Creating a research poster
December 10 Poster Fair

• During class in 4th floor Gates lobby

• 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 but TA can print for you if you plan ahead)
    • 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 large, easy-to-read font
  – Most text should be at least 20 point font, >36 point font is even better
  – 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
Towards Information Extraction From Natural Language Privacy Policies In Retail & News Sectors

Options: News Entertainment
- Key Features
  - News Entertainment
    - Services other just offering news?
    - Share behavioral data with other third parties?
    - Collection and usage of social media data increase 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

Methodology
- Identify key features in each sector
- Build a 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

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

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

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
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
    - Example: 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 involve 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
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)

<table>
<thead>
<tr>
<th>Title</th>
<th>Version</th>
<th>Certification?</th>
<th>Accreditation?</th>
<th>Summary</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verizon Wireless Policy</td>
<td>English</td>
<td>Yes</td>
<td>Yes</td>
<td>B88OnLine</td>
<td>13</td>
</tr>
<tr>
<td>AT&amp;T Wireless Policy</td>
<td>English</td>
<td>Yes</td>
<td>Yes</td>
<td>TrustE</td>
<td>15</td>
</tr>
<tr>
<td>Sprint Privacy Policy</td>
<td>English</td>
<td>No</td>
<td>Yes</td>
<td>FAQ</td>
<td>3</td>
</tr>
<tr>
<td>T-Mobile Privacy Policy</td>
<td>English</td>
<td>Yes</td>
<td>No</td>
<td>STMT</td>
<td>2</td>
</tr>
</tbody>
</table>

Why the Electronic Communications Sector?
- 220,000 subscribers in US
- 69,000 subscribers in Turkey

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.

Metada on Privacy Policies (TR)

<table>
<thead>
<tr>
<th>Title</th>
<th>Version</th>
<th>Certification?</th>
<th>Accreditation?</th>
<th>Summary</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turkcell Security and Privacy Policy</td>
<td>Turkish</td>
<td>Yes</td>
<td>Yes</td>
<td>TRU</td>
<td>61</td>
</tr>
<tr>
<td>Vodafone Privacy Policy</td>
<td>Turkish</td>
<td>Yes</td>
<td>Yes</td>
<td>VOD</td>
<td>1</td>
</tr>
<tr>
<td>Avea Security and Privacy</td>
<td>Turkish</td>
<td>Yes</td>
<td>Yes</td>
<td>AVE</td>
<td>1</td>
</tr>
</tbody>
</table>

Analysis of Privacy Policies (US)

Top Wireless Communication Companies

<table>
<thead>
<tr>
<th>US Market Shares (%)</th>
<th>TR Market Shares (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verizon</td>
<td>Turkcell</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Vodafone</td>
</tr>
<tr>
<td>Sprint</td>
<td>Avea</td>
</tr>
<tr>
<td>T-Mobile</td>
<td></td>
</tr>
</tbody>
</table>

Analysis of Privacy Policies (TR)

<table>
<thead>
<tr>
<th>Fair Information Practices Implementation</th>
<th>Turkcell</th>
<th>Vodafone</th>
<th>Avea</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Limitation</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Data Quality</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Purpose Specification</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Security Safeguards</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Openness</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Individual Participation</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Accountability</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
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

Enhanced P3P-Enabled Search Engine
Damon Smith
15508 Privacy Policy, Law, and Technology

Policy Retrieval
- Problem: performance bottleneck
- Solution: parallel policy requests

Serial Request Timeline

Parallel Request Timeline

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

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

Architectural

P3P-Enabled Search Results

Proactive Caching

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

Concerns

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

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

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

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

Default Privacy Settings

- WinMessenger (Top Left)
- YIM (Bottom Left)
- AIM (Bottom Right)

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!
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

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 an 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
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 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 33.1% of marketshare. Users can be tracked and individually identified through a browser’s fingerprint, which may include:
- Cookies
- IP addresses
- User agent strings
- System fonts
- Installed local storage

Companies specialize in aggregating browsing data to amass significant knowledge about users’ online activities and personal interests.

