Bridging the Gap between Privacy by Design and Privacy in Practice

Luke Stark
Department of Media, Culture, and Communication
New York University
New York, NY 10003
luke.stark@nyu.edu

Jen King
School of Information
University of California Berkeley
Berkeley, CA 94720-4600
jenking@ischool.berkeley.edu

Xinru Page
Department of Computer Information Systems
Bentley University
Waltham, MA 02452
xpage@bentley.edu

Airi Lampinen
Mobile Life Centre
Stockholm University
Kista, Sweden
airi.lampinen@iki.fi

Jessica Vitak
College of Information Studies
University of Maryland
College Park, MD 20742
jvitak@umd.edu

Pamela Wisniewski
College of Engineering and Computer Science
University of Central Florida
Orlando, FL 32816
pamwis@ucf.edu

Tara Whalen
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
tjwhalen@google.com

Nathan Good
Good Research
828 San Pablo Avenue #218
Albany, CA 94706
nathan@goodresearch.com

CHI'16 Extended Abstracts, May 07-12, 2016, San Jose, CA, USA ACM 978-1-4503-4082-3/16/05.
http://dx.doi.org/10.1145/2851581.2856503

Abstract
While there has been considerable academic work over the past decade on preserving and enhancing digital privacy, little of this scholarship has influenced practitioners in design or industry. By bringing together leading privacy academics and commercial stakeholders, this workshop builds on previous gatherings at ACM conferences and in the broader privacy community. Workshop attendees will address the 'privacy by design' implementation problem, and will work together to identify actionable methods and design heuristics for closing the gap between academic research and industry solutions for protecting user privacy in the design of systems, digital products and services.

Author Keywords
Privacy; privacy by design; design practice; guidelines; heuristics

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous; K.4.1. Computers and society: Public Policy Issues (Privacy)

Introduction

Much of the effort around translating privacy insights from academia into practical technical and design strategies has focused on the idea of "*privacy by design*" (PbD), a set of principles initially promoted by former Ontario (Canada) privacy commissioner Ann Cavoukian that seek to integrate the value of privacy into the technical design process from start to finish [4,10,26]. Despite ongoing PbD work on data protection and engineering requirements, there has been little agreement as to how to translate these principles into a set of guidelines or practices relevant and useful to design practitioners. As such, the gap between the academic work on privacy and practitioner norms is wide, and there have been few attempts to translate these ideas in a systematic way.

This intensive one-day workshop seeks to reinvigorate conversations in the CHI community around privacy and design to refocus our attention on developing methods to systematically incorporate privacy into design processes. The workshop will bring together leading privacy researchers in academia and industry to unpack the barriers preventing PbD concepts from being implemented in design. Outcomes of this workshop will include a) revising the existing PbD principles to better address the challenges that have prevented their adoption, b) moving beyond previous workshops at CHI and CSCW by focusing specifically on concrete strategies for bridging the divide between privacy research, design, and implementation, and c) strengthening academic-industry partnerships to enable new research opportunities that span fields.

Background: A Disconnect between Privacy Discourse and Application

There has been no shortage of scholarly work within computer science in general, and human-computer interaction in particular, on digital and networked privacy [1,3,6,8,21]. Meanwhile, ongoing privacy-related controversies, such as the revelations of Edward Snowden and the corporate policies of companies like Google and Facebook, have kept digital privacy firmly on the public agenda [2,7]. Despite a plethora of research and public attention on privacy's broader social and political benefits [6], the vast majority of scholarship on digital privacy has failed to have a major impact on product and software development or change the consumer experience toward one of privacy protection [12,20]. Simply put, privacy may be a hot topic at academic conferences and in trade magazines, yet *solutions* for privacy's practical preservation and protection are sorely lacking. The disconnect between academic research in this area and the work of practitioners suggests a need for collaborative conversations between these groups to help ensure insights and opportunities to improve networked privacy outcomes identified in our research to come to practical fruition.

