffrey Su

Privacy Policy, Law, Technology - Fall 2010

New Approach: A Graphical Editing Tool

Benefits:

- Web-based
- Faster to learn
- Point and click interface
- Easy update of existing P3P policies
- No need for user to be a P3P expert
- Easier to compare privacy policy with P3P policy to discover inconsistencies
- Easier to visualize differences between privacy policies

Privacy Policies on the Web Today

- Long
- College age reading level
- Full of legalese

A snippet from Capital One's online privacy policy - who wants to read and understand all of this?

What does this mean?

...insofar as you provide us with payment made on your account, the date of your login will depend upon the expiration date of the cookie on your current browser, in accordance with the previous sections, with the exception of ...

Sample Graphical P3P Policy

Capital One

Traditional Tools

Information Collected About Dynamic Data

Confusing?

Why are P3P and the Privacy Label Editor needed?

P3P - a standardized description of privacy policies

But what if the P3P policy for a website is created incorrectly?

•Capital One's P3P policy has numerous inconsistencies with its privacy policy

Privacy Label Editor - visual representation for viewing and editing P3P policy

Sample Graphical P3P Policy

Pittsburgh Dynamo

Using the Privacy Label Editor

Private, Inc.

Contact Information to Other Companies

Data breaches and identity theft

Data breach

- Personal data lost or stolen
  - How?
- Data breach may lead to identity theft (but not always, and not for all people involved)
- Many states have notification statutes
- What can organizations do to prevent?

Identity theft

- Fraudulent acquisition and use of a person's identifying information, usually for financial gain
- Range of offenses
  - Making purchases on someone else's credit card
  - Opening credit in someone else's name
  - Providing someone else's identity to get a job
  - Providing someone else's identity to avoid arrest, or to have someone else arrested
- How it happens
  - Physical theft, phishing, malware, computer security breaches, acquaintances, hospitals and nursing homes, ….

Data breach laws

- First enacted in CA in 2002 – SB 1386
- Most states in the US now have them
  - 47 states, DC, Guam, Puerto Rico, Virgin Islands
  - Alabama, New Mexico, and South Dakota do not
- Require notifying customers of PII data breaches
- Who must comply, definitions of PII, definitions of breach, types of notification, exemptions, etc. vary
- http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Pennsylvania Statutes
Title 73: Trade and Commerce
Chapter 43: Breach of Personal Information Notification Act
Effective: June 20, 2006

§ 2301. Short title. This act shall be known and may be cited as the Breach of Personal Information Notification Act.

§ 2302. Definitions. The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

"Encryption." The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

"Individual." A natural person.

"Notice." May be provided by any of the following methods of notification:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.

(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

(4) (i) Substitute notice, if the entity demonstrates one of the following:
(A) The cost of providing notice would exceed $100,000.
(B) The affected class of subject persons to be notified exceeds 175,000.
(C) The entity does not have sufficient contact information.

(ii) Substitute notice shall consist of all of the following:
(A) E-mail notice when the entity has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.
(C) Notification to major Statewide media.

"Personal information."
(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
(i) Social Security number.
(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.
(iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

"Records." Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

"Redact." The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data.

"State agency." Any agency, board, commission, authority or department of the Commonwealth and the General Assembly.

§ 2303. General rule.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 [FN1] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

(c) Vendor notification.--A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

§ 2304. Exceptions. The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

§ 2305. Notification to Consumer Reporting Agencies. When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy