The Saucer

The Newsletter of the
CyLab Usable Privacy and Security (CUPS) Laboratory

Issue 2, Summer 2011

CUPS Doctoral Training Program Grows

We are getting ready to welcome the third class of the Carnegie Mellon Usable Privacy and Security Doctoral Training Program in August. Students in PhD programs from throughout Carnegie Mellon University have the opportunity to participate in the CUPS doctoral training program and earn a CyLab Usable Privacy and Security Meritorious Achievement Certificate through the CMU Information Networking Institute (INI). This past May we awarded a CUPS Meritorious Achievement Certificate to our first graduate, Aleecia McDonald.

Thanks to an NSF Integrative Graduate Education and Research Traineeship (IGERT) grant, students who are US citizens can also apply for an IGERT traineeship, which provides two years of tuition and stipend support for students in the doctoral training program. Each year the IGERT grant provides support for 5 or 6 students.

The CUPS doctoral training program offers students a cross-disciplinary training experience that prepares them to produce the key research advances necessary to reconcile ostensible tensions between security, privacy, and usability, moving away from an "either-or" view of these goals to a deeper understanding of underlying tradeoffs and eventually towards solutions where security, privacy, and usability are configured to reinforce each other. The goal of this program is to serve as a catalyst to shape the field of usable privacy and security by developing and training a new generation of researchers in methodologies, principles, and approaches that can be applied across systems and applications.
Continued on next page

Contents

CUPS research sponsors

- Alcatel-Lucent
- Army Research Office (ARO)
- Fundacao para a Ciencia e Tecnologia (FCT)
- Google
- IBM
- Microsoft
- National Science Foundation (NSF)
- The Privacy Projects

CUPS Lab members gather in the Collaborative Innovation Center Atrium.

CyLab
Usable
Privacy *and*
Security
Laboratory

http://cups.cs.cmu.edu

Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Director
Lorrie Faith Cranor
lorrie@cmu.edu

Core Faculty
Alessandro Acquisti
Lujo Bauer
Nicolas Christin
Julie Downs
Jason Hong
Norman Sadeh
Marios Savvides

Supporting Faculty
Travis Breaux
Wandi Bruine de Bruin
David Brumley
Kathleen Carley
Laura Dabbish
Anupam Datta
Baruch Fischhoff
Greg Ganger
Virgil Gligor
Jim Herbsleb
Robert Kraut
Ramayya Krishnan
George Lowenstein
Benoit Morel
Brad Myers
Adrian Perrig
Michael Shamos
Rahul Telang

CUPS Doctoral Training Program Grows

Continued from page 1

This program leverages CMU's strong research programs in security, privacy, human computer interaction (HCI), behavioral economics, computer systems, artificial intelligence, and decision making, as well as a long tradition and strong commitment to interdisciplinary research.

Students in the CUPS doctoral training program are required to take our graduate-level Usable Privacy and Security course, plus three approved full-semester courses from the CUPS course list. The CUPS course list includes courses in security, privacy, human computer interaction, social and decision sciences, and other areas. Students are also expected to participate in the weekly CUPS research seminar for at least two years and present their work at this seminar at least once per year. We also expect CUPS students to be engaged in usable privacy and security research.

CUPS faculty from a variety of disciplines participate in the CUPS research seminar and mentor students in the program. Students in the program are currently pursuing degrees in computer science, electrical and computer engineering, engineering and public policy, human computer interaction, and public policy and management. Each student is mentored by at least two CUPS faculty members from complementary fields.

Prospective students should apply directly to a CMU PhD program of their choice, and also send a letter of interest to the CUPS program administrator indicating which CMU doctoral program they have applied to and describing their interest in CUPS-related research. There is additional information on the CUPS website at http://cups.cs.cmu.edu/igert/ — including information for current CMU students interested in participating in the program.

Students in the second class of IGERT trainees.

From the Director

We've had another busy year in the CUPS Lab. As you will read in this issue, we've published a large number of papers and our faculty have been invited to speak to audiences around the globe. I have so many students and post-docs that we've had to resort to sending some of them to overflow space as there just isn't enough room in the row of cubicles outside my office door. And we've been busy learning how to use our brand new eye tracker.

We've continued to enjoy strong industry support for our research. In addition, CUPS PhD students have benefited from industry internships. Patrick Kelley spent the spring at the Intel Lablet in Seattle and Saranga Komanduri is currently interning at Google in Mountain View.

This year has been an exciting year to be doing privacy research. Privacy has been on the Congressional agenda for most of the year. The Federal Trade Commission and Department of Commerce issued draft reports on privacy. And the Federal Communication Commission is examining privacy issues associated with location-based services. Law makers and regulators have been discussing the need for a "Do Not Track" mechanism that would allow consumers to easily opt-out of online tracking by behavioral advertisers. In response, popular web browsers have implemented Do Not Track headers, and efforts are underway to standardize these mechanisms and determine what do not track actually means. Meanwhile, the online advertising industry developed a behavioral advertising icon and is pushing adoption of this icon along with opt-out cookie mechanisms.