Privacy by Design

PbD has been at the forefront of privacy discourse that has attempted to bring together academic research,

government regulation, and industry engagement and design. It broadly addresses policy, legal compliance, and data protection, yet designers have generally not been part of the conversation [14]. In 2012, the Federal Trade Commission, in their landmark report on consumer privacy, urged companies to actively incorporate PbD, but they provided no substantive guidance on how to proceed, particularly with respect to design [4]. Related iterations, such as the promulgation of privacy-enhancing or privacy-preserving technologies (PETs and PPTs) have been met with similarly mixed design successes, and have not seen widespread adoption [5,15].

Due to the limited success of recent PbD efforts, the Community Computing Consortium (CCC) has organized a series of workshops in 2015 and 2016 to engage a broad audience and determine why PbD has faced barriers to implementation. This series included one workshop, "Privacy Enabling Design," devoted to opening up the "design" challenges of PbD [27]. We outline some of these challenges below and argue that the CHI community is uniquely positioned to address these design-focused challenges through a workshop focused explicitly on solutions aimed at bridging the gap between PbD and privacy practice.

Privacy Challenges: New Technology, Old Problem

Pace of Change and Lack of Transparency

Design challenges take place at various points in the "privacy interface" – not just where users engage with a technology, but also where designers and technologists envision, create, and build systems with privacy in (or not in) mind. Challenges faced by designers, technologists, and scholars working to integrate digital privacy protections into technological designs include the pace of technological change and the opacity of data flows on the part of large institutional actors. While algorithmic transparency (the notion that outside actors should be able to assess the ways information is processed and correlated in big data analyses) has generated discussion in recent years [13], a lack of transparency has been identified as one of the key challenges of PbD.

User Context and Design Modularity

While designers have found it challenging to capture the nuance demanded by privacy, users desire even more nuance, contextual subtlety, and modularity within the privacy interfaces of everyday digital products and services [19,23]. Moreover, users' mental models of privacy also shape individual and group behavior around privacy in unexpected and often underappreciated ways. User mental models that understand privacy as control [24], privacy as contextual integrity [17], privacy as an emotional variable [11,12,22], privacy as a commodity [18], or privacy as a universal right [25], are just a few possible facets structuring the so-called "privacy gap."

Designing for Trust

Users lose trust in the privacy protections of a product or system if they experience context collapse, or feel as if the system is collecting data inappropriately or unnecessarily [9]. Designing for trust could potentially mitigate this problem, invoking transparency, user choice, and active engagement with the product or service, yet also leaving designers and users vulnerable to further breaches of trust, both real and perceived. This tension underlies PbD and highlights the need for ethics to be included in these discussions to avoid

deceptive designs that work to build trust while masking unethical business practices.

Workshop Theme: Beyond Privacy by/and/through Design

Our goal with this workshop is to address these privacy design challenges in a way that bridges the divide between privacy discourse and practice. This workshop will capitalize on CHI's diverse attendees to reorient and ignite the privacy by design agenda and formulate a set of workable strategies and methods for viable privacy design practices. CHI presents an excellent opportunity to capitalize on the wealth of attendee expertise to further this mission, through a conversation and collaboration between academics and practitioners around workable design solutions for protecting, fostering, or encouraging privacy as a human value within human-computer interaction design.

Previous workshops, paper sessions, and panels at CHI and CSCW have addressed a variety of challenges in networked privacy scholarship: How to negotiate conflicting interests (citizens, businesses, governments), and how to improve the design of privacy policies and technical tools to support privacy decisions (CHI 2011); how to study collective privacy practices and design for them (CSCW 2011); how to make privacy important to both the architect and the user (CSCW 2012); how to measure privacy in networked, interpersonal settings (CSCW 2013); and how to provide users with the knowledge, awareness, and visibility of their social footprint at the time they make decisions, and thus provide real agency—not just false choices (CSCW 2015).[1] This workshop follows up on these themes by foregrounding the challenges of advocating for PbD in commercial contexts, and brings together designers and technologists with PbD experts in academia to break down barriers to PbD's widespread adoption by industry.

