Lightning Introductions

ENGINEERING PRIVACY

August 31-September 1st, 2015

CCC

Computing Community Consortium

Catalyst

Annie Antón / Georgia Institute of Technology

Georgia Tech School of Interactive Computing
College of Computing

What is the nature of privacy and security threats posed by the Internet of Things in the context of meaningful applications in the home, for the individual, and for a community of people?

What should the modern technical, social, and legal conceptions of privacy be given these privacy and security threats?

CCC
Computing Community Consortium
Catalyst

Eleanor Birrell / Cornell University

How should we express and enforce restrictions on how information is used?

Cornell University
Department of Computer Science

CCC
Computing Community Consortium
Catalyst

Travis Breaux / CMU

Carnegie Mellon University

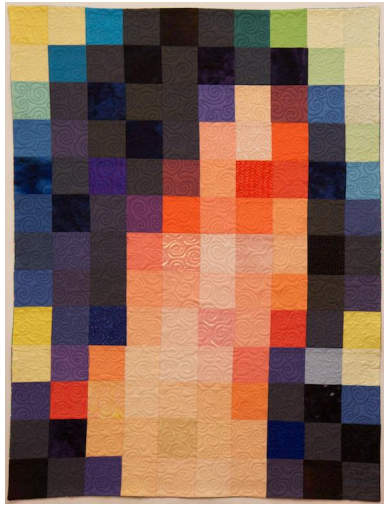
We're developing new notations and tools to empower software engineers to reason about design trade-offs affecting privacy

I also teach a course on Engineering Privacy as part of CMU's Masters of Privacy
http://privacy.cs.cmu.edu/

Koen Buyens/ Cigital

Cigital

- I am helping clients to build security/privacy into their software at every stage of the SDLC.
- How can we (automatically) identify privacy problems throughout the SDLC?
- How do we make the most appropriate design decision given the client's, sometimes conflicting, requirements?



Carnegie Mellon University

Lorrie Cranor / CMU

- How can we evaluate the usability and effectiveness of privacy notices and tools?
- What factors do people consider when they make decisions about privacy?
- How can we communicate more effectively about privacy?
- How can we make privacy tools more usable and useful, and less burdensome on users?

Bethan Cantrell / Microsoft

Identity / identifiers
Privacy tools & processes
Technical privacy

Microsoft

CCC
Computing Community Consortium
Catalyst

Richard Chow / Intel

Privacy Researcher and Architect

Working on:
Retaining control of your data in this era of Big Data, IoT, and the Cloud

Anupam Datta / CMU

Privacy through Accountability:

<u>Privacy as restrictions on personal information flow</u>

- Privacy policy specification languages
- Formalizing contextual integrity
- Formalizing purpose restrictions on data use

<u>Accountability mechanisms for privacy protection</u>

- Audit algorithms for checking logs
- Algorithms/tools for checking big data systems in white-box and black-box settings

Frank Dawson / Nokia

Privacy Engineer's Motto

de quibus confidendum, sed verificare veritate

Privacy Engineer's Theorem

$$RK = \sum_{i=1}^{n}(Fn(\mathrm{Tt}_i, \mathrm{Hm}_i, \mathrm{Hp}_i, \mathrm{Rm}_i))$$
$$TH = \sum_{i=1}^{n}(Fn(\mathrm{Pp}_i, \mathrm{Pl}_i, \mathrm{Ti}_i, \mathrm{Ps}_i))$$
$$In = Fn(Id_i, Lk_i, Ob_i)$$
$$PI = \sum_{i=1}^{n}(Fn(Pi_i, In_i)$$

CCC
Computing Community Consortium
Catalyst

Jose del Alamo / Universidad Politecnica de Madrid

What is the status of the privacy by design practice: craftsmanship or engineering?

Can we systematize privacy engineering activities to be adopted by a wider community of engineers in a reliable and efficient way?