The most popular Firefox extension, Adblock Plus, has over 12 million daily users.

Evaluation

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

<table>
<thead>
<tr>
<th>NoScript</th>
<th>Adblock Plus</th>
<th>TrackMeNot</th>
<th>BetterPrivacy</th>
<th>RequestPolicy</th>
<th>HTTPS Enforcing Extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NoScript</td>
<td>Adblock Plus</td>
<td>TrackMeNot</td>
<td>BetterPrivacy</td>
<td>RequestPolicy</td>
<td>HTTPS Enforcing Extensions</td>
</tr>
</tbody>
</table>

**NoScript**
- 84 million downloads
- The best security you can get a web browser!
- "…and when you see a site that requires X-Scripting, you know we're there!
- Avoids clicking on malicious and phishing websites
- Blocks JavaScript, which is commonly the source of ad content

Advantages
- Blocks intrusive JavaScript
- Blocks malicious and phishing websites

Shortcomings
- Blocks JavaScript, which is commonly the source of ad content

**Adblock Plus**
- 134 million downloads
- "…and when you see a site that requires X-Scripting, you know we're there!
- Blocks JavaScript, which is commonly the source of ad content

Advantages
- Blocks intrusive JavaScript
- Blocks malicious and phishing websites

Shortcomings
- Blocks JavaScript, which is commonly the source of ad content

**TrackMeNot**
- 8.9 million downloads
- "…and when you see a site that requires X-Scripting, you know we're there!
- Blocks JavaScript, which is commonly the source of ad content

Advantages
- Blocks intrusive JavaScript
- Blocks malicious and phishing websites

Shortcomings
- Blocks JavaScript, which is commonly the source of ad content

**BetterPrivacy**
- 1.8 million downloads
- "…and when you see a site that requires X-Scripting, you know we're there!
- Blocks JavaScript, which is commonly the source of ad content

Advantages
- Blocks intrusive JavaScript
- Blocks malicious and phishing websites

Shortcomings
- Blocks JavaScript, which is commonly the source of ad content

**RequestPolicy**
- 84 million downloads
- "…and when you see a site that requires X-Scripting, you know we're there!
- Blocks JavaScript, which is commonly the source of ad content

Advantages
- Blocks intrusive JavaScript
- Blocks malicious and phishing websites

Shortcomings
- Blocks JavaScript, which is commonly the source of ad content

**HTTPS Enforcing Extensions**
- Blocks connections to sites that do not use HTTPS
- Blocks connections to sites that do not use secure sockets layer (SSL)
- Blocks connections to sites that do not use transport layer security (TLS)

Advantages
- Blocks connections to sites that do not use HTTPS
- Blocks connections to sites that do not use secure sockets layer (SSL)
- Blocks connections to sites that do not use transport layer security (TLS)

Shortcomings
- Blocks connections to sites that do not use HTTPS
- Blocks connections to sites that do not use secure sockets layer (SSL)
- Blocks connections to sites that do not use transport layer security (TLS)

**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 obfuscating 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
- Ghosdy
- 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


For more info
Look at my draft paper. Contact me at aaroncouch@cmu.edu.
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 Lorne Cranor for her guidance on the project, and our peers: Marya Sleeper, Zheng Sun and Yasmine Kandissoun for their help with the project.
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?

<table>
<thead>
<tr>
<th>Area of inquiry</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy at home</td>
<td>Closing bedroom doors, areas that are off-limits, knocking</td>
</tr>
<tr>
<td>Social privacy</td>
<td>Knowing their friends, always knowing where they are</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Reading texts, monitoring computer, parental controls</td>
</tr>
</tbody>
</table>

Preliminary Results

<table>
<thead>
<tr>
<th>Theme</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respect for teen → Privacy</td>
<td>P0, P1</td>
</tr>
<tr>
<td>A parent’s concerns override a teen’s right to privacy</td>
<td>P0, P1</td>
</tr>
<tr>
<td>Privacy as parent-teen negotiation</td>
<td>P0, P1</td>
</tr>
</tbody>
</table>