Workshop Structure and Planned Activities

We propose a one-day workshop, on Saturday May 7th, including up to 25 participants from academia, industry, and the public sector. The overall workshop structure will be roughly as follows:

- **Convene and Introductions (45 minutes)**
  The workshop organizers will set out the workshop's agenda and goals. They will moderate a lightning round of talks introducing participants, positions, and thoughts stemming from position papers and online pre-workshop discussions.
- **Large Group Discussion: Privacy Mental Models (30 minutes)**
  Participants will discuss the mental models that users have in connection with privacy in a variety of settings for collecting user data, including a focus on context and the audience with whom the user is explicitly or implicitly communicating.
- **Break (15 minutes)**
- **Break-out groups: Heuristics Synthesis (60 minutes)**
  Having identified a core set of mental models to work with, participants will collaborate in small groups to translate privacy by design principles and

[1] Please visit networkedprivacy.com for details about these past workshops.

privacy findings from research into concrete design recommendations. They will detail existing privacy design heuristics, produce templates to help practitioners apply these heuristics, and make notes on the process for this kind of translation.

- **Lunch (60 minutes)** ***(to be potentially combined with the keynote)***
- **Keynote (60 minutes)**
  Privacy scholar Deirdre Mulligan, Associate Professor at the School of Information at UC Berkeley and lead organizer of the CCC PbD workshops, will give a keynote address followed by a Q & A session.
- **Discussion and Exploration (30 minutes)**
  Small groups will present their templates to the whole group and get feedback. The overall goal is to produce three or four possible design frameworks, and explore ways to make PbD more accessible and useful to working designers.
- **Break (30 minutes)**
- **Activity: Divide and Conquer (60 minutes)**
  In pairs, participants will work through design scenarios using the morning's heuristics, to evaluate the usefulness of those guidelines and refine them. In mobilizing design heuristics build on principles such as transparency or viscerality, participants will strive to produce designs closer to the way people actually think, and feel, about privacy.
- **Reporting Back and Troubleshooting (60 minutes)**
  Participants will rearrange into larger groups and present their ideas to each other – these groups will work to identify how to bridge problem areas or otherwise strengthen both the guiding principles and the resulting design ideas.
- **Report and Synthesize (30 minutes)**
  The workshop will conclude with a group discussion of opportunities for further collaboration between academia and industry around PbD implementation, and the role of policy and regulation in supporting PbD.

Deliverables for the workshop

- Connecting academic and industry researchers studying privacy in HCI.
- Facilitating and scaffolding collaborative work across disciplines by devising ways to bridge the gap between social science, information science, and computer science in privacy design.
- Identifying and acting on areas in HCI particularly amenable to new privacy by design ideas;
- Prototyping potential solutions.
- Assessing what role policy, law, and regulation might need to play in supporting privacy by design solutions [16].
- Producing a set of templates for practitioners that assist them in translating PbD principles into concrete design.

Organizers

Luke Stark (New York University) is completing his doctorate in the Department of Media, Culture, and Communication at NYU. His research examines privacy, emotion and digital media, quantification and self-tracking, and ethics and values in technological design.

Jennifer King (UC Berkeley) is completing her doctorate at the School of Information at UC Berkeley. Her research focuses on the intersection of information privacy, social computing, and public policy.

Program Committee

- Bettina Berendt, KU Leuven
- Michelle Mazurek, University of Maryland
- Vance Ricks, Guilford College
- Jessica Staddon, NC State
- Nazanin Andalibi, Drexel University
- Lorraine Kisselburgh, Purdue University
- Solon Barocas, Princeton
- Priya Kumar, Ranking Digital Rights
- Ralf De Wolf, Ghent University
- Roberto Hoyle, Oberlin College
- Jose M. Such, Lancaster University
- Darren Stevenson, University of Michigan & Stanford
- Heather Lipford, UNC Charlotte
- Bart Knijnenburg, Clemson University
- Coye Cheshire, UC Berkeley
- Kelly Caine, Clemson University
- Deirdre Mulligan, UC-Berkeley
- Yang Wang, Syracuse University
- Seda Gurses, Princeton University
- Stacy Blasiola, University of Illinois at Chicago
- Michael Zimmer, UW-Milwaukee
- Hamed Haddadi, Queen Mary University of London
- Tristan Henderson, University of St. Andrews
- Luke Hutton, University of St. Andrews

Xinru Page (PhD, UC Irvine) is an Assistant Professor of Computer Information Systems at Bentley University. Her research explores technology adoption and non use, social media, individual traits, and, of course, privacy.

