Using A Multi-Dimensional Analytic for Privacy Theory, Design, and Analysis

Richmond Y. Wong
UC Berkeley
School of Information
Berkeley, CA 94720, USA
richmond@ischool.berkeley.edu

Deirdre K. Mulligan
UC Berkeley
School of Information
Berkeley, CA 94720, USA
dmulligan@berkeley.edu

Abstract
Privacy is a fluid, ongoing, and situated concept that takes on many theoretical forms. We describe a tool, a multi-dimensional privacy analytic created by Mulligan, Koopman, and Doty [8], which helps map multiple dimensions and concepts of privacy that can be applied in specific situations when privacy arises. We then provide three examples of CSCW, HCI, and design work where we have used the analytic as a way to explore and grapple with multiple theoretical dimensions of privacy.

Author Keywords
Privacy analytic; privacy theory; design

ACM Classification Keywords
K.4.1. Public Policy Issues: Privacy

Introduction
Privacy scholars have attempted to define privacy in a wide range of ways, such as conceptualizing privacy as having control over personal information, as protections from government searches and seizures, as the protection of physical spaces and bodies, as freedom of thought, and more. However, no one definition applies well to every situation. Reacting to the plethora of definitions for privacy, privacy scholar Dan Solove has written that privacy as "a concept in disarray. Nobody can articulate what it means" [12].

Shifting from searching for grand theories of privacy, recent work has tried to acknowledge the multiplicity of conceptions of privacy, such as Solove's work articulating a taxonomy of types of harms that occur when privacy is violated [14], and his work articulating at least six different conceptions of privacy [13]. Nissenbaum's theory of contextual integrity formulates how privacy is dependent on contextual and situational norms, rather than a universal property, and that a violation of privacy is caused by a violation in norms in a specific context [9]. Beyond privacy, recent values in design work in CSCW and HCI has begun to view values more broadly (including privacy) as instantiated through specific situated practices [2,5,7,11], rather than as universal and stable phenomena, or as Houston et al. describe, "a more fluid and emergent model that treats value as an active and ongoing *process*" [5]. Thus it becomes important to surface, analyze, discuss, and design for specific conceptions of privacy might be at play in a given design, situation, or practice.

Limits of Impact Assessments

While valuable, tools like Privacy Impact Assessments (PIA) run the risk of enshrining the wrong conceptions of privacy. In 2008 the U.S. Transportation Security