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

The Saucer

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

Issue 3, Summer 2012

Contents

CUPS research sponsors

Army Research Office (ARO)

Fundacao para a Ciencia e Tecnologia (FCT)

Google

Microsoft

National Science Foundation (NSF)

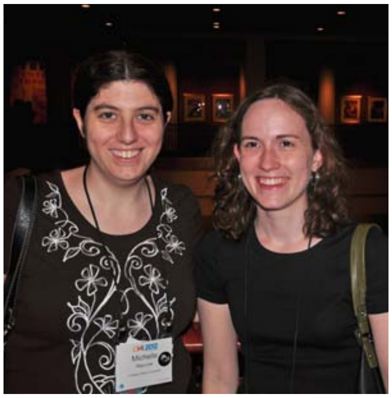
The Privacy Projects

Carnegie Mellon University
CyLab

An Award-Winning Year

CUPS students had a terrific year, winning numerous prestigious awards.

Michelle Mazurek, who just finished her fourth year in the ECE PhD program, was among 12 students nationwide chosen as Facebook Fellows for 2012-13. Mazurek is researching ways to let users share their content accurately and quickly, secure in the knowledge that only the right people will see it. Rather than setting specific permissions for each piece of content, her system will let users easily set comprehensive, human-understandable rules for controlling access to certain types of data. Each Facebook Fellow receives full tuition, a $30,000 stipend to cover study expenses, $5,000 for conference travel, and $2,500 for a personal computer. Michelle is co-advised by Greg Ganger and Lujo Bauer.



Michelle Mazurek and Manya Sleeper, at CHI 2012 in Austin, TX.

Blase Ur, who just finished his first year in the COS PhD program, received several impressive awards this year. Blase received a Yahoo! Key Scientific Challenges Award for his research in privacy and security. He received $5,000 in unrestricted seed funding. Blase received a National Defense Science and Engineering Graduate (NDSEG) Fellowship, which provides three years of graduate tuition and a stipend. Blase also received an honorable mention in the NSF Graduate Research Fellowship program. Blase is working on research in a variety of areas, including privacy and online tracking, passwords, usable access control, and cross-cultural privacy concerns. He finished his first year of graduate school with 9 published papers! Blase is advised by Lorrie Cranor.

Sauvik Das, who just finished his first year in the HCII PhD program, also received an NDSEG Fellowship. He is doing research on casual authentication, mobile accelerometer attacks, and alternative password inputs. He is advised by Jason Hong.

Manya Sleeper, who just finished her second year in the COS PhD program, received an honorable mention in the NSF Graduate Research Fellowship program. Manya is doing research on usable security for digital home storage and privacy nudges. She is advised by Lorrie Cranor.

The paper “Why Johnny Can’t Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising” by Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, Yang Wang received a CHI 2012 best paper award honorable mention. The paper “The Livehoods Project: Utilizing Social Media to Understand the Dynamics of a City” by Justin Cranshaw, Raz Schwartz, Jason Hong, and Norman Sadeh, won the best paper award at the International AAAI Conference on Weblogs and Social Media (ICWSM-12).

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
David Brumley
Kathleen Carley
Laura Dabbish
Anupam Datta
Baruch Fischhoff
Greg Ganger
Virgil Gligor
Jim Herbsleb
Robert Kraut
Ramayya Krishnan
George Lowenstein
Brad Myers
Adrian Perrig
Michael Shamos
Rahul Telang

CUPS Doctoral Training Program Offers Unique PhD in Usable Privacy & Security

We are getting ready to welcome the fourth class of the Carnegie Mellon Usable Privacy and Security Doctoral Training Program in August. Students in PhD programs from throughout CMU have the opportunity to participate in the CUPS doctoral training program and earn a CyLab Usable Privacy and Security Meritorious Achievement Certificate. 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.

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.

CUPS Students in Action

Several CUPS students have been volunteering their time to help with science and technology education in our community. Blase Ur and Manya Sleeper have been visiting the Pittsburgh Science and Technology Academy (SciTech) to teach a weekly computational thinking course to middle school students. SciTech is a public school in Oakland with a curriculum focusing on science, technology, engineering, and math. Michelle Mazurek and her husband Kyle Orland have been volunteering weekly with the Pittsburgh Project, providing homework assistance and leading math and science activities for at risk children. Peter Klemperer was a robot inspector at the 2012 Pittsburgh Regional FIRST competition in March and served as a robot judge at the 2011 First LEGO League challenge last December.

From the Director

It's been another great year at the CUPS Lab. There has been lots of good news, and I have been especially excited to see the impact our research papers and our people are having on the world.

This was another exciting year to be doing privacy research. The White House and the Federal Trade Commission both released important privacy reports (citing our research!) and there have been a number of privacy hearings and workshops on Capital Hill. In October, Alessndro Aquisti testified at a hearing on "Understanding Consumer Attitudes About Privacy" held by the House Subcommittee on Commerce, Manufacturing, and Trade. In May I spoke at an FTC workshop on advertising and privacy disclosures in online and mobile media. CUPS alumnus Aleecia McDonald has spent the year co-chairing the W3C's effort to develop a "Do Not Track" standard, a central component of privacy self-regulatory efforts.

Our research has brought important insights into the effectiveness of privacy self-regulation. We interviewed 48 Internet users and tested nine online behavioral advertising (OBA) opt-out tools to provide data on the knowledge and attitudes of users about OBA and the usability of these tools. We also developed a method for measuring whether these tools are effective at preventing targeted ads. Our research found that existing tools are not very usable, users are unfamiliar with OBA icons developed by the industry, and that users are unable to make decisions about the myriad of tracking companies, most of which they have never heard of. We surveyed 1,500 Internet users about the OBA icons and taglines and found that not only are users unfamiliar with them, but they are afraid to click on them.

In 2010 we published a paper that documented the deceptive use of the Platform for Privacy Preferences (P3P) standard by many websites to avoid having Internet Explorer block their cookies. That paper received renewed attention this winter when Microsoft announced it had just discovered that companies were circumventing its browser cookie controls. In addition, several lawsuits were filed in 2011 and 2012 against companies alleged to be using P3P deceptively to prevent cookie blocking.

Another paper from the CUPS archive, published in 2008, resurfaced this year. Aleecia McDonald's *I/S Journal* paper on "The Cost of Reading Privacy Policies" was discussed this spring in several publications, including *The Atlantic, NPR Morning Edition,* and even *News of the Weird.* (Is this further evidence that people who read privacy policies are weird?)

We've also had lots of exciting developments in our passwords research. Short summary: we've found that long passwords give you better security and usability than complicated passwords, XKCD's password advice is not a panacea, and most password meters currently in use are too lenient on their users. We're currently working with our local CMU computing services team both to collect more real-world password data and to put our research results into practice.

Lorrie

Students

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

Post-Docs & Staff

Tiffany M. Todd
Mandy Holbrook
Eyal Peer
Fred Stutzman
Yang Wang

"Cowgirl" Lorrie Cranor was interviewed in the red chair at CHI 2012 in Austin, TX.

CUPS postdoc Yang Wang and students Blase Ur and Rich Shay at SOUPS 2011 at Carnegie Mellon University.

CUPS faculty member Lujo Bauer finds his balance at the CyLab holiday party at the Pittsburgh Children's Museum.

CUPS student Saranga Komanduri presents a paper at the IEEE Security & Privacy conference.

Year in Review

September 2011

- David Brumley won a Presidential Early Career Award for Scientists and Engineers (PECASE) – the highest honor bestowed by the U.S. government on scientists and engineers beginning their independent careers.
- Postdoc Fred Stutzman (and co-author Woodrow Hartzon) had a paper published in the second annual *Privacy Papers for Policy Makers Journal.*
- Norman Sadeh was a panelist at Qualcomm's Contextual Awareness Symposium.

October 2011

- ACM named Virgil Gligor recipient of its 7th Annual Outstanding Innovation Award for Computer Privacy and Security Expertise.
- "Why Johnny Can't Opt-Out" study was featured in a *Wall Street Journal* article.
- Alessandro Aquisti was a keynote speaker at the Conference on the Economics of Information and Communication Technologies in Paris.
- Alessandro Acquisti testified at a hearing "Understanding Consumer Attitudes About Privacy" held by the House Subcommittee on Commerce, Manufacturing, and Trade.

November 2011

- Lorrie Cranor was interviewed by *Marketplace Tech Report* about opt-out toolstudy.
- Norman Sadeh was featured in a *ComputerWorld* article titled "Supreme Court set to hear landmark GPS tracking case: Ruling will determine whether warrants are needed to use GPS technology to track criminal suspects."
- Alessandro Aquisiti was a keynote speaker at the International Association of Privacy Professionals - Australia and New Zealand - Annual Conference.
- Timothy Vidas won second place in the NYU Poly Kaspersky American Cup competition with his paper "Towards a General Collection Methodology for Android Devices."

December 2011

- Lorrie Cranor was a presenter and Alessandro Aquisti was a keynote speaker at the Silicon Flatirons conference on the Economics of Privacy at the Univ. of Colorado.
- Lorrie Cranor was quoted in a *USA Today* article about Do Not Track.

January 2012

- Norman Sadeh was featured on the Carnegie Mellon University homepage. In the article titled "Defensive Maneuvers," Sadeh discussed the work that he has done with Wombat Security Technologies to create anti-phishing training products.