- 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
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

<table>
<thead>
<tr>
<th>Presence of Inappropriate Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
</tr>
<tr>
<td>Partially Agree</td>
</tr>
<tr>
<td>Disagree</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Individual's Identification of Inappropriate Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefer Help</td>
</tr>
<tr>
<td>Don't Want Help</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replies to Inappropriate Posts</th>
<th>Will Reply</th>
<th>Will Not Reply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identified</td>
<td>27%</td>
<td>34.61%</td>
</tr>
<tr>
<td>Anonymous</td>
<td>65.39%</td>
<td>73%</td>
</tr>
</tbody>
</table>

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.
**Demonstration of financial companies’ privacy practices**

**Privacy Bank**

**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 only on the main features, but also on communication and presentation.

**HOW?**

- PRIVACYBANK=
  - User-friendly Interface
  - Comprehensive and detailed data

**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!
Analyzing Software Architectures for Privacy

Jeff Barnes (jmbarnes@cs.cmu.edu)

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.
- **2004:** 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 used 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 easier 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.

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, Acme Studio, which allows easy usage of Acme, provides graphical representation of architectures and supports extensions for analysis.

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 screenshot of our example in Acme Studio:

7. Future Work
- Basic improvements: better UI, more sophisticated definition of data types
- Sophisticated description and analysis of how and where 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
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 their real figures? Research from the American Health, a world-wide leader in medical news, stated in an article about the harmful effects of body image on women's health and self-esteem. One study reported that women's perception of themselves and others is significantly impacted by these images. A growing number of women and girls who seek to look like celebrities are using digital enhancement programs to alter their bodies. However, are these images truly accurate and as they are perceived by society? This leads to the question of whether these images are truly a representation of reality or if they are distorted.

Issue

Supermodel Tyra Banks commented on E! 170 Best Kept Hollywood Secrets that modeling for Victoria's Secret is very different from reality. In order to look perfect, she had to be 5 feet 9 inches tall and completely body-fit. She even had to wear contact lenses, and her hair and skin needed to be flawless. She added, "You don't know how hard it is to maintain this. If you don't, you won't have a job." This statement highlights the importance of digital enhancement and its impact on society.

Experiments Concerning Women and Advertising

Digital Enhancement Programs

There are many programs that can enhance photos. A few programs include Adobe Photoshop, Corel Paint Shop, and Adobe Lightroom. These programs can be used for photo editing within a few clicks of MakeMyPhoto®. One can see that there are significant differences between the photos, including skin tone and texture. More accurate results can be achieved by using professional photography services. The results obtained from these programs allow individuals to enhance their appearance and present themselves in a more favorable light.

Experiments conducted by researchers have shown that digital enhancement programs can significantly affect how people perceive women. A study conducted at Harvard University found that women who had their images edited to appear more attractive were perceived as more intelligent, confident, and successful.

Conclusion

It is difficult to absolutely assert whether digital enhancement of the female figure is a harmful fallacy or a fair marketing tool. Further research is needed to determine whether society is a whole benefited from this technology. Expanding upon these discussions in ethical frameworks, the supplementary paper concludes that further research should be conducted to determine whether society is a whole benefited from this technology. Digital enhancement of the female figure is a complex issue that requires a comprehensive understanding of the potential benefits and drawbacks. Further research is needed to determine the ethical implications and consequences of digital enhancement.
Diaspora, "The privacy aware, personally controlled do-it-all open source social network."