Related work: PRIPARE contribution to ISO/IEC JTC1/SC27/WG5 study period on Privacy Engineering Framework

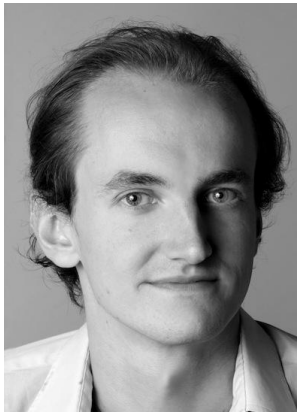
Damien Desfontaines / Google

Google

How can we monitor & verify privacy properties at scale?

How can we ensure that all product launches are compliant with a set of privacy principles?

Nick Doty / UC Berkeley



Berkeley School of Information

I’m studying how engineers think about privacy and security in Internet and Web standard-setting. How do voluntary, multistakeholder processes affect privacy in technology?

Ann Drobnis / CCC

How can we ensure that privacy practices are adopted across disciplines?

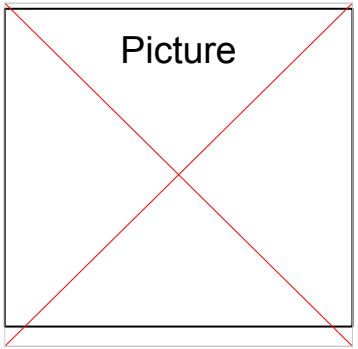
CCC
Computing Community Consortium
Catalyst

CCC
Computing Community Consortium
Catalyst

Khaled El Emam / University of Ottawa

uOttawa

Robert Ferguson / Automatic Labs



AUTOMATIC

For decades most people hadn't considered our cars to be computers, but as cars and other things are coming online (IoT) they have lots to say about us. How do we design for privacy as old systems come online when they were not designed for it in the first place?

Matt Fredrikson / CMU

Carnegie Mellon University

Practical, rigorous approaches for reasoning about privacy in software

- Tools that help developers implement privacy correctly
- Formal methods and analysis to ensure confidentiality via information flow
- Algorithms that balance privacy and functionality

Gerald Friedland / ICSI & UC Berkeley

Interests:

- Privacy Education
- Privacy for Multimedia (videos, images)
- Dark data flows

Current work:

www.teachingprivacy.org

multimedia.icsi.berkeley.edu

Simson Garfinkel / NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Related work:

- Draft NISTIR 8063, De-Identification of Personally Identifiable Information
- Draft NISTIR 8062, Privacy Risk Management for Federal Information Systems
- National Privacy Research Strategy

Carmela Troncoso / Gradiant

What is privacy engineering? is it a technical issue or not? Will PETs solve everything?

Is privacy engineering within reach for everybody? What are we missing?

Gradiant

CCC
Computing Community Consortium
Catalyst

Nathan Good / Good Research

good RESEARCH

How much is privacy by design a part of existing design processes, and what can privacy by design learn from these?

Susan Graham / UC Berkeley & CCC

Berkeley
UNIVERSITY OF CALIFORNIA

Technology changes rapidly. How can Privacy by Design keep up?

How can privacy services be made understandable by the typical user?

Related work: *Big Data: A Technological Perspective.* Executive Office of the President; President's Council of Advisors on Science and Technology. May 2014

CCC
Computing Community Consortium
Catalyst

Paul Grassi / NIST, NSTIC NPO

NIST National Institute of Standards and Technology U.S. Department of Commerce

NSTIC

Senior Standards and Technology Advisor, NIST

Supporting the development of publicly built, open standards that advance privacy enhancing techniques.

Focused on applying these standards into solutions such as Connect.Gov and NSTIC pilot programs.

Lead for upcoming revision of NIST SP 800-63-2

CCC Computing Community Consortium Catalyst

Mohit Gupta / Clever

Product Manager, Infrastructure. Technical Lead, Security and Privacy

- How to design processes, tooling and organizational policy for early stage companies?
- Design Patterns for Privacy

Clever

clever.com
privacypatterns.org

Seda Gürses / NYU

How do we reconcile different privacy research paradigms in computer science and engineering when addressing privacy in systems?

What is the impact of the upcoming cybersecurity strategy on privacy research and practice?