February 2012

- Lorrie Cranor was quoted in articles in the *Wall Street Journal, Computerworld, ReadWriteWeb,* and dozens of other publications on the topic of circumvention of IE P3P cookie controls.
- Lorrie Cranor was interviewed on *NPR Morning Edition* and *NPR Science Friday* about online privacy.
- Lorrie Cranor was quoted in the *Pittsburgh Post-Gazette* and other publications about anonymous emails used in the University of Pitt bomb threats.
- Norman Sadeh was quoted in the article "How a coke dealer busted by GPS tracking is changing privacy law" in *The Verge.*
- Tiffany Todd joined the CUPS Lab as our new administrative coordinator.

March 2012

- An article in *The Atlantic* discussed "The Cost of Reading Privacy Polices" by Aleecia McDonald and Lorrie Cranor.

April 2012

- Blase Ur won a Yahoo! 2012 Key Scientific Challenges Award.
- Michelle Mazurek was named a 2012 Facebook Fellow.
- Manya Sleeper and Blase Ur received honorable mentions in the NSF Graduate Research Fellowship competition.
- Blase Ur and Sauvik Das were awarded National Defense Science and Engineering Fellowships, which cover full tuition and stipend for three years.
- Alessandro Acquisti was quoted in an article in the *New York Times Sunday Review* on the post-cash, post-credit card economy.
- Nicolas Christin was quoted in a *Scientific American* article "Big Mac Attack: Apple Security Bruised after OS X Infections."
- Jason Hong was interviewed in *Technology Review* in an article "Using Crowdsourcing to Protect Your Privacy."
- Lorrie Cranor was interviewed on *NPR Morning Edition* about the cost of reading privacy policies.
- The Livehoods project (developed by Norman Sadeh, Jason Hong, Justin Cranshaw and Raz Schwartz) was featured in an article in *Technology Review*.
- Alessandro Aquisti was a featured speaker at the WSJ Data Transparency Weekend.

May 2012

- The paper "Why Johnny Can't opt Out" by Pedro Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang received a Best Paper Honorable Mention award at CHI 2012.
- Alessandro Aquisti was quoted in an *Ars Technica* article "Facial detection cameras ready to creep out San Francisco Bar patrons."
- Nicolas Christian was interviewed by NPR radio on "5 Questions, Answers about the Megaupload Case."
- Seven papers authored or co-authored by CyLab researchers were presented at the *33rd Annual IEEE Symposium on Security and Privacy* in San Francisco, California.
- Lorrie Cranor spoke at the FTC's Advertising Disclosures in a Digital World workshop.
- Julie Downs' interactive movie aimed at reducing risky sexual behavior among teens, "Seventeen Days," premiered. Supported by a five-year, $7.4 million grant from the U.S. Department of Health and Human Services, the film is an update of Downs' earlier interactive video, "What Could You Do?" which was shown to increase abstinence among teenage girls.

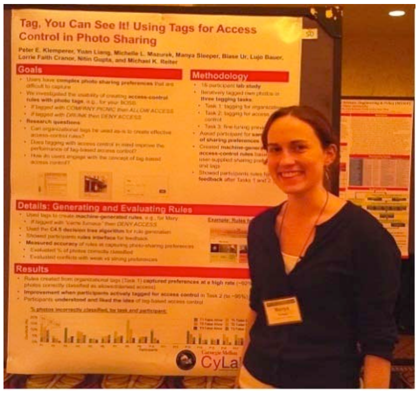
June 2012

- Justin Cranshaw, Raz Schwartz, Jason Hong, and Norman Sadeh received a best paper award for "The Livehoods Project: Utilizing Social Media to Understand the Dynamics of a City" in Proc. of the 6th International AAAI Conference on Weblogs and Social Media, Dublin, Ireland.
- Alessandro Aquisti was quoted in several articles about privacy and facial recognition.

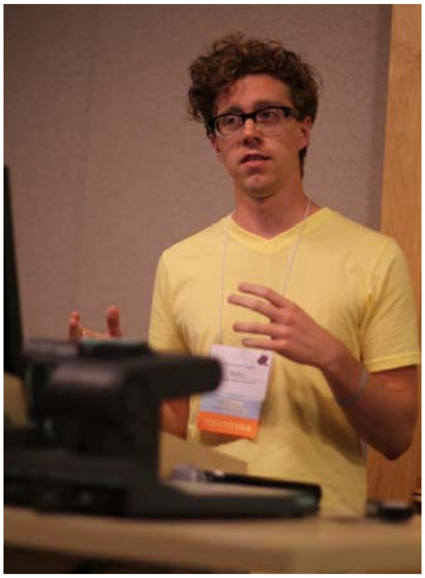
July 2012

- SOUPS 2012 will be held July 11-13 in Washington, DC.

CUPS faculty member Alessandro Acquisti testifies at a Congressional hearing in October.