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
- Invites only pod hosted by the team
- Continuing focus on security
- More extensibility and third-party client APIs
- Better documentation
- Easier upgrade path
- Cleaner code

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

Location User Interface
- Design Goals
  - Ability to specify location
  - Warning before sending conflicting locations to individuals in multiple contexts
  - Location based customization without leaking information to third parties
- Future Considerations
  - Adding location context to the user interface
  - Integrating with other location APIs
Survey of Online Privacy Browser Extensions

Privacy Policy Law and Technology

Brian Johnson, Steven Johnson, Jorge Mejia

Objectives

- Create a complete picture of the marketplace of internet privacy browser extensions.
- Develop a detailed framework for the available privacy tools.
- Analyze the key features of privacy extensions on the market.
- Complete a broad survey and categorization of privacy related browser extensions.
- Focus on existing browsers like Firefox, Chrome, and Safari.

Privacy Framework

- Detection/Blocking of third-party trackers.
- Detection and blocking of social networks.
- Detection and blocking of malware and adware.
- Recovery from privacy breaches.
- Monitoring of privacy policies.

Final Thoughts

- Many of the most popular browser extensions have not yet been categorized by privacy tools.
- Most of the extensions that have paid versions.
- Especially extensions that have paid versions.

Carnegie Mellon University
Heinz College
Protection Practices of Facebook Users: Awareness, Attitudes, and Privacy

Background and Motivation
- Facebook's interfaces for controlling privacy settings for features have gone through many changes and have faced criticism since the inception of Facebook's social media platform.

Methodology
- Survey: To gain a first-hand understanding of these privacy settings and methods people use, their intentions for using these mechanisms and what they are hoping to protect against, in order to get insights into how privacy mechanisms could be improved.
- Research Discoveries: The survey revealed commonalities and differences between users of Facebook in their individual privacy strategies. We analyzed the results of the survey and use them to discuss potential areas of improvement for privacy interfaces that will allow users the best opportunities to protect their online privacy.

Preliminary Findings & Recommendations

Main Results: We found that Facebook users mainly used the privacy settings that control who can see one's posts, profiles and which photos they are tagged in. These privacy settings were mainly used to keep their activity on social media private to prevent strangers from contacting them, to protect against identity theft and stalkers, and to protect their personal information. We also found that many users were satisfied with the current privacy settings, yet still felt as if Facebook could make significant changes to improve privacy. Users expressed other concerns/insight about their privacy on Facebook. This data is currently being analyzed.

Recommendations: Increase controls for privacy over timeline activity, increase and improved disclosures about how data is being used/shared with third parties, clear easy to understand policies, limit how much and what data is shared with third parties like advertising companies, consider the option for users not to use their real name.
Privacy Software Development: Tracker Analyzer
08-533/08-733/19-608/95-818 Privacy Policy, Law, and Technology
Chunye Du, Sally Lee, Majeed Alibrahim, Rahul Yadav

Browser trackers are everywhere. But what do we actually know about them? With ideas behind Ghostery, Lightbeam and Disconnect, we started our project to make a browser extension that would more intuitively show and analyze trackers so that users can clearly control the flow of information to these trackers. Our plan was to take each key feature of each existing extensions and incorporate them into our own extension for Chrome.

**Method:**
1) researched all source codes of all extensions.
2) attempted to merge Disconnect’s map with Ghostery’s detailed tracker information as a sidebar.
3) This turned out to be a problem because there is no centralized database of all the trackers; each has its own.
4) Tried again with just Disconnect.
5) Modify the code and change around javascript to display tracker information we obtained from Disconnect’s database in the source code.
6) After figuring out the data structures of each tracker, javascript code was written to display the details as a sidebar.
7) Tweaked the code and CSS to adjust the design and the layout.

**Results:**
I. Analyzing trackers found to be difficult due to lack of standardized database of trackers.
II. Finding the relationship between the sites with first-party/third-party tracker was also difficult due to lack of information on each tracker.

In order to protect the Internet users’ privacy, there is a dire need of a centralized database that keeps track of trackers.

**References**
Variations in Online Tracking in Relation to Geographic Location

Nathaniel Fruchter, Hsin Han, Scott Stevenson

(nbf, hsinn, sbstev)@andrew.cmu.edu • Privacy Policy, Law, and Technology

Background

Different countries have different privacy regulatory models. These models impact how countries handle privacy both legally and culturally, specifically in the realms of online tracking and advertising policy.