NEW YORK UNIVERSITY
INFORMATION LAW INSTITUTE

CCC
Computing Community Consortium
Catalyst

Greg Hager / Johns Hopkins & CCC

Is there a science of privacy that will provide a principled framework for design and regulation?

Is it possible to create “learning privacy systems” that adapt to individual and societal behaviors?

Joseph Hall / CDT

CENTER FOR DEMOCRACY & TECHNOLOGY

How might we effectively embed privacy (and other human rights values) into sociotechnical infrastructure?

What are promising (even, viral) methods for making security and privacy tools more understandable, useful, satisfying, and effective?

Peter Harsha / CRA

What does a privacy research agenda look like and how do we explain it to policymakers when they ask?

CRA
Computing Research Association

CRA
Government Affairs
For America!

(Unofficial logo)

CCC
Computing Community Consortium
Catalyst

Hanan Hibshi / CMU

Carnegie Mellon University

Exploring factors contributing to privacy risk assessment

Jaap-Henk Hoepman / Radboud University Nijmegen

Radboud University

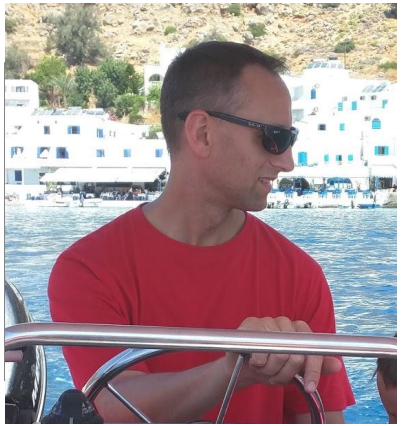
Privacy & Identity Lab

Research topic: privacy enhancing protocols and privacy by design.

Interest: providing lawyers and policy makers with key insights from privacy engineering research and computer science in general.

CCC
Computing Community Consortium
Catalyst

Giles Hogben / Google

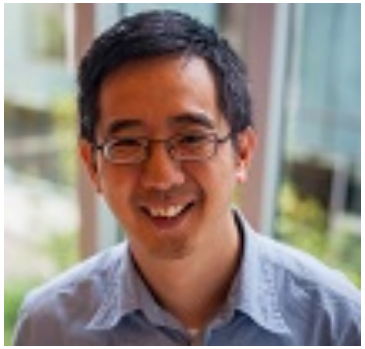


Google

Android and Ads privacy at Google. Lots of privacy design decisions.

Research interests: multi-user data collection, privacy for machine learning, understanding user-impact.

Jason Hong / CMU



Carnegie Mellon University

Brian Ince / DNI

Limin Jia / CMU

Carnegie Mellon University
CyLab

- **Privacy:** logic-based policy specification and policy enforcement mechanisms
- **Security:** applying logic and language-based techniques to analyze and build secure software systems

Dawn Jutla / Saint Mary's University

How can software engineers document their compliance with Privacy by Design principles?

Related Work: OASIS Annex Guide to PbD Documentation for Software Engineers and

OASIS Privacy by Design Documentation for Software Engineers. Committee Draft Specification.

SOBEY SCHOOL OF BUSINESS | MASTER OF TECHNOLOGY ENTREPRENEURSHIP AND INNOVATION

OASIS
Advancing open standards for the information society

CCC
Computing Community Consortium
Catalyst

Apu Kapadia / Indiana University

Pragmatic privacy mechanisms
understand needs + usable and effective design

Wearable cameras + IoT
Identifying and transforming 'sensitive' imagery

Accountable anonymity
constraining anonymous behaviors

Interdisciplinary approaches
Computer Vision, Network+Information Science, Sociology, Engineering+Clinical Psychology

INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING
Center for Security Informatics
Bloomington

David Kelts / MorphoTrust USA

Director of Product Architecture: Responsible for coherence of software architectures across MorphoTrust Digital Identity product lines

Principal Investigator: http://morphotrust.com/NSTIC

Turning technologies such as UMA, and OpenID Connect into functional, high-trust, privacy-enhancing Citizen-Managed Identity for the US

