# PRIVACY BY DESIGN WORKSHOPS AND NATIONAL PRIVACY RESEARCH STRATEGY COMMUNITY INPUT

*Ann Drobnis*
*Director, CCC*
*adrobnis@cra.org*

CCC
Computing Community Consortium
Catalyst

# THE COMPUTING COMMUNITY CONSORTIUM

The **mission** of Computing Research Association's Computing Community Consortium (CCC) is to:

**catalyze** the computing research community and
**enable** the pursuit of innovative, high-impact research.

CCC conducts activities that

**strengthen** the research community,
**articulate** compelling **research visions**, and
**align** those visions with pressing **national and global challenges**.

CCC **communicates** the importance of those visions to **policymakers**, **government** and **industry stakeholders**, the **public**, and the **research community** itself.

CCC
Computing Community Consortium
Catalyst

# THE CCC COUNCIL – EXECUTIVE COMMITTEE

- Greg Hager, Johns Hopkins Univ. (Chair)
- Beth Mynatt, Georgia Tech (Vice Chair)
- Susan Graham, UC Berkeley (Past Chair)
- Bob Sproull, formerly Sun Labs Oracle
- Liz Bradley, University of Colorado, Boulder
- Mark Hill, University of Wisconsin, Madison
- Ann Drobnis, Director
- Andy Bernat, CRA Executive Director

* Executive Committee
** 1 year leave

CCC
Computing Community Consortium
Catalyst

# THE CCC COUNCIL








- Terms ending June 2017
  - Lorenzo Alvisi, UT Austin
  - Vasant Honavar, Penn State
  - Jennifer Rexford, Princeton
  - Debra Richardson, UC Irvine
  - Klara Nahrstedt, UIUC
  - Ben Zorn, Microsoft Research
- Terms ending June 2016
  - Randy Bryant, CMU**
  - Limor Fix, formerly Intel
  - Tal Rabin, IBM
  - Daniela Rus, MIT
  - Ross Whitaker, Univ. Utah
- Terms ending June 2015
  - Sue Davidson, Univ. Pennsylvania
  - Joe Evans, Univ. Kansas
  - Ran Libeskind-Hadas, Harvey Mudd College
  - Shashi Shekhar, Univ. Minnesota







** 1 year leave

CCC
Computing Community Consortium
Catalyst

# HOW DO WE DO IT?

**Community-initiated visioning:**

- Workshops to discuss “out-of-the-box” ideas
- Blue Sky Ideas tracks at conferences

**Outreach to White House, funding agencies:**

- Outputs of visioning activities
- Short reports to inform policy makers
- Task Forces – Health IT, Computing in the Physical World, Manufacturing, Big Data, Industry, High Performance Computing, Education


**Communicating CS Research:**

- CCC Blog [http://cccblog.org/]
- Computing Research in Action Video Series
- Great Innovative Ideas
- “The Impact of NITRD” symposium

**Nurturing the next generation of leaders:**

- Computing Innovation Fellows Project
- Leadership in Science Policy Institute
- Postdoc Best Practices Program

CCC
Computing Community Consortium
Catalyst

# WHAT DISTINGUISHES CCC?

**Proactive, rapid response**

- Identify, plan, and execute in a matter of weeks to months

**Community-based**

- Diverse Council with representation from varied academic institutions and industry
- Find and foster ideas from germination to fruition and beyond

**Leadership incubator**

- Everyone is expected to do something!

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN

## THE FUTURE OF PRIVACY CANNOT BE ASSURED SOLELY BY COMPLIANCE WITH LEGISLATION AND REGULATORY FRAMEWORKS; PRIVACY ASSURANCE MUST IDEALLY BECOME AN ORGANIZATION'S DEFAULT MODE OF OPERATION[1]

Workshop Series proposed in 2014 by:

- Deirdre Mulligan (Chair), UC Berkeley
- Annie Anton, Georgia Tech
- Ken Bamberger, UC Berkeley
- Travis Breaux, Carnegie Mellon
- Nathan Good, Good Research
- Peter Swire, Georgia Tech
- Ira Rubinstein, New York University
- Helen Nissenbaum, New York University

Additional Members of Organizing Committee:

- Fred Schneider, Cornell University
- Susan Landau, WPI
- Susan Graham, UC Berkeley / CCC

[1] https://www.privacybydesign.ca/index.php/about-pbd/applications/

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## 4 WORKSHOPS

State of Research and Practice
- February, 2015
- UC, Berkeley

Privacy Enabling Design
- May, 2015
- Georgia Tech

Engineering Privacy
- August, 2015
- Carnegie Mellon University

Regulation as Catalyst
- Fall, 2015
- Georgetown University

http://cra.org/ccc/visioning/visioning-activities/privacy-by-design

# PRIVACY BY DESIGN
## WORKSHOP 1: STATE OF RESEARCH AND PRACTICE

49 Participants

- 23 from academia
- 11 from industry
- 6 from civil association
- 9 from government (state and federal)

