Lightning Introductions

PRIVACY BY DESIGN

February 5-6, 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

Alvaro Bedoya / Georgetown Privacy

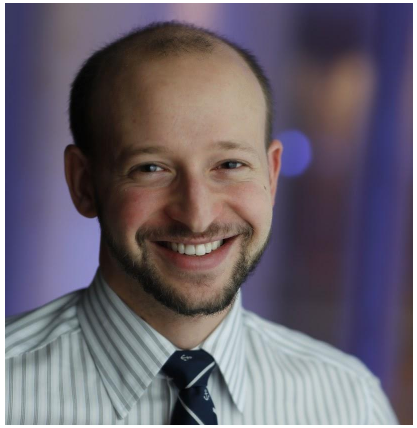
GEORGETOWN LAW
Center on Privacy & Technology

What does surveillance and Big Data mean for vulnerable communities?

Why are our commercial privacy laws so bad? And what might lobbying and campaign donations have to do with it?

How do we teach lawyers to work with technologists, and vice versa?

Mike Berger / UCB



Berkeley School of Information

What role can each of the three branches of government play in catalyzing privacy by design?

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/

Justin Brookman / CDT

CENTER FOR DEMOCRACY & TECHNOLOGY

How do we convert consumer concern about privacy into consumer demand for privacy features?

What easy tools can we offer to consumers exercise meaningful agency over the sharing of their personal information?

CCC
Computing Community Consortium
Catalyst

Sean Brooks / NIST

NIST is developing a set of engineering objectives to better enable effective organizational privacy risk assessment.

What inputs should be considered when assessing privacy risk to individuals, and how do those inputs relate to one another?

Alissa Cooper / Cisco

Can Privacy by Design be made relevant to iterative, agile, continuous software and systems engineering efforts where very little is “by design”?

Carnegie Mellon University
COMPUTER SCIENCE DEPARTMENT
SCHOOL OF COMPUTER SCIENCE
Electrical & Computer ENGINEERING

Anupam Datta / CMU

Privacy through Accountability:
Computational foundations of privacy principles and tools for checking software systems and audit logs for compliance with privacy principles, policies, and regulations

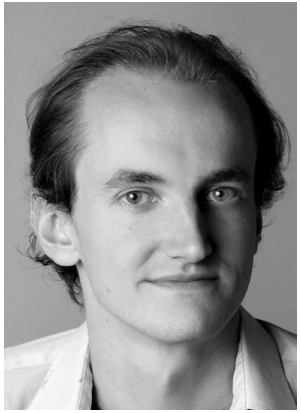
Results: Formalizing Contextual Integrity, Purpose Restrictions, Information Flow Experiments, Privacy Compliance of Big Data Software Systems

John Delong / NSA

Four research areas to develop the *Science* of Privacy to support the *Art* of Privacy:

- Assessing risk
- Mathematical models of risk
- Accountability tied to risk
- Applied privacy engineering

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

Ed Felten / Princeton

PRINCETON UNIVERSITY

Research topic: Using computer science tools to improve accountability of algorithmic processes.

Policy interest: Improving public policy discourse by incorporating valid privacy science, reducing influence of privacy pseudoscience.

Edward Fok / USDOT-FHWA

We are designing privacy into Connected Vehicle systems in order to transform surface mobility one step at a time.

CCC
Computing Community Consortium
Catalyst

Jonathan Fox / Intel Security

How do we demystify privacy so stakeholders can understand, design, and engineer user experiences and functional requirements accordingly?

intel Security

CCC
Computing Community Consortium
Catalyst

Robert Gellman

Picture

Pose a question to the group or briefly describe your current research topic

Academia or Industry Logo

Ari Gesher / Palantir

Currently working on The Architecture of Privacy, a high-level architecture manual for privacy-protective safeguards inside of systems that hold sensitive data.

Palantir

Jesse Goldhammer / UC Berkeley

Berkeley School of Information

Pose a question to the group or briefly describe your current research topic

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?

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

Seda Gurses / NYU

NEW YORK UNIVERSITY

Pose a question to the group or briefly describe your current research topic

CCC
Computing Community Consortium
Catalyst

Joseph Lorenzo Hall / CDT

How much of privacy in design is about better *operationalizing processes and rhythms* and how much needs to come from *changes in norms and "culture"* of tech innovation and development?

Assuming we can figure that out, what do we do?

CENTER FOR DEMOCRACY & TECHNOLOGY

CCC
Computing Community Consortium
Catalyst

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

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

Jen King / UC Berkeley

How can we design for privacy at the human-interaction level?
How can we bring “designers” (user experience professionals and researchers) into the Privacy by Design discussion?

Berkeley School of Information

CCC
Computing Community Consortium
Catalyst

Colin Koopman / University of Oregon

UNIVERSITY
OF OREGON

My research focus is information ethics and politics. I am a philosopher by training, so I love theoretical challenges and research spaces where there are no obviously-correct answers.

I am involved in two collaborations on privacy:

- A taxonomy of privacy, with Deirdre Mulligan and others at the UC Berkeley iSchool
- Metrics for privacy, with Jun Li and others in Computer Science at the Univ. of Oregon.

CCC
Computing Community Consortium
Catalyst

Keith Marzullo / NSF

Developing a strategic plan for federal research into the scientific foundations of privacy.