CUPS research continues to play a role in informing the privacy policy debate. The privacy nutrition label approach we developed is mentioned frequently as regulators encourage the adoption of more consumer-friendly privacy notices. Our work on location privacy is also cited frequently on Capital Hill. Our work on understanding consumer beliefs and attitudes about behavioral advertising is relevant to the do-not-track debate. And we expect our ongoing work evaluating the usability and effectiveness of various behavioral advertising choice mechanisms to shed light on the usefulness of these tools in practice. Recent events have made our work on social network regrets, part of our larger privacy nudges project, extremely timely.

A number of CUPS projects leverage the Platform for Privacy Preferences (P3P) standard for computer-readable privacy policies. As we've worked with P3P, we've observed large numbers of websites using P3P incorrectly. This inspired us to conduct a survey of errors in P3P compact privacy policies last summer. We found thousands of sites with P3P errors, and found evidence that sites were misrepresenting their privacy practices with P3P to render the Microsoft Internet Explorer cookie-blocking mechanism ineffective. While this seems to me to be a deceptive practice, to date regulators have not used their authority to force companies to make accurate P3P statements. Several months ago a class action law suit was filed against Amazon.com for several alleged privacy violations, including having a deceptive P3P compact policy. If self-regulatory privacy standards like P3P and Do Not Track headers are to be effective, they need to have enforcement behind them. It remains to be seen whether that will happen.

Students

Idris Adjerid
Hazim Saleh Almuhimedi
Rebecca Balebako
Cristian Bravo-Lillo
Justin Cranshaw
Pedro Giovanni Leon
David Gordon
Hanan Hibshi
Patrick Kelley
Peter Klemperer
Saranga Komanduri
Michelle Mazurek
Emmanuel Owusu
Sasha Romanosky
Rich Shay
Manya Sleeper
Blase Ur
Kami Vaniea
Timothy Vidas
Jason Wiese

Post-Docs & Staff

Keri Burd
Mandy Holbrook
Janne Lindqvist
Jonathan Mugan
Greg Norcie
Eyal Peer
Fred Stutzman
Yang Wang

Visiting Researchers

Melanie Volkamer
Technische Unitersität Darmstadt

Patrick Kelley presents at the weekly CUPS seminar.

Lorrie Cranor played for blue in the annual International Association of Privacy Professionals Global Football Friendly, held this year at Hebrew University in Jerusalem. Future of Privacy Forum Director Jules Polonetsky and former FTC Commissioner Pamela Jones Harbour played for black.

Nicolas Christin speaking about passwords on Channel 4 News.

The *Tribute-Review* ran this photo of Jonathan Mugan demonstrating Locaccino at the CMU Privacy Day poster session.

Year in Review

July 2010

- Lorrie Cranor gave a keynote talk at the IEEE POLICY 2010 conference in Washington, DC
- The CUPS Lab received a gift from Microsoft Research to study password complexity rules and their contribution to password entropy

August 2010

- Lorrie Cranor gave a keynote talk at the Workshop on Integrating Usability and Accessibility in Information Assurance Education at Bowie State University

September 2010

- A research paper by Pedro Leon, Lorrie Cranor, Aleecia McDonald, and Marty McGuire that documented thousands of errors in website P3P compact policies was discussed in a September 17 *New York Times* article
- Three CUPS papers were featured in the *Privacy Papers for Policy Makers Journal*

October 2010

- Lorrie Cranor was interviewed in an *NPR Morning Edition* story on Facebook privacy on October 19
- Alessandro Acquisti was featured on *NPR All Things Considered* on October 26, speaking about his research on privacy through the lens of behavioral economics
- Benoit Morel was the distinguished speaker for the Cyber Security Malaysia Awards, Conference and Exhibition (CSM-ACE) 2010 held on October 25-29 in Kuala Lumpur
- Idris Adjerid gave a presentation at the Workshop on Health IT and Economics (WHITE) in Washington, D.C.
- Idris Adjerid participated in a poster session at the Annual Symposium of The American Medical Informatics Association (AMIA) in Washington D.C.
- Pedro Leon presented a paper at the ACM Workshop on Privacy in the Electronic Society in Chicago, IL: "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens"
- Aleecia McDonald presented a paper at the ACM Workshop on Privacy in the Electronic Society in Chicago, IL: "Americans' Attitudes About Internet Behavioral Advertising Practices"
- Lorrie Cranor and Alessandro Acquisti spoke at the International Data Protection and Privacy Commissioners Conference in Jerusalem