Airi Lampinen (PhD, University of Helsinki) is a Postdoctoral Researcher at Mobile Life Centre, Stockholm University in Sweden. Her research focuses on interpersonal boundary regulation in social network services and in the so-called sharing economy.

Jessica Vitak (PhD, Michigan State) is an assistant professor at the University of Maryland. Her research examines the social processes underlying privacy negotiations and the impact of context collapse in networked spaces.

Pamela Wisniewski (PhD, UNC Charlotte) is an Assistant Professor at the University of Central Florida in the College of Engineering and Computer Science. Her research interests are situated at the juxtaposition of Social Computing and Privacy.

Tara Whalen (PhD, Dalhousie) is a Staff Privacy Analyst at Google and a Non-Resident Fellow at the Stanford Center for Internet and Society. Her research interests include usable security and privacy, as well as technology policy.

Nathan Good (PhD, UC Berkeley) is Principal of Good Research and Faculty in UC Berkeley's Master of Data Science Program. He specializes in user experience research, modeling and investigating behavior where design overlaps with data.

Pre-Workshop Plans

Participants will be recruited from the CHI community, from attendees of previous CHI and CSCW privacy workshops, and from the extended research networks of the workshop organizers, who will work actively to ensure a balanced mix of participants from academia, design practice, industry, and the public sector. We will advertise the workshop on relevant listservs and through social media, with the help of the workshop's program committee (see list on the left).

Workshop Website

We have space for this workshop at networkedprivacy2016.wordpress.com, and have linked it to our community's permanent website, networkedprivacy.com. Detailed information will be made available on the workshop website.

Post-Workshop Plans

The workshop will facilitate collaborations that address the three major challenges noted above: translating privacy heuristically, designing modularity for user context, and designing for trust rigorously and honestly. Specifically, we aim to produce a white paper detailing recommendations stemming from the workshop, and explore the possibility of a special journal issue to elaborate on the workshop's outcomes. In addition, we will work to initiate a joint effort to produce a collection of privacy heuristics and design principles, similar to the ongoing work of PrivacyPatterns.org. We will make resulting materials available through the workshop website and networkedprivacy.com.

Call for Participation

This intensive one-day workshop aims to reinvigorate conversations in the CHI community around privacy and design by refocusing attention on developing methods to systematically incorporate privacy into design processes. The workshop will bring together leading privacy researchers in academia and industry to unpack the barriers preventing "privacy by design" (PbD) concepts from being implemented in design contexts. Through this workshop, participants will formulate privacy heuristics focused explicitly on PbD to better address the challenges that have prevented their adoption by practitioners; formulate concrete strategies for bridging the divide between privacy research, design, and implementation; build and strengthen academic-industry partnerships to enable new research opportunities that span these arenas.

Potential participants are asked to submit 2-4 page position papers in CHI extended abstracts format that address the workshop themes and highlighted topics provided in the call. We encourage the submitters to make suggestions about relevant design guidelines, heuristics, or existing research in their papers for discussion at the workshop. Submitters should also review the report from the CCC Privacy Enabling Design workshop (http://cra.org/ccc/events/pbd-privacy-enabling-design/) for background on the ongoing discussion in this area. To encourage broader participation, we also encourage designers and other industry practitioners to submit alternative material of rough equivalence (e.g., a design portfolio, white paper, or similar). Submissions will be accepted based on the relevance and development of their chosen topic, as well as their potential to contribute to the workshop discussions and goals. Papers will be peer-reviewed by the workshop's Program Committee.

Please submit position papers and other materials at networkedprivacy2016.wordpress.com. Please note that at least one author of each accepted position paper must attend the workshop and that all participants must register for both the workshop and for at least one day of the conference.

References

[1] Acquisti, A., Brandimarte, L., and Loewenstein, G. Privacy and human behavior in the age of information. *Science 347*, 6221 (2015), 509–514.