Key Insights

- Privacy is an "essentially contested" concept
- In the US, there are many sources of privacy law, which reflects different conceptualizations of privacy
- Research in CS has produced a large variety of solutions for privacy, which operate at different levels of use and reflect different concepts of privacy
- Standards setting bodies have begun engaging more with privacy
- Engaging academics and practitioners from multiple disciplines and sectors is essential to develop a privacy research strategy that addresses the complexity of privacy in practice

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## WORKSHOP 1: STATE OF RESEARCH AND PRACTICE

Privacy Programs in the Wild / Reports from the Field

- Industry:
  - Implements cross-functional privacy teams
  - Engages in multiple types of research to better understand privacy
  - Develops educational tools for end users
  - Agile development process is a double-edge sword
  - Creates privacy resources within an organization
  - Develops access and use-based controls for data to protect privacy
- Government Agencies
  - Explores science of privacy, in particular, mathematical approaches
  - Implements technical standards for the protection of information
  - Sets controls on use of data through internal standards

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN

## WORKSHOP 1: STATE OF RESEARCH AND PRACTICE

Key Questions raised at the workshop:

1. How can privacy be operationalized in engineering and design?
2. What are the drivers of implementing privacy in the wild?
   - How can we get tools and insights from computer science privacy research more widely adopted?
3. How to know how long data should be kept?
4. What is the life cycle of data, with respect to privacy?
5. Who is responsible for privacy within an organization?
6. What new tools are needed for privacy conversations and implementations across the legal, ethical, and technical domains?
7. What research areas impact privacy by design?

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## WORKSHOP 1: STATE OF RESEARCH AND PRACTICE

Barriers

- Lack of common tools and nomenclature to identify and discuss privacy concepts
- A gap between research and operationalization or implementation of privacy tools
- Privacy is not only a data or system requirement, but also a business requirement
- Ambiguity about where privacy expertise should be found in an organization
- The challenge of bringing together multidisciplinary researchers

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## WORKSHOP 2: PRIVACY ENABLING DESIGN

49 Participants

- 27 from academia
- 18 from industry
- 4 from government

Key Insights

- Designers lack adequate heuristics for designing applications
- Users want control of their privacy for different relationships
- Designs likely to engender trust should be preferred
- "Encroaching Externalities" limit the freedom to support privacy in system designs
- Users trust themselves most to protect their own privacy
- Even non-traditional interfaces should support privacy because they could become widespread
- There is a lack of economic incentive for designing with privacy

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN

## WORKSHOP 2: PRIVACY ENABLING DESIGN

Examples of How Privacy Principles have been Implemented in:

- Healthcare:
  - Companies trade privacy protections for user satisfaction
  - Lack of trust leads to user drop-off
  - Engaging with clients on topic of privacy is difficult
- Web Browsers:
  - Users have a strong mental model of advertisers and 3rd party tracking online activity to target ads
  - Tracker blocking has hard to quantify benefits, but easily identified pitfalls
  - Privacy tutorials made users more aware of tracking
- Designers:
  - Privacy is usually not their top priority
  - Privacy is pitched to them
  - Lack of Expertise in privacy
  - Lack of Resources for privacy

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## WORKSHOP 2: PRIVACY ENABLING DESIGN

Key Research Statements / Topics

1. In the HCI tradition, we should conduct more research on the mental models that users have in connection with privacy, in a variety of settings for collecting user data.
2. People act with an understood audience. Research should focus on context – the audience with whom the user is explicitly or implicitly communicating.
3. Privacy by Design is pervasively multi-disciplinary. Research should be done on how best to determine (1) when in the process designers should get involved to achieve privacy and other goals? (2) what team structure works best, in what contexts?
4. There is tension between the complexity of data collection and use. Research on Privacy by Design should more systematically address this tension.
5. Research should address how to design for privacy, understanding that it is often a third- or fourth-level concern for users.
6. We need building blocks closer to the way people think about design.