December 2010

- Lorrie Cranor was interviewed by Jon Delano, Pittsburgh's KDKA News Money Editor as part of a story on the FTC proposal for an Internet Do Not Track List
- Lorrie Cranor received a Google Research Award to study user perceptions of advertisement landing page quality
- Greg Ganger was named a fellow of the Institute for Electronic and Electrical Engineers (IEEE) for contributions to metadata integrity in file systems
- The National Academy of Sciences released a workshop report, "Toward Better Usability, Security, and Privacy of Information Technology." Lorrie Cranor was a member of the workshop steering committee and CUPS faculty Alessandro Acquisti, Lujo Bauer, Jason Hong, and Norman Sadeh also participated in the workshop

January 2011

- Nicolas Christin was featured in a Channel 4 news story about password security
- Lorrie Cranor was the featured guest on WHYY Radio Times on January 6, discussing online privacy, the consumer and do not track lists
- CMU hosted an International Data Privacy Day celebration, organized by Alessandro Acquisti and featuring a poster session and panel discussion
- Yang Wang and Lorrie Cranor received a grant from the Privacy Projects for a study on the usability and effectiveness of opt-out tools for behavioral advertising

February 2011

- Greg Ganger received the Stephen J. Jatras Professorship in Electrical and Computer Engineering at a reception in his honor
- Lorrie Cranor gave the 4th Annual Privacy Lecture at Berkeley Law: "Standardizing Privacy Notices: Privacy Taxonomy, Privacy Nutrition Labels, and Computer-Readable Policies"

March 2011

- Alessandro Acquisti was the opening speaker at the Privacy Symposium: Vie Privie & Riseaux Sociaux en Ligne: Nouveaux Comportements et Nouvelles Regulations, "From the Illusion of Control to Discounting the Past: Privacy and Behavior," Universite Paris-Sud, Faculte Jean Monnet

April 2011

- Keri Burd joined the CUPS Lab as the IGERT program administrator
- Alessandro Acquisti was interviewed on *Marketplace Tech Report* on April 28: "How secure is the data you put online? No one really knows"
- Lorrie Cranor co-chaired the W3C Workshop on Web Tracking and User Privacy
- Manya Sleeper and Blase Ur received honorable mentions in the NSF Graduate Research Fellowship competition
- Jason Wiese won a Yahoo! Key Scientific Challenges Award
- Jason Wiese was a finalist for the 2011 Facebook Fellowship

May 2011

- CUPS lab members presented 6 papers, 2 notes, and several workshop papers at CHI 2011 in Vancouver, Canada
- The paper "Of Passwords and People: Measuring the Effect of Password-Composition Policies" by Saranga Komanduri, Rich Shay, Patrick Kelley, Michelle Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Cranor, and Serge Egelaman received an honorable mention award at CHI 2011
- Fred Stutzman co-organized a CHI 2011 workshop on Privacy for a Networked World: Bridging Theory and Design
- Aleecia McDonald was awarded the first CUPS Meritorious Achievement Certificate at commencement
- Michelle Mazurek received an IGERT poster finalist award for her poster presented at the IGERT poster competition: "Measuring the Effect of Pa$$w0rd-Composition Policies on Security and Usability"
- Jason Hong spoke at the Congressional Internet Caucus State of the Mobile Net Conference in Washington, DC

June 2011

- Alessandro Acquisti gave a keynote talk at the Computers, Freedom, and Privacy Conference in Washington, DC: "Privacy in the Age of Augmented Reality"
- Idris Adjerid gave a presentation at the Workshop on the Economics of Information Security (WEIS) in Washington, D.C.
- Idris Adjerid gave a presentation at INFORMS Healthcare in Montreal
- Yang Wang was interviewed on the *IEEE Spectrum* blog about his international study of privacy on social networks
- Yang Wang presented the paper, "Privacy on Social Networks: American, Chinese, and Indian Perspectives" at the Trust 2011 4th International Conference on Trust and Trustworthy Computing in Pittsburgh
- Lorrie Cranor spoke at a CMU Cyber Security Briefing in Washington, DC
- Lorrie Cranor spoke at the Federal Communication Commission Forum on Helping Consumers Harness the Potential of Location-Based Services in Washington, D.C.

July 2011

- An *ISR* journal paper by Janice Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti was discussed on *Marketplace Morning Report*
- SOUPS 2011 will be held July 20-22 at Carnegie Mellon University

CUPS faculty Alessandro Acquisti and Travis Breaux on the CMU Privacy Day panel.

Greg Ganger receiving the Stephen J. Jatras Professorship (and chair) in Electrical and Computer Engineering.

Lorrie Cranor speaking at the FCC Location-Based Services Forum.

Baby Boom!