Tag, You Can See It! Using Tags for Access Control in Photo Sharing
Goals
Methodology
Details: Generating and Evaluating Rules
Results
CyLab

CUPS student Manya Sleeper at the IGERT poster competition.



CUPS student Patrick Kelley giving a talk at SOUPS 2011.

Alumni Updates

Ponnurangam "PK" Kumaraguru (CUPS COS PhD 2009) has been successfully running the research group PreCog@IIIT-Delhi for more than a year now. Some highlights from the last year: All five PhD students from the group are visiting different universities around the world during spring/summer 2012, three in the US, one in Europe, and one in Brazil. In addition, two masters students and one undergrad are traveling abroad for academic purposes. One undergrad student is visiting CMU for Summer 2012.

PK co-organized a workshop on Privacy and Security in Online Social Media (PSOSM), co-located with WWW 2012 (and attended by current CUPS PhD student Blase Ur). PK, in collaboration with CMU, co-organized a Winter School in December 2011. Students from all over India participated. PreCog was featured on MIT Technology Review, Washington Post, and EDU Tech in this period. Student publications were recently presented at PSOSM 2012, IndiaHCI 2012, CEAS 2011 (Best paper award), SOCIALCOM 2011, SOUPS 2011, CHI 2011, HotMobile 2011. One student received a TCS PhD research fellowship to work on usable security and another student won the Google India Anita Borg Memorial Scholarship 2012!

Students graduating from PreCog have joined Microsoft, IBM-IRL, Paypal, Arizona State University, and Opera Systems. For more on what is keeping PK busy, visit precog.iiitd.edu.in.

PK at PSOSM.

Congratulations to CUPS alumnus **Serge Egelman** (CUPS COS PhD 2009) who is engaged to marry Carolyn Denomme. Serge and Carolyn got engaged while under water in Bonaire in March. They expect their wedding to take place on dry land sometime in the next year. Serge is currently a researcher at UC Berkeley.

Janice Tsai (CUPS EPP PhD 2009) and Richard Sharp welcomed Alexander Winslow Sharp on Jan. 13, 2012. Janice works as a Privacy Manager at Microsoft ensuring that the US and Canadian Sales and Marketing divisions are doing their work in a way that meets US and Canadian Privacy laws and satisfies the Microsoft Privacy Standard. In July, Janice will become the new Privacy Manager for Microsoft Research. She will be responsible for making sure researchers adhere to Microsoft's Privacy Standard as they conduct their research, and will be conducting usable privacy research on the side.

Welcome Alexander Winslow Sharp!

Aleecia McDonald (CUPS EPP 2010) has had a busy year as co-chair of the W3C Tracking Protection Working Group. She is a privacy researcher and Fellow at the Stanford Center for Internet and Society and consults for Mozilla on their "Do Not Track" web browser feature.

Together again: Alumni Serge Egelman, Rob Reeder and Janice Tsai reunite with Lorrie Cranor (in hat) at CHI 2012.

Recent Publications

Most CUPS publications are available on the CUPS website. The following are a selection of publications from the past year.

Privacy and Online Tracking

Can Users Control Online Behavioral Advertising Effectively?

Lorrie Faith Cranor

IEEE Security and Privacy, March/April 2012

Online Behavioral advertising (OBA) is the increasingly widespread practice of targeting users with specific online ads on the basis of a user's previous online behavior. Advertisers pay a premium for targeted ads because users are more likely to make purchases after viewing relevant ads. On the other hand, whereas some users might appreciate seeing more relevant advertisements, many say they find targeted advertising creepy and don't like the idea of companies tracking their online activities. Many tools empower users to control whether and when they're tracked for behavioral advertising; however, whether users can effectively control tracking and OBA using these tools in unclear.

Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising

Pedro Giovanni Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang

CHI 2012

We present results of a 45-participant laboratory study investigating the usability of tools to limit online behavioral advertising (OBA). We tested nine tools, including tools that block access to advertising websites, tools that set cookies indicating a user's preference to opt out of OBA, and privacy tools that are built directly into web browsers. We interviewed participants about OBA, observed their behavior as they installed and used a privacy tool, and recorded their perceptions and attitudes about that tool. We found serious usability flaws in all nine tools we examined. The online opt-out tools were challenging for users to understand and configure. Users tend to be unfamiliar with most advertising companies, and therefore are unable to make meaningful choices. Users liked the fact that the browsers we tested had built-in Do Not Track features, but were wary of whether advertising companies would respect this preference. Users struggled to install and configure blocking lists to make effective use of blocking tools. They often erroneously concluded a tool was blocking OBA when they had not properly configured it to do so.

Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising

Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang

SOUPS 2012

We report results of 48 semi-structured interviews about online behavioral advertising (OBA). We investigated non-technical users' attitudes about and understanding of OBA, using participants' expectations and beliefs to explain their attitudes. Participants found OBA to be simultaneously useful and privacy invasive. They were surprised to learn that browsing history is currently used to tailor advertisements, yet they were aware of contextual targeting. Our results identify mismatches between participants' mental models and current approaches for providing users with notice and choice about OBA. Participants misinterpreted icons intended to notify them about behavioral targeting and expected that they could turn to their browser or antivirus software to control OBA. Participants had strong concerns about data collection, and the majority of participants believed that advertisers collect personally identifiable information. They also misunderstood the role of advertising networks, basing their opinions of an advertising network on that company's non-advertising activities. Participants' attitudes towards OBA were complex and context-dependent. While many participants felt tailored advertising could benefit them, existing notice and choice mechanisms are not effectively reaching users.

Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising

Rebecca Balebako, Pedro G. Leon, Richard Shay, Blase Ur, Yang Wang, and Lorrie Faith Cranor

W2SP 2012

Online Behavioral Advertising (OBA) is the practice of tailoring ads based on an individual's activities online. Users have expressed privacy concerns regarding this practice, and both the advertising industry and third parties offer tools for users to control the OBA they receive. We provide the first systematic method for evaluating the effectiveness of these tools in limiting OBA. We first present a methodology for measuring behavioral targeting based on web history, which we support with a case study showing that some text ads are currently being tailored based on browsing history. We then present a methodology for evaluating the effectiveness of tools, regardless of how they are implemented, for limiting OBA. Using this methodology, we show differences in the effectiveness of six tools at limiting text-based behavioral ads by Google. These tools include opt-out webpages, browser Do Not Track (DNT) headers, and tools that block blacklisted domains. Although both opt-out cookies and blocking tools were effective at limiting OBA in our limited case study, the DNT headers that are being used by millions of Firefox users were not effective. We detail our methodology and discuss how it can be extended to measure OBA beyond our case study.

What Do Online Behavioral Advertising Disclosures Communicate to Users?

Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu

Technical Report CMU CyLab 2012

Online Behavioral Advertising (OBA) is the practice of tailoring ads based on an individual's online activities. We conducted a 1,505-participant online study to investigate Internet users' perceptions of OBA disclosures while performing an online task. We tested icons, accompanying taglines, and landing pages intended to inform users about OBA and provide opt-out options; these were based on prior research or drawn from those currently in use. The icons, taglines, and landing pages fell short both in terms of notifying participants about OBA and clearly informing participants about their choices. Half of the participants remembered the ads they saw but only 12% correctly remembered the disclosure taglines attached to ads. The majority of participants mistakenly believed that ads would pop up if they clicked on disclosure icons and taglines, and more participants incorrectly thought that clicking the disclosures would let them purchase their own advertisements than correctly understood that they could then opt out of OBA. "Ad-Choices," the tagline most commonly used by online advertisers, was particularly ineffective at communicating notice and choice. 45% of participants who saw "AdChoices" believed that it was intended to sell advertising space, while only 27% believed it was an avenue to stop tailored ads. A majority of participants mistakenly believed that opting out would stop all online tracking, not just tailored ads. We discuss challenges in crafting disclosures, and we provide suggestions for improvement.

Privacy Decision Making

Online Social Networks in a Post-Soviet State: How Hungarians Protect and Share on Facebook

Blase Ur and Yang Wang

IConference 2012

As Facebook has become global, users from different cultural and socio-political contexts have joined the site. We present a case study investigating how both current and historical political events, as well as the migration from a local social networking site to Facebook, impact Hungarians' privacy attitudes on Facebook. We report the results of 19 semi-structured interviews of Hungarian Facebook users, focused on behaviors, motivations and attitudes. Our results uncover a stark generation gap in Facebook privacy attitudes, with the youngest generation expressing little concern about personal information or intimate photos, whereas users older than 30 explain that they and their peers rarely share information on Facebook. Members of all age groups agree that political opinions should be kept off Facebook, but the motivating factors differ between generations. We also highlight how users' dissatisfaction with iWiW, the local social network, can be contrasted with the high degree of trust they have in Facebook.

{Privacy, Privacidad, Приватност} Policies in Social Media: Providing Translated Privacy Notice

Blase Ur, Manya Sleeper, and Lorrie Faith Cranor

PSOSM 2012

As online social media have become a global phenomenon, popular sites have been translated into many languages. However, since many social media sites rely on crowdsourced translation, privacy-critical pages are not always translated into all languages in which the sites are offered. In this paper, we examine whether or not privacy settings, privacy policies, and terms of service pages have been translated into each language available on five popular, global social networks: Facebook, Flickr, Google+, LinkedIn, and Twitter. We find large differences across sites in the availability of translated privacy pages. Some sites, such as Google+, offer privacy pages in a range of languages. In contrast, Facebook and Twitter's privacy policies have been fully translated for only 14-15% of the languages in which the sites are offered. Since "notice" is a core principle of privacy, we argue that social media users who don't speak English are not afforded complete privacy rights. We further assert that it should be the responsibility of the social networks, not the crowd, to ensure that privacy information is fully translated.