SAFRAN
MorphoTrust USA

Simplify protect and secure the lives of the American people

Aleksandra Korolova / USC

- Practically useful algorithms for data mining and sharing with rigorous and measurable privacy guarantees
- Data-driven understanding of individuals' privacy preferences

USC Viterbi
School of Engineering

CCC
Computing Community Consortium
Catalyst

Susan Landau / WPI

- I have worked in academia (Wesleyan, UMass, WPI) and industry (Sun Microsystems, Google).
- I have been a theoretician, a policy wonk, and a privacy analyst.
- My current research is communications surveillance, public policy, and privacy.
- I have previously worked on identity management, DRM, and cryptography/crypto policy.

Naomi Lefkovitz / NIST

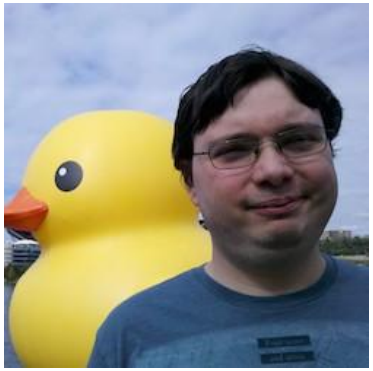
Using privacy engineering objectives and risk management to implement privacy principles in information systems

Related work: Draft NISTIR 8062, Privacy Risk Management for Federal Information Systems

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CCC
Computing Community Consortium
Catalyst

CM Lubinski / 18f



18F

Software Engineer

18F (General Services Administration)
Consumer Financial Protection Bureau
United States Digital Service

http://cfpb.github.io/eRegulations/

Ashwin Machanavajjhala / Duke

Duke
UNIVERSITY

Bridging the theory and practice of private data analysis

- Applying differential privacy on real data and live systems.
- Designing usable and rigorous privacy notions resulting in useful data releases.

Keith Marzullo / NITRD

Aaron Massey / UMBC

UMBC
AN HONORS UNIVERSITY IN MARYLAND

How do software engineers and designers demonstrate compliance with privacy laws?

Ilya Mironov / Google

Google

- 2003–2014 worked in Microsoft Research contributing to development of differential privacy
- 2014–present working in Google on making rigorous privacy usable and useful

Deirdre Mulligan / UC Berkeley

Berkeley School of Information

Current Research:
How do organizations understand and manage privacy? What external factors--policies, institutions, non-state actors, etc.--lead to deeper engagement with privacy as a social and political concept, and richer policies and practices that embed privacy into technical systems and business processes.

Helen Nissenbaum / NYU

NYU INFORMATION LAW INSTITUTE
PRIVACY RESEARCH GROUP

- ➔ What can and cannot be achieved with privacy technology?
- ➔ Challenging famous privacy survey findings
- ➔ Achieving privacy with data obfuscation
- ➔ PbD in Practice: Compass project: modeling privacy in social networks with contextual norms

Lake Polan / UChicago

Cultural anthropologist, researching the social, political, and conceptual effects of tech- and market-based efforts to save privacy. How do our understanding and experience of privacy change as it becomes embedded within technical systems? How do such changes impact the forms of freedom, dignity, and democratic participation available today?

THE UNIVERSITY OF CHICAGO

CCC
Computing Community Consortium
Catalyst

Sören Preibusch / Google

Google employee, attending in personal capacity

Consumers' privacy choices on the Web: social, search, shopping

Behavioural economics: large field and lab experiments (*N*=300..500)

Current research:

- Guide to measuring privacy concern (IJHCS)
- Privacy Behaviours after Snowden (CACM)
- Value of Privacy in Web Search (S&P)
- Web form filling behaviour

Rebecca Richards / NSA

NSA Civil Liberties and Privacy Officer

Developing a methodical, repeatable approach to assessing civil liberties and privacy risks.

Building a Civil Liberties and Privacy Program at NSA.
Previously worked at DHS building a privacy program.