[2] Aguirre, A. Laura Poitras on Filming Edward Snowden and Her New Documentary About Him, *Citizenfour*. *Vogue*, 2014. http://www.vogue.com/2865709/laura-poitras-edward-snowden-documentary-citzenfour/.

[3] Braman, S. Privacy by design: Networked computing, 1969−1979. *New Media & Society 0*, 0 (2011), 1–18.

[4] Bureau of Consumer Protection. *Protecting Consumer Privacy in an Era of Rapid Change*. Federal Trade Commission, 2010.

[5] Burkert, H. Privacy-Enhancing Technologies: Typology, Critique, Vision. In P.E. Agre and M. Rotenberg, eds., *Technology and Privacy: The New Landscape*. The MIT Press, Cambridge, MA, 1997, 125–142.

[6] Cohen, J.E. What Privacy Is For. *Harvard Law Review 126*, (2013), 1904–1933.

[7] Drum, K. The Google Panopticon Is Set to Become Even More Omniscient. *Mother Jones*, 2013. http://www.motherjones.com/kevin-drum/2013/09/google-panopticon.html.

[8] Dwork, C. and Mulligan, D.K. It‟s Not Privacy,

and It"s Not Fair. *Stanford Law Review Online 66*, (2013), 35–40.

[9] Grodzinsky, F.S. and Tavani, H.T. Applying the "Contextual Integrity" Model of Privacy to Personal Blogs in the Blogosphere. *International Journal of Internet Research Ethics 3*, (2010), 38–47.

[10] Hoepman, J.-H. Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam and T. Sans, eds., *ICT Systems Security and Privacy Protection*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, 446–459.

[11] Li, H., Sarathy, R., and Xu, H. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems 51*, 3 (2011), 434–445.

[12] Li, H., Sarathy, R., and Zhang, J. The Role of Emotions in Shaping Consumers' Privacy Beliefs about Unfamiliar Online Vendors. *Journal of Information Privacy & Security 4*, 3 (2008), 36–62.

[13] Lohr, S. Workplace Surveillance and the "Transparency Paradox." *The New York Times*, 2014. http://bits.blogs.nytimes.com/2014/06/21/workplace-surveillance-and-the-transparency-paradox/?_r=0.

[14] Mulligan, D.K. and King, J. Bridging The Gap Between Privacy And Design. *University of Pennsylvania Journal of Constitutional Law 14*, 4 (2012), 989–1034.

[15] Nippert-Eng, C. Privacy in the United States: Some Implications for Design. *International Journal of Design 1*, 2 (2007), 1–11.

[16] Nissenbaum, H. From Preemption to Circumvention. *Berkeley Technology Law Journal 26*, 3 (2011), 1367–1386.

[17] Nissenbaum, H. A Contextual Approach to Privacy Online. *Daedalus 140*, 4 (2011), 32–48.

[18] Posner, R.A. An Economic Theory of Privacy. *Regulation 2*, 3 (1978), 19–26.

[19] Rainie, L., Kiesler, S., Kang, R., and Madden, M. *Anonymity, Privacy, and Security Online*. Pew Research Center's Internet & American Life Project, Washington, D.C., 2013.

[20] Simpson, J.M. Google Tells Court You Cannot Expect Privacy When Sending Messages to Gmail. *Consumer Watchdog*, 2013, 1–2. http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy.html.

[21] Solove, D.J. A Taxonomy of Privacy. *University of Pennsylvania Law Review 154*, 3 (2006), 477–564.

[22] Stark, L. The Emotional Context of Information Privacy. *The Information Society 32*, 1 (2016).

[23] Strandburg, K.J. Social Norms, Self Control, and Privacy in the Online World. 2005, 1–24.

[24] Tene, O. and Polonetsky, J. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property 11*, 5 (2013), 239–273.

[25] Westin, A.F. Social and Political Dimensions of Privacy. *Journal of Social Issues 59*, 2 (2003), 431–453.

[26] *Privacy by Design in the Age of Big Data*. 2012.

[27] Privacy by Design. *Computing Community Consortium*. http://cra.org/ccc/visioning/visioning-activities/2015-activities/privacy-by-design/.