With these differences in mind, we investigated if regulatory models had any effect on the amount of tracking present on websites that were accessed from or based in locations with these varying models.

Methodology

We used OpenWPM [2], hosted on Amazon EC2, to crawl the 250 most popular websites as listed by Alexa (see Figure 1). We recorded attributes including third-party cookies and HTTP requests, both of which were used as a metric of tracking activity. The Adblock Plus EasyList [3] was used as an additional metric of tracking activity. Comparisons were then made between countries and regulatory models. A similar process was used with a list of the top 500 sites globally to determine the presence of tracker churn.

Results

• Third-party cookies were more prevalent in the US compared to JP, but there were no significant differences by model.
• Third-party domain requests were also higher in the US with no significant difference between models. This agrees with our Adblock analysis, which showed a 2.4% higher proportion of tracking related ‘hits’ in the US, compared to other countries.
• Location-based tracker churn is insignificant across our countries.
• Using Adblock rules, a significant difference was found in the number of tracking hits between regulatory regimes. Pairwise comparisons are shown in Table 2.

Conclusions

• Location-dependent tracker churn does not seem to be significant across a set of top worldwide sites.
• Most sites have a proportionally higher number of trackers than ads.
• Tracking activity is much higher in the top 250 sites from the United States.
• All countries had notable outliers, some with over 1000 cookies. Most were news sites.
• No significant differences found between regulatory models using third-party metrics.
• Top sites in comprehensive model countries have fewer trackers according to the Adblock metric.
A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior

Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, Blase Ur

Motivation

- Websites provide requirements feedback and multi-step password creation to help users make passwords under strict requirements
- Do feedback and guidance help users make passwords? Are the passwords still as secure? What kind of feedback works best?

Methodology

- Online MTurk study with 6,435 participants
- Password made with different feedback conditions
- Recall password after 5 minutes and in 3 days
- Metrics include password cracking, user sentiment, and attempts to create/recall

Results

Feedback helps users create secure passwords with fewer errors and improved sentiment

Guiding and inserting random characters both reduce final password strength

How requirements are presented to users is important.

Base

- Create a password
- Enter your password

Base w/ Feedback

- Create a password
- Enter your password

Pattern

- Create a password
- Enter your password

Pattern w/ Feedback

- Create a password
- Enter your password

Guided Password Creation

- Create a password
- Enter your password

Guiding and inserting random characters both reduce final password strength

This research was supported in part by NSF grants DGE-0903659 and CNS-1116776, and by a gift from Microsoft Research.
Measuring Password Guessability for an Entire University
Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer,
Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur

Studying real passwords

- Password research is plentiful, but usually based on leaked data (unreliable) or experimental data (artificial)
- We studied 25,000 high-value CMU passwords
- Strong safeguards to protect users
- Required: Upper, lower, digit, symbol, dictionary check, length 8

Analysis approach

- Access plaintext passwords only indirectly
- Compare to leaked sets, online survey sets
- Measure guessability using modified Weir cracking algorithm [1,2]
- Survival analysis to correlate demographic, behavior, sentiment factors with guessability

Results – Correlating password strength

Computer science passwords: 1.5x stronger than business school

- Users who said creating a password was annoying: 1.5x weaker

Results – Comparing password sets

Online surveys are more consistently similar to real CMU passwords than leaked password sets are, both in guessability and composition

Online comp8 studies: MTsim, MTcomp8,
Leaked plaintext sets: Rockyou, CSDN, Yahoo!
Leaked cracked sets: Gawker, Stratfor
Paper survey: SVcomp8
Other online studies: MTbasic8, MTdictionary8

Poster creation

• Have poster draft ready to discuss in class on Tuesday

• If you want Abby to print it on SCS poster printer, email it to her by 9 pm Tuesday
  – Alternatively, you can print it yourself at Kinkos or other CMU printer
  – Or you can print on 8.5x11 paper