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## WORKSHOP 3: ENGINEERING PRIVACY

Cross Cutting Themes

- Privacy review of products designed without privacy in mind vs. starting with privacy requirements to drive design early
- The effect of different business models on privacy
- The effect of organization size: small companies vs. startups vs. end-user programmers vs. large companies
- Relevant industry practices suitable in light of cost, performance, production schedule, and other design pressures

CCC
Computing Community Consortium
Catalyst

# PRIVACY BY DESIGN
## WORKSHOP 4: REGULATION AS A CATALYST

Goals:

- Examine how existing regulatory models, along with other factors, shape organizations' understanding of privacy problems, approaches, and solutions
- Consider how well regulatory models respond to privacy-by-design challenges, and identify open research questions.
- Gain understanding of the forces that drive the choice of methods, tools, and approaches
- Identify open research questions about the relationship between regulatory form and other external and internal features of the privacy field, and the expression of privacy in firm practice

CCC
Computing Community Consortium
Catalyst

# TOWARDS A PRIVACY RESEARCH ROADMAP FOR THE COMPUTING COMMUNITY

*Editors of the report:*
*Lorrie Cranor, Tal Rabin,*
*Vitaly Shmatikov, Salil Vadhan,*
*Danny Weitzner*

CCC
Computing Community Consortium
Catalyst

# FOCUS OF REPORT

- Privacy concerns raised by the:
  - Collection
  - Sharing
  - Analysis
  - Use

  of personal data in information systems

http://cra.org/ccc/files/docs/white-papers/CCC%20National%20Privacy%20Research%20Strategy.pdf

CCC
Computing Community Consortium
Catalyst

# WHY IS PROVIDING PRIVACY DIFFICULT?

Tension between:

- Advances in computing and communication technology are bringing many benefits to society in areas such as: health care, transportation, national security, commerce
- Benefits involve use of sensitive personal data

Goal of research to balance the benefits with privacy rights and requirements of individuals

CCC
Computing Community Consortium
Catalyst

# DESIRED CAPABILITIES TO SUPPORT PRIVACY

- Measurement
  *be able to precisely define various privacy objectives and be able to measure the extent to which a system meet those objectives*
- Social Science
  *understand the privacy needs of humans who use information systems, the institutional dynamics of the organizations that use personal data, and how larger social and economic forces relate to privacy.*
- Security
  *understand the relationship between security and privacy, and be able to secure information systems from unauthorized access to personal info.*
- Engineering
  *be able to design and build information systems that meet privacy objectives while allowing us to enjoy the beneficial uses of personal data.*
- Policy

  *be able to design laws, regulations, policies, and best practices regarding the use of personal data in information systems in a way that recognizes the unique capabilities and limitations of information systems.*

CCC
Computing Community Consortium
Catalyst

# HIGH-LEVEL RECOMMENDATIONS

- A rigorous science of privacy:
  - To define and measure the privacy of information systems
  - Major challenge: not agreed upon definition of privacy (– can there be one?)
  - When examining a problem:
    - Precisely define the objective
    - Evaluate it with scientific rigor to prove whether the objective is met
- Support the stages and dimensions of privacy research:
  - Foundational work that aims to understand phenomena and range of technological possibilities and limitations
  - Applied research that is directed at specific privacy objectives
  - Translational work that seeks practical impact on particular application domains.

CCC
Computing Community Consortium
Catalyst

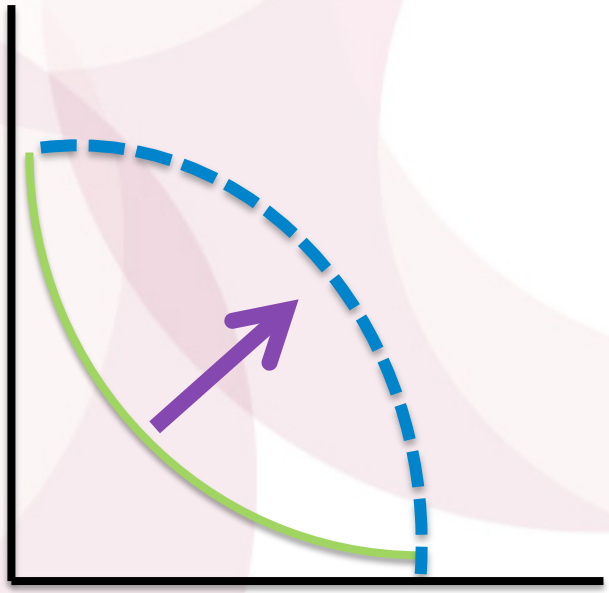
# HIGH-LEVEL RECOMMENDATIONS (CON'T)

- Priority to enable interdisciplinary research strategies:
  - Requires a combined understanding of computing technology, information, human behavior, and governance mechanisms
- Technology and policy dialogue:
  - Conversation that enables regulators, lawmakers, standards creators and system builders
    - To understand what is and is not possible to achieve with technology, and
    - Be informed of what should be integral privacy properties of systems, procedures and processes

CCC
Computing Community Consortium
Catalyst

# AGENDA SEEKS TO LEAD TO A STATE WHERE

Systems can enable both privacy and the benefits of use of data, showing we can achieve better tradeoff than we currently have




Privacy engineering

Privacy by-design

# CCC: CATALYZING AND ENABLING COMPUTING RESEARCH

*cra.org/ccc*

*cccblog.org*

CCC
Computing Community Consortium
Catalyst