Are You Close With Me? Are You Nearby? Investigating Social Groups, Closeness, and Willingness to Share

Jason Wiese, Patrick G. Kelley, Lorrie Faith Cranor, L. Dabbish, Jason I. Hong, and J. Zimmerman

UBICOMP 2011

As ubiquitous computing becomes increasingly mobile and social, personal information sharing will likely increase in frequency, the variety of friends to share with, and range of information that can be shared. Past work has identified that whom you share with is important for choosing whether or not to share, but little work has explored which features of interpersonal relationships influence sharing. We present the results of a study of 42 participants, who self-report aspects of their relationships with 70 of their friends, including frequency of collocation and communication, closeness, and social group. Participants rated their willingness to share in 21 different scenarios based on information a UbiComp system could provide. Our findings show that (a) self-reported closeness is the strongest indicator of willingness to share, (b) individuals are more likely to share in scenarios with common information (e.g. we are within one mile of each other) than other kinds of scenarios (e.g. my location wherever I am), and (c) frequency of communication predicts both closeness and willingness to share better than frequency of collocation.

An Investigation into Facebook Friend Grouping

Patrick Gage Kelley, Robin Brewer, Yael Mayer, Lorrie Faith Cranor, and Norman Sadeh

INTERACT'2011

With increasingly large friend networks, Facebook users may be losing sight of exactly with whom they are sharing content they post to Facebook. When Facebook released a new privacy interface in summer 2010 they simplified privacy controls; however, group-based permissions remain at the core of fine-grained privacy control. In order to use these fine-grained controls, users must be able to accurately and usefully specify friend groups. In a series of 46 semi-structured interviews, we investigated how participants group their online friends using four different grouping methods. Our results show that these different mechanisms alter the strategies and groups that users create, that groups created a priori need further refinement before they can adequately address privacy decisions, and that users are adapting their online behavior to avoid the need to specify groups in the current Facebook interface. We conclude with several recommendations that would allow users improved group-based access control.

Privacy, Location, and Mobile Devices

The Livehoods Project: Utilizing Social Media to Understand the Dynamics of a City

Justin Cranshaw, Raz Schwartz, Jason Hong, Norman Sadeh

Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media, ICWSM

Studying the social dynamics of a city on a large scale has traditionally been a challenging endeavor, often requiring long hours of observation and interviews, usually resulting in only a partial depiction of reality. To address this difficulty, we introduce a clustering model and research methodology for studying the structure and composition of a city on a large scale based on the social media its residents generate. We apply this new methodology to data from approximately 18 million check-ins collected from users of a location-based online social network. Unlike the boundaries of traditional municipal organizational units such as neighborhoods, which do not always reflect the character of life in these areas, our clusters, which we call Livehoods, are representations of the dynamic areas that comprise the city. We take a qualitative approach to validating these clusters, interviewing 27 residents of Pittsburgh, PA, to see how their perceptions of the city project onto our findings there. Our results provide strong support for the discovered clusters, showing how Livehoods reveal the distinctly characterized areas of the city and the forces that shape them.

A Comparative Study of Location-sharing Privacy Preferences in the U.S. and China

Jialiu Lin, Norman Sadeh, Michael Benisch, Jianwei Niu, Jason Hong, Banghui Lu, Shaohui Guo

CyLab Technical Report cmu-cylab-12-003

While prior studies have provided us with an initial understanding of people's location-sharing privacy preferences, they have been limited to Western countries and have not investigated the impact of the granularity of location disclosures on people's privacy preferences. We report findings of a three-week comparative study collecting location traces and location-sharing preferences from two comparable groups in the U.S. and China. Results of the study shed further light on the complexity of people's location-sharing privacy preferences and key attributes influencing willingness to disclose locations to others and to advertisers. While our findings reveal many similarities between U.S. and Chinese participants, they also show interesting differences, such as differences in willingness to share location at 'home' and at 'work' and differences in the granularity of disclosures people feel comfortable with. We conclude with a discussion of implications for the design of location-sharing applications and location-based advertising.

A Conundrum of Permissions: Installing Applications on an Android Smartphone

Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, David Wetherall

Workshop on Usable Security (USEC) 2012

Each time a user installs an application on their Android phone they are presented with a full screen of information describing what access they will be granting that application. This information is intended to help them make two choices: whether or not they trust that the application will not damage the security of their device and whether or not they are willing to share their information with the application, developer, and partners in question. We performed a series of semi-structured interviews in two cities to determine whether people read and understand these permissions screens, and to better understand how people perceive the implications of these decisions. We find that the permissions displays are generally viewed and read, but not understood by Android users. Alarmingly, we find that people are unaware of the security risks associated with mobile apps and believe that app marketplaces test and reject applications. In sum, users are not currently well prepared to make informed privacy and security decisions around installing applications.

Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing

Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, Joy Zhang

Workshop on Usable Security (USEC) 2012

Smartphone security research has produced many useful tools to analyze the privacy-related behaviors of mobile apps. However, these automated tools cannot assess people's perceptions of whether a given action is legitimate, or how that action makes them feel with respect to privacy. For example, automated tools might detect that a blackjack game and a map app both use one's location information, but people would likely view the map's use of that data as more legitimate than the game. Our work introduces a new model for privacy, namely privacy as expectations. We report on the results of using crowdsourcing to capture users' expectations of what sensitive resources mobile apps use. We also report on a new privacy summary interface that prioritizes and highlights places where mobile apps break people's expectations. We conclude with a discussion of implications for employing crowdsourcing as a privacy evaluation technique.

Who's your best friend?: targeted privacy attacks In location-sharing social networks

Vassilis Kostakos, Jayant Venkatanathan, Bernardo Reynolds, Norman Sadeh, Eran Toch, Siraj A Shaikh, Simon Jones

UBICOMP 2011

This paper presents a study that aims to answer two important questions related to targeted location-sharing privacy attacks: (1) given a group of users and their social graph, is it possible to predict which among them is likely to reveal most about their whereabouts, and (2) given a user, is it possible to predict which among her friends knows most about her whereabouts. To answer these questions we analyse the privacy policies of users of a real-time location sharing application, in which users actively shared their location with their contacts. The results show that users who are central to their network are more likely to reveal most about their whereabouts. Furthermore, we show that the friend most likely to know the whereabouts of a specific individual is the one with most common contacts and/or greatest number of contacts.

Passwords and Authentication

Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms

Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Tim Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez

2012 IEEE Symposium on Security and Privacy

Text-based passwords remain the dominant authentication method in computer systems, despite significant advancement in attackers' capabilities to perform password cracking. In response to this threat, password composition policies have grown increasingly complex. However, there is insufficient research defining metrics to characterize password strength and evaluating password-composition policies using these metrics. In this paper, we describe an analysis of 12,000 passwords collected under seven composition policies via an online study. We develop an efficient distributed method for calculating how effectively several heuristic password-guessing algorithms guess passwords. Leveraging this method, we investigate (a) the resistance of passwords created under different conditions to password guessing; (b) the performance of guessing algorithms under different training sets; (c) the relationship between passwords explicitly created under a given composition policy and other passwords that happen to meet the same requirements; and (d) the relationship between guessability, as measured with password-cracking algorithms, and entropy estimates. We believe our findings advance understanding of both password-composition policies and metrics for quantifying password security.

How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor

USENIX Security, 2012

To help users create stronger text-based passwords, many web sites have deployed password meters that provide visual feedback on password strength. Although these meters are in wide use, their effects on the security and usability of passwords have not been well studied. We present a 2,931-subject study of password creation in the presence of 14 password meters. We found that meters with a variety of visual appearances led users to create longer passwords. However, significant increases in resistance to a password-cracking algorithm were only achieved using meters that scored passwords stringently. These stringent meters also led participants to include more digits, symbols, and uppercase letters. Password meters also affected the act of password creation. Participants who saw stringent meters spent longer creating their password and were more likely to change their password while entering it, yet they were also more likely to find the password meter annoying. However, the most stringent meter and those without visual bars caused participants to place less importance on satisfying the meter. Participants who saw more lenient meters tried to fill the meter and were averse to choosing passwords a meter deemed "bad" or "poor." Our findings can serve as guidelines for administrators seeking to nudge users towards stronger passwords.

Correct horse battery staple: Exploring the usability of system-assigned passphrases

Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor

SOUPS 2012

Users tend to create passwords that are easy to guess, while system-assigned passwords tend to be hard to remember. Passphrases, space-delimited sets of natural language words, have been suggested as both secure and usable for decades. In a 1,476-participant online study, we explored the usability of 3- and 4-word system-assigned passphrases in comparison to system-assigned passwords composed of 5 to 6 random characters, and 8-character system-assigned pronounceable passwords. Contrary to expectations, system-assigned passphrases performed similarly to system-assigned passwords of similar entropy across the usability metrics we examined. Passphrases and passwords were forgotten at similar rates, led to similar levels of user difficulty and annoyance, and were both written down by a majority of participants. However, passphrases took significantly longer for participants to enter, and appear to require error-correction to counteract entry mistakes. Passphrase usability did not seem to increase when we shrunk the dictionary from which words were chosen, reduced the number of words in a passphrase, or allowed users to change the order of words.