It has been a busy year for CUPS babies. Six new arrivals have joined the families of CUPS community members this year.

In September, CUPS alumnus Steve Sheng and his wife Phoebe announced the arrival of their daughter Teresa. The family now lives in the LA area where Steve works for ICANN.

In October, CUPS Alumnus Ponnurangam Kumaraguru and his wife Pranjali announced the arrival of their daughter Aarya. Aarya joins her big brother Aarav. The family now lives in Delhi where PK is on the faculty of IIIT Delhi.

Also in October, CUPS faculty member Julie Downs welcomed her son Theo. Theo loves to eat and enjoys coming to research meetings with his mom.

CUPS PhD student Eiji Hayashi and his wife Erikio welcomed their second daughter, Sara, to their family in December. Sara is both an American name and a traditional Japanese name.

CUPS PhD student Rebecca Balebako and her husband Eric welcomed their daughter Meghan Mayen Balebako in May. Mayen is a Losso name that means "independent."

At the end of June, CUPS PhD student Idris Adjerid and his wife Hayet announced the birth of their son Yunes. The proud parents predict he will be a future NBA all-star and Nobel Laureate.

In Other News

CUPS faculty member Alessandro Acquisti comes from a family of musicians. Before going into academia he wrote soundtracks for theater, short movies, and Italian TV. He also wrote lyrics for Italian pop singers and musicals. Alessandro recently collaborated with his father, composer Giancarlo Acquisti, on the lyrics for a new musical titled *Raffaello e la Leggenda della Fornarina,* based on the real life of the painter Raffaello and his

In August 2010 CUPS alumna Janice Tsai started working at Microsoft as the North American privacy manager supporting Microsoft's marketing efforts.

Recent Publications

Privacy Policy

Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens

Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M. McDonald, and Robert McGuire

WPES 2010

Platform for Privacy Preferences (P3P) compact policies (CPs) are a collection of three-character and four-character tokens that summarize a website's privacy policy pertaining to cookies. User agents, including Microsoft's Internet Explorer (IE) web browser, use CPs to evaluate websites' data collection practices and allow, reject, or modify cookies based on sites' privacy practices. CPs can provide a technical means to enforce users' privacy preferences if CPs accurately reflect websites' practices. Through automated analysis we can identify CPs that are erroneous due to syntax errors or semantic conflicts. We collected CPs from 33,139 websites and detected errors in 11,176 of them, including 134 TRUSTe-certified websites and 21 of the top 100 most-visited sites. Our work identifies potentially misleading practices by web administrators, as well as common accidental mistakes. We found thousands of sites using identical invalid CPs that had been recommended as workarounds for IE cookie blocking. Other sites had CPs with typos in their tokens, or other errors. 98% of invalid CPs resulted in cookies remaining unblocked by IE under its default cookie settings. It appears that large numbers of websites that use CPs are misrepresenting their privacy practices, thus misleading users and rendering privacy protection tools ineffective. Unless regulators use their authority to take action against companies that provide erroneous machine-readable policies, users will be unable to rely on these policies.

A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies

Aleecia McDonald and Lorrie Cranor

CyLab Technical Report cmu-cylab-11-001

Website developers can use Adobe's Flash Player product to store information locally on users' disks with Local Shared Objects (LSOs). LSOs can be used to store state information and user identifiers, and thus can be used for similar purposes as HTTP cookies. In a paper by Soltani et al, researchers documented at least four instances of "respawning," where users deleted their HTTP cookies only to have the HTTP cookies recreated based on LSO data. In addition, the Soltani team found half of the 100 most popular websites used Flash technologies to store information about users. Both respawning and using LSOs to store data about users can reduce online privacy. One year later, we visited popular websites plus 500 randomly-selected websites to determine if respawning still occurs. We found no instances at all of respawning in a randomly-selected group of 500 websites. We found two instances of respawning in the most popular 100 websites. While our methods are different from the Soltani team and we cannot compare directly, our results suggest respawning is not increasing, and may be waning.

AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements

Saranga Komanduri, Richard Shay, Greg Norcie, and Lorrie Faith Cranor

CyLab Technical Report cmu-cylab-11-005

Online behavioral advertisers track users across websites, often without users' knowledge. Over the last twelve years, the online behavioral advertising industry has responded to the resulting privacy concerns and pressure from the FTC by creating private self-regulatory bodies. These include the Network Advertising Initiative (NAI) and an umbrella organization known as the Digital Advertising Alliance (DAA). In this paper, we enumerate the notice and choice requirements the DAA and NAI place on their members and check for compliance with those requirements by examining members' privacy policies and reviewing ads on the top 100 websites. We also test DAA and NAI opt-out mechanisms and categorize how their members define opting out. Our results show that most members are in compliance with some of the notice and choice requirements, but there are numerous instances of non-compliance. Most examples of non-compliance are related to the "enhanced notice" requirement, which requires advertisers to mark behavioral ads with a link to further information and a means of opting out.