Ira Rubinstein / NYU

New York University
A private university in the public service

What regulatory structures best support privacy by design?
Where privacy engineers hold competing views (e. g., on deidentification), how can they reconcile their differences in support of sound regulatory policy?
Recent papers: Anonymization and Risk

Norman Sadeh / CMU

Master of Science in Information Technology

privacy ENGINEERING

- **Notice and Choice for IoT**: Can we reconcile privacy and usability?
  - Could **Personalized Privacy Assistants** be the solution?
- I co-founded & co-direct **CMU's Master's Program in Privacy Engineering** --- www.privacy.cs.cmu.edu
- I lead an NSF Frontier project on "**Usable Privacy Policies**" - combining crowdsourcing, machine learning and natural language processing to annotate privacy policies at scale - joint project CMU, Fordham, Stanford, Columbia and UW --- www.usableprivacy.org
- Professor of Computer Science at CMU

Tomas Sander / HP

Researcher at HP Labs.
I'm interested in the enterprise side of privacy.

How can organizations handle data in a privacy protecting way?
What are best privacy practices for emerging areas such as sharing of security and threat data?

Stuart Shapiro / MITRE

MITRE

Principal Cyber Security & Privacy Engineer

How do you integrate privacy into systems engineering in a way that systems engineers can relate to, while still leveraging privacy-specific techniques?

Katie Shilton / UM College Park

What work processes and practices encourage developers to prioritize data protection and privacy by design?

What factors encourage social and political issues to become central design concerns?

How do developers translate social issues into technical affordances?

UNIVERSITY OF MARYLAND

CCC
Computing Community Consortium
Catalyst

Manya Sleeper / CMU

Carnegie Mellon University

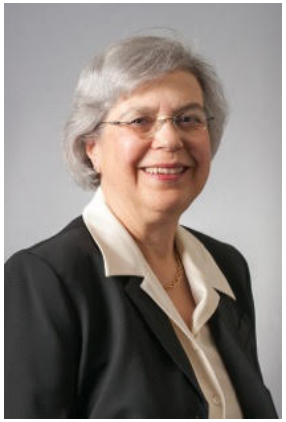
I’m interested in exploring factors that drive online sharing decisions

Daniel Smullen / CMU

Carnegie Mellon University

Developing new tools to help software engineers reason about requirements and architectural decisions affecting privacy and security.

Karen Sollins / MIT



MIT CSAIL

- Network architecture: Information Centric Networking, architecture evaluation
- Networking: Naming, addressing, network management, security, performance
- Privacy: Chair, MIT Big Data Privacy Working Group, Chair, MIT Communications Futures Privacy and Security Working Group, Member, MIT Cybersecurity Initiative (Privacy and DDoS)

Michael Tschantz / ICSI

The International Computer Science Institute

Models of privacy and security using techniques from formal methods, artificial intelligence, and machine learning

Manya Sleeper / CMU

I’m interested in exploring factors that drive online sharing decisions

Carnegie Mellon University

CCC
Computing Community Consortium
Catalyst

Blase Ur / CMU

Carnegie Mellon University

I'm interested in many privacy-related topics: data-driven privacy, online behavioral advertising, teens and parents, and passwords.

Elizabeth Van Couvering / Karlstad University

Social scientist studying the industrial organisation of digital media; focus has been on search engines & social media

Currently, strong economic incentives support a lack of privacy in company/individual relations - any privacy design has to consider how these barriers to privacy can be overcome

Everyone wants to snoop,
but no one wants to be watched.
Citizens want privacy, governments and companies want secrecy, and everyone wants everyone else to be “open”.

Richmond Wong / UC Berkeley

Berkeley School of Information

What types of cultural values regarding privacy are associated with, or embedded in technologies and in policy? How can design techniques play a role in thinking about these values?

Helen Wright / CCC

Enabling researchers from various disciplines to interact and collaborate to develop solutions that address privacy needs

CCC
Computing Community Consortium
Catalyst

CCC
Computing Community Consortium
Catalyst

Heng Xu / NSF & Penn State

The White House Big Data reports recommend adoption of a “responsible use framework” that would provide greater focus on the use of data, and would hold entities that utilize data accountable for responsible use of the data.

How to develop the “responsible use framework”?