Access Control

Tag, You Can See It! Using Tags for Access Control in Photo Sharing

Peter F. Klemperer, Yuan Liang, Michelle Mazurek, Manya Sleeper, Blase Ur, Lujo Bauer, Lorrie Faith Cranor, Nitin Gupta, Michael K. Reiter

CHI 2012

Users often have rich and complex photo-sharing preferences, but properly configuring access control can be difficult and time-consuming. In an 18-participant laboratory study, we explore whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access-control policies. We find that (a) tags created for organizational purposes can be repurposed to create efficient and reasonably accurate access-control rules; (b) users tagging with access control in mind develop coherent strategies that lead to significantly more accurate rules than those associated with organizational tags alone; and (c) participants can understand and actively engage with the concept of tag-based access control.

Out of sight, out of mind: Effects of displaying access-control information near the item it controls

Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter

Privacy, Security, and Trust 2012

We take a detailed look at how users, while focusing on non-permission tasks, notice and fix access-control permission errors depending on where the access-control policy is spatially located on a photo-sharing website. The access-control policy was placed on an online photo-sharing website under the photo or album, on the sidebar, or on a separate settings page. We find that placing the access-control policy directly under photos and album thumbnails improves participants' ability to notice errors in their access-control settings without negatively impacting non-access-control tasks.

Computer Security Warnings

Improving Computer Security Dialogs

Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri and Manya Sleeper

INTERACT' 2011

Security dialogs warn users about security threats on their computers; however, people often ignore these important communications. This paper explores the links between warning dialog design and user understanding of, motivation to respond to, and actual response to computer security warnings. We measured these variables through a 733-participant online study that tested a set of four existing computer security warnings and two redesigned versions of each across low- and high-risk conditions. In some cases our redesigned warnings significantly increased participants' understanding and motivation to take the safest action; however, we were not able to show that participants' responses were differentiated between low and high risk conditions. We also observed that motivation seemed to be a more important predictor of taking the safest action than understanding. However, other factors that may contribute to this behavior warrant further investigation.

Dissertations

Measuring and Modeling Security and Privacy Laws: A Doctoral dissertation

Sasha Romanosky

April 2012

The popularity of social media, e-commerce, and mobile services affords consumers many benefits. However, firms engaging in these services can impose externalities on consumers have been lost form over 2,800 data breaches, and identity theft caused an estimated $13.3 billion in consumer financial loss in 2010. This manuscript discusses policy interventions designed to address these externalities caused by data breaches and resulting identity theft. I first present an overview of three common interventions: *ex ante* regulation, information disclosure, and *ex post* liability. The three substantive chapters then provide both empirical and analytical analysis of information disclosure, and *ex post* liability.

Finally, I examine *ex post* liability. If customers are indeed harmed by data breaches, litigation may provide one form of financial redress. However, given that very little is known about these suits, I collected of a representative sample of over 230 federal lawsuits in order to understand which breaches are being litigated and which data breach lawsuits settle. I find that firms are much less likely to be sued when they provide some form of redress following a breach (e.g. credit monitoring), but are much more likely to be sued for breaches involving financial data. However, while the compromise of financial information leads to more litigation, legal procedural matters, and the compromise of medical information is most strongly correlated with settlement.

The analyses presented in this manuscript seek to provide deeper insights into the mechanisms, incentives, costs and outcomes of data breaches and the privacy harms caused by the loss or theft of personal information. While I anticipate that the main audience of this work will be policy makers and legislators, we believe these results can also inform firms that collect and innovate using personal information, and the consumers that disclose their information.

Lorrie Cranor's art quilt, "Lying on the Floor of the Pittsburgh Children's Museum Staring at the Ceiling" was on display at the Pittsburgh Center for the Arts from May through July. The quilt won the award for best interpretation of theme in the exhibition: Lenses and Filters: A view through the needle's eye.

After over five years of service to our lab, the CUPS couch turned vicious and began attacking those who walked by. As evidenced by the graduate students with gaping holes in their pants, the couch had become hazardous. As all usable security experts know, the best thing to do when confronted with a hazard is to remove it. In the meantime, a warning was posted.

After the hazardous couch was removed, the CUPS students selected a brand new purple couch to replace it. Pictured above, Lorrie Cranor, Patrick Kelley, Manya Sleeper, Pedro Leon, and Kami Vaniea try out the new couch while Cristian Bravo-Lillo and Yang Wang have to settle for a seat on the floor.

All dressed up! Pedro Leon, Blase Ur, Jim Graves, Dave Gordon, and Lorrie Cranor at the Privacy Law Scholars Conference reception in Washington, DC.

Lorrie Cranor did a radio interview at WQED on Halloween.