Impact of Health Disclosure Laws on Health Information Exchanges

Idris Adjerid, Alessandro Acquisti, Rema Padman, Rahul Telang, and Julia Adler-Milstein

WEIS 2011

Health information exchanges (HIEs) are expected to facilitate collaboration between healthcare entities and improve efficiency and quality of care through enhanced information sharing capabilities. Privacy concerns have been consistently cited as one of the primary challenges to HIE development and adoption. Currently, it is unclear how privacy laws—in particular, legislation restricting the disclosure of health records—have impacted the adoption of HIEs intended to facilitate sharing of health information. This study explores the landscape of health privacy legislation at the State level and examines the impact of variations in such privacy and confidentiality laws across the United States on the progress of HIEs. Our current results suggest a strong association between states with laws that limit the disclosure of health information and positive HIE outcomes and that the impact of health disclosure laws is tied closely with incentives for HIE adoption. This points to some non-obvious benefits of such laws and suggests that it is some balanced appropriation of both carrot and substantive stick that works best to promote HIE growth and success.

Privacy Decision Making

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study

Janice Y. Tsai, Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti
Information Systems Research, June 2011

Although online retailers detail their privacy practices in online privacy policies, this information often remains invisible to consumers, who seldom make the effort to read and understand those policies. This paper reports on research undertaken to determine whether a more prominent display of privacy information will cause consumers to incorporate privacy considerations into their online purchasing decisions. We designed an experiment in which a shopping search engine interface clearly and compactly displays privacy policy information. When such information is made available, consumers tend to purchase from online retailers who better protect their privacy. In fact, our study indicates that when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites. This result suggests that businesses may be able to leverage privacy protection as a selling point.

I Regretted the Minute I Pressed Share: A Qualitative Study of Regrets on Facebook

Yang Wang, Saranga Komanduri, Pedro Giovanni Leon, Greg Norcie, Alessandro Acquisti, and Lorrie Faith Cranor
SOUPS 2011

We investigate regrets associated with users' posts on a popular social networking site. Our findings are based on a series of interviews, user diaries, and online surveys involving 569 American Facebook users. Their regrets revolved around sensitive topics, content with strong sentiment, lies, and secrets. Our research reveals several possible causes of why users make posts that they later regret: (1) they want to be perceived in favorable ways, (2) they do not think about their reason for posting or the consequences of their posts, (3) they misjudge the culture and norms within their social circles, (4) they are in a "hot" state of high emotion when posting, or under the influence of drugs or alcohol, (5) their postings are seen by an unintended audience, (6) they do not foresee how their posts could be perceived by people within their intended audience, and (7) they misunderstand or misuse the Facebook platform. Some reported incidents had serious repercussions, such as breaking up relationships or job losses. We discuss methodological considerations in studying negative experiences associated with social networking posts, as well as ways of helping users of social networking sites avoid such regrets.

Who Is Concerned about What? A Study of American, Chinese and Indian Users Privacy Concerns on Social Network Sites

Yang Wang, Greg Norcie, and Lorrie Faith Cranor
TRUST 2011

We present a study that investigates American, Chinese, and Indian social networking site (SNS) users' privacy attitudes and practices. We conducted an online survey of users of three popular SNSs in these countries. Based on 924 valid responses from the three countries, we found that generally American respondents were the most privacy concerned, followed by the Chinese and Indians. However, the US sample exhibited the lowest level of desire to restrict the visibility of their SNS information to certain people (e.g., co-workers). The Chinese respondents showed significantly higher concerns about identity issues on SNS such as fake names and impersonation.

Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising

Aleecia M. McDonald and Lorrie Faith Cranor
38th Research Conference on Communication, Information and Internet Policy (TPRC 2010)

This paper presents empirical data on American adult Internet users' knowledge about and perceptions of Internet advertising techniques. We present the results of in-depth interviews and an online survey focusing on participants' views of online advertising and their ability to make decisions about privacy tradeoffs. We find users hold misconceptions about the purpose of cookies and the effects of clearing them, which limits cookie management as a self-help mechanism enabling user choice. Only 11% of respondents understood the text description of NAI opt-out cookies, which are a self-help mechanism that enables user choice. 86% believe ads are tailored to websites they have visited in the past, but only 39% believe there are currently ads based on email content, and only 9% think it is ok to see ads based on email content as long as their email service is free. About 20% of participants want the benefits of targeted advertising, but 64% find the idea invasive, and we see signs of a possible chilling effect with 40% self-reporting they would change their online behavior if advertisers were collecting data. We find a gap between people's willingness to pay to protect their privacy and their willingness to accept discounts in exchange for private information. 69% believe privacy is a right and 61% think it is "extortion" to pay to keep their data private. Only 11% say they would pay to avoid ads. With the exception of contextual advertisements, we find most participants would prefer random ads to tailored ads, but approximately 20% of participants would rather tailored ads. We find participants are comfortable with the idea that advertising supports free online content, but they do not believe their data are part of that exchange. We conclude with observations for public policy, technologists, and education.