Sigurd Meldal / SJSU

Where (and how) does privacy fit into the general education of an informed citizenry?
Of an informed engineer?

SJSU SAN JOSÉ STATE UNIVERSITY

CCC
Computing Community Consortium
Catalyst

Mary Morshed / CalPERS

CalPERS

Can a cost-benefit analysis be made for privacy by design, as opposed to following a traditional privacy impact assessment methodology?

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.

Erik Neuenschwander / Apple

As product features change, how can users proactively maintain an appropriate privacy balance?

As implementations of those features evolve, how do product teams measure and maintain that same balance?

Helen Nissenbaum / NYU

NEW YORK UNIVERSITY

Obfuscation: A User's Guide to Privacy and Protest
Privacy, Big Data, and the Public Good
AdNauseam, TrackMeNot
Values at Play in Digital Games
Privacy in Context: Technology, Policy and the Integrity of Social Life
Application Areas: Education, Court records, Health records, web search, online privacy, security/privacy.

Nicole Ozer / ACLU

I am the Technology and Civil Liberties Policy Director for the ACLU of California and lead our state-wide team working on the intersection of privacy, free speech, and new technology.

Related publications/work:
Privacy & Free Speech: It's Good for Business. Primer of case studies and tips to help companies bake privacy and free speech safeguards into design and business development process. www.aclunc.org/business/primer

Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change (2012). New York University Review of Law & Social Change, Vol. 36, 2012. http://ssrn.com/abstract=2083733

ACLU
AMERICAN CIVIL LIBERTIES UNION of CALIFORNIA

CCC
Computing Community Consortium
Catalyst

Edward Palmieri / Facebook

- Working to maintain a strong privacy program that balances innovation and efficient product development.

➔ What trends in privacy design are most effective/desirable? Any concerns?

Audrey Plonk / Intel

Can privacy by design provide an internationally acceptable solution set?

Are there elements that conflict with the resurgence of governmental policies around product design (e. g., cryptography)?

Tal Rabin / IBM & CCC

Research area; Multiparty Computations

Question: How do we bring the existing privacy enabling technologies (such as MPC) from theory to practice? Why is it hard for them to gain traction?

Aaron Rieke / Robinson + Yu

robinson +yu

Where and how does privacy overlap with civil rights issues?

How can society benefit from new data while ensuring fairness and respecting autonomy?

Where might data use limitations, as opposed from limits on collection, be wise and feasible?

Thomas Roessler / Google

Google

Pose a question to the group or briefly describe your current research topic

Ira Rubinstein / NYU

New York University
A private university in the public service

How do we translate the Fair Information Practices into engineering and usability principles and how do we create the regulatory incentives to ensure that companies engage in privacy by design?

Fred Schneider / Cornell

Current Research: Determining whether usage-based privacy is feasible and, if so, where.

Elaine Sedenberg / UC Berkeley

Berkeley School of Information

My research focuses on the legal, policy, and ethical aspects of data access for research purposes. How can we design systems that open up user-generated data for research without compromising the autonomy and privacy interests of individuals?

Peter Swire / Georgia Tech/ Alston & Bird

In what way is the baseline for Privacy by Design the same or different from Security by Design/Security by Default?

Georgia Tech

CCC
Computing Community Consortium
Catalyst

Aimee Tabor / Berkeley

Berkeley
UNIVERSITY OF CALIFORNIA

Who is the privacy professional of the future & what are the knowledge and skills they will need to be successful?

Current Research:
Best practices for teaching and learning in STEM fields.

Michael Tschantz / ICSI

I use the models of artificial intelligence and statistics to solve the problems of privacy and security. My current research includes automating information flow experiments to hold information collectors accountable.

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

CCC
Computing Community Consortium
Catalyst

Tomas Vagoun / NITRD

Developing a federal privacy R&D strategic plan.

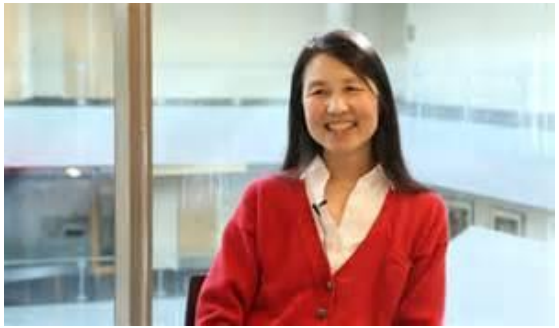
- What objectives should guide the plan?
- What capabilities should the research aim to achieve?

Tara Whalen / Google

Google

- applying design thinking and value-centric design methods to privacy
- exploring how organizational behavior research could be applied to privacy decision-making processes

Jeannette Wing / Microsoft (and CMU)



- Foundations of privacy
  - Models, logics, and concepts, e.g., inverse privacy
- Privacy compliance at scale
  - How do we ensure institutions abide by privacy policies? (Oakland 2014)
- Security and privacy
  - Secure computation to ensure data confidentiality

Microsoft

CARNEGIE MELLON UNIVERSITY PITTSBURGH PENNSYLVANIA 1900

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 we better address these values in design processes?

CCC
Computing Community Consortium
Catalyst

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

Scott Young / Kaiser Permanente

How can we make data and information available to individuals to allow for co-design and co-production of health and healthcare?

KAISER PERMANENTE
care management | institute

CCC
Computing Community Consortium
Catalyst