Location-Based Services and Location Privacy

Undistracted Driving: A Mobile Phone that Doesn't Distract

Janne Lindqvist and Jason Hong
HotMobile 2011

Distracted driving is a major problem that leads to unnecessary accidents and human casualties. The ubiquity of mobile phones is one cause of distracted driving. In United States alone, operating mobile phones while driving has been cited as a

factor in crashes that have led to 995 deaths and 24,000 injuries in 2009. To mitigate the problem of distracted driving caused by mobile phones, we propose using context-awareness to implement burden-shifting, time-shifting, and activity-based sharing. Although the first two concepts have been introduced before in the research literature and the latter two are novel, none of these concepts have yet been explored in the context of mobile phones and driving. We present our initial interaction designs on the Android platform.

Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs
Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor
Personal and Ubiquitous Computing, December 2010
We present a 3-week user study in which we tracked the locations of 27 subjects and asked them to rate when, where, and with whom they would have been comfortable sharing their locations. The results of analysis conducted on over 7,500 hours of data suggest that the user population represented by our subjects has rich location-privacy preferences, with a number of critical dimensions, including time of day, day of week, and location. We describe a methodology for quantifying the effects, in terms of accuracy and amount of information shared, of privacy-setting types with differing levels of complexity (e.g., setting types that allow users to specify location- and/or time-based rules). Using the detailed preferences we collected, we identify the best possible policy (or collection of rules granting access to one's location) for each subject and privacy-setting type. We measure the accuracy with which the resulting policies are able to capture our subjects' preferences under a variety of assumptions about the sensitivity of the information and user-burden tolerance. One practical implication of our results is that today's location-sharing applications may have failed to gain much traction due to their limited privacy settings, as they appear to be ineffective at capturing preferences revealed by our study.

Empirical Models of Privacy in Location Sharing
Eran Toch, Justin Cranshaw, Paul H. Drielsma, Janice Y. Tsai, Patrick Gage Kelley, Jay Springfield, Lorrie Faith Cranor, Jason Hong and Norman Sadeh
Ubicomp 2010
The rapid adoption of location tracking and mobile social networking technologies raises significant privacy challenges. Our understanding of people's location sharing privacy preferences remains limited, including how these preferences are impacted by the type of location tracking device or the nature of the locations visited. To address this gap, we deployed Locaccino, a mobile location sharing system, in a four week long field study, where we examined the behavior of study participants (n=28) who shared their location with their acquaintances (n = 373). Our results show that users appear more comfortable sharing their presence at locations visited by a large and diverse set of people. Our study also indicates that people who visit a wider number of places tend to also be the subject of a greater number of requests for their locations. Over time these same people tend to also evolve more sophisticated privacy preferences, reflected by an increase in time- and location-based restrictions.

Rethinking Location Sharing: Exploring the Implications of Social-Driven vs. Purpose-Driven Location Sharing
Karen Tang, J. Lin, Jason Hong, and Norman Sadeh
Ubicomp 2010
The popularity of micro-blogging has made general-purpose information sharing a pervasive phenomenon. This trend is now impacting location sharing applications (LSAs) such that users are sharing their location data with a much wider and more diverse audience. In this paper, we describe this as social-driven sharing, distinguishing it from past examples of what we refer to as purpose-driven location sharing. We explore the differences between these two types of sharing by conducting a comparative two-week study with nine participants. We found significant differences in terms of users' decisions about what location information to share, their privacy concerns, and how privacy-preserving their disclosures were. Based on these results, we provide design implications for future LSAs.

Modeling People's Place Naming Preferences in Location Sharing
Jialiu Lin, Guang Xiang, Jason Hong, and Norman Sadeh
Ubicomp 2010
Most location sharing applications display people's locations on a map. However, people use a rich variety of terms to refer to their locations, such as "home," "Starbucks," or "the bus stop near my house." Our long term goal is to create a system that can automatically generate appropriate place names based on real-time context and user preferences. As a first step, we analyze data from a two-week study involving 26 participants in two cities, focusing on how people refer to places in location sharing. We derive a taxonomy of place naming methods, and show that factors such as a person's perceived familiarity with a place and the entropy of that place (i.e. the variety of people who visit it) strongly influence the way people refer to it when interacting with others. We also present a machine learning model for predicting how people name places. Using our data, this model is able to predict the place naming method people choose with an average accuracy higher than 85%.

User-Controllable Learning of Location Privacy Policies with Gaussian Mixture Models
Justin Cranshaw, Jonathan Mugan, and Norman Sadeh
AAAI-11
With smart-phones becoming increasingly commonplace, there has been a subsequent surge in applications that continuously track the location of users. However, serious privacy concerns arise as people start to widely adopt these applications. Users will need to maintain policies to determine under which circumstances to share their location. Specifying these policies however, is a cumbersome task, suggesting that machine learning might be helpful. In this paper, we present a user-controllable method for learning location sharing policies. We

use a classifier based on multivariate Gaussian mixtures that is suitably modified so as to restrict the evolution of the underlying policy to favor incremental and therefore human-understandable changes as new data arrives. We evaluate the model on real location-sharing policies collected from a live location-sharing social network, and we show that our method can learn policies in a user-controllable setting that are just as accurate as policies that do not evolve incrementally. Additionally, we highlight the strength of the generative modeling approach we take, by showing how our model easily extends to the semi-supervised setting.

When Are Users Comfortable Sharing Locations with Advertisers?

Patrick Gage Kelley, Michael Benisch, Lorrie Faith Cranor, and Norman Sadeh

CHI 2011

As smartphones and other mobile computing devices have increased in ubiquity, advertisers have begun to realize a more effective way of targeting users and a promising area for revenue growth: location-based advertising. This trend brings to bear new questions about whether or not users will adopt products involving this potentially invasive form of advertising and what sorts of protections should be given to users. Our real-world user study of 27 participants echoes earlier findings that users have significant privacy concerns regarding sharing their locations with advertisers. However, we examine these concerns in more detail and find that they are complex (e.g., relating to not only the quantity of ads, but the locations they receive them at). With advanced privacy settings users stated they would feel more comfortable and share more information than with a simple opt-in/opt-out mechanism.

I'm the Mayor of My House: Examining Why People Use Foursquare - a Social-Driven Location Sharing Application

Janne Lindqvist, Justin Cranshaw, Jason Wiese, Jason Hong, and John Zimmerman

CHI 2011

There have been many location sharing systems developed over the past two decades, and only recently have they started to be adopted by consumers. In this paper, we present the results of three studies focusing on the foursquare check-in system. We conducted interviews and two surveys to understand, both qualitatively and quantitatively, how and why people use location sharing applications, as well as how they manage their privacy. We also document surprising uses of foursquare, and discuss implications for design of mobile social services.

Passwords

Of Passwords and People: Measuring the Effect of Password-Composition Policies

Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman

CHI 2011 ***Honorable Mention***

Text-based passwords are the most common mechanism for authenticating humans to computer systems. To prevent users from picking passwords that are too easy for an adversary to guess, system administrators adopt password-composition policies (e.g., requiring passwords to contain symbols and numbers). Unfortunately, little is known about the relationship between password-composition policies and the strength of the resulting passwords, or about the behavior of users (e.g., writing down passwords) in response to different policies. We present a large-scale study that investigates password strength, user behavior, and user sentiment across four password-composition policies. We characterize the predictability of passwords by calculating their entropy, and find that a number of commonly held beliefs about password composition and strength are inaccurate. We correlate our results with user behavior and sentiment to produce several recommendations for password-composition policies that result in strong passwords without unduly burdening users.

Security through a Different Kind of Obscurity: Evaluating Distortion in Graphical Authentication Schemes

Eiji Hayashi, Jason Hong, and Nicolas Christin

CHI 2011

While a large body of research on image-based authentication has focused on memorability, comparatively less attention has been paid to the new security challenges these schemes may introduce. Because images can convey more information than text, image-based authentication may be more vulnerable to educated guess attacks than passwords. In this paper, we evaluate the resilience of a recognition based graphical authentication scheme using distorted images against two types of educated guess attacks through two user studies.

The first study, consisting of 30 participants, investigates whether distortion prevents educated guess attacks primarily based on information about individual users. The second study, using Amazon Mechanical Turk, investigates whether distortion mitigates the risk of educated guess attacks based on collective information about users. Our results show that authentication images without distortion are vulnerable to educated guess attacks, especially when information about the target is known, and that distortion makes authentication images more resilient against educated guess attacks.

Access Control

More than Skin Deep: Measuring Effects of the Underlying Model on Access-Control System Usability
Robert W. Reeder, Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter, and Kami Vaniea
CHI 2011
In access-control systems, policy rules conflict when they prescribe different decisions (ALLOW or DENY) for the same access. We present the results of a user study that demonstrates the significant impact of conflict-resolution method on policy-authoring usability. In our study of 54 participants, varying the conflict-resolution method yielded statistically significant differences in accuracy in five of the six tasks we tested, including differences in accuracy rates of up to 78%. Our results suggest that a conflict-resolution method favoring rules of smaller scope over rules of larger scope is more usable than the Microsoft Windows operating system's method of favoring deny rules over allow rules. Perhaps more importantly, our results demonstrate that even seemingly small changes to a system's semantics can fundamentally affect the system's usability in ways that are beyond the power of user interfaces to correct.

Exploring Reactive Access Control
Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor
CHI 2011
As users store and share more digital content at home, access control becomes increasingly important. One promising approach for helping non-expert users create accurate access policies is reactive policy creation, in which users can update their policy dynamically in response to access requests that would not otherwise succeed. An earlier study suggested reactive policy creation might be a good fit for file access control at home. To test this, we conducted an experience-sampling study in which participants used a simulated reactive access-control system for a week. Our results bolster the case for reactive policy creation as one mode by which home users specify access-control policy. We found both quantitative and qualitative evidence of dynamic, situational policies that are hard to implement using traditional models but that reactive policy creation can facilitate. While we found some clear disadvantages to the reactive model, they do not seem insurmountable.

Computer Security Warnings

Bridging the Gap in Computer Security Warnings: A Mental Model Approach
Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri
IEEE Security and Privacy, March/April 2011
Computer security warnings are intended to protect users and their computers. However, research suggests that these warnings might be largely ineffective because they're frequently ignored. The authors describe a mental model interview study designed to gain insight into how advanced and novice computer users perceive and respond to computer warnings. Developers can leverage the approaches of advanced users to design more effective warnings for novice users.

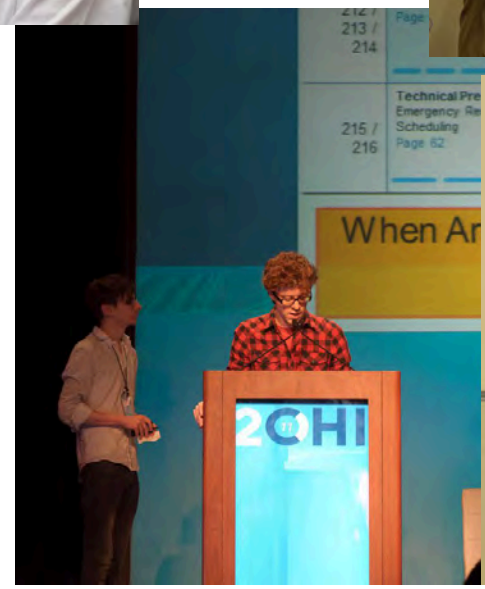
Dissertations & Proposals

Footprints Near the Surf: Individual Privacy Decisions in Online Contexts
Aleecia M. McDonald
PhD Thesis, Engineering & Public Policy Department
December 2010
As more people seek the benefits of going online, more people are exposed to privacy risks from their time online. With a largely unregulated Internet, self-determination about privacy risks must be feasible for people from all walks of life. Yet in many cases decisions are either not obvious or not accessible. As one example, privacy policies are written beyond most adults reading comprehension level, and few people read policies let alone act based on the information policies contain. In my thesis I examine decisions made about threats from website data collection. In the course of multiple studies I use a variety of tools including lab-based studies, online studies, mental models interviews, economic analysis, and analysis of cookies used for tracking. Privacy literature is full of apparent conflicts between people saying they care very much about their privacy, yet not taking the steps required to protect their privacy. By using multiple approaches and crossing multiple disciplines I am able to contribute to a more coherent picture of whether people are able to make choices about protecting their online privacy. (Advisor: Lorrie Cranor)

Thesis Proposal: Designing Privacy Interfaces Design Patterns for Understanding and Control
Patrick Gage Kelley
Computation, Organizations, and Society
December 7, 2010
Users are increasingly expected to manage complex privacy settings in their normal interactions online. From shopping to social networks, users make decisions about sharing their personal information with corporations and contacts, frequently with little assistance. Current solutions largely require consumers to read long textual documents, to go out of their way to manage complex settings buried deep in interfaces, or give them no control at all. The goal of this work is to collect, describe, test, and refine a series of design patterns for privacy interfaces which help consumers better understand data practices, take more active control of their information, and can compel them to behave in a more privacy-protecting manner. The design patterns I will explore include: simplified design, standardization, explanation, automation, nudging, and holistic views. (Advisors: Lorrie Cranor and Norman Sadeh)

Anticipating the final Harry Potter movie, CUPS students and faculty model their snuggies.

Manya Sleeper presents a poster at the CyLab corporate partners conference.



Patrick Kelley gives a 20-second teaser for his paper during CHI madness. Saranga Komanduri, Rich Shay, Eiji Hayashi, and Michelle Mazurek present papers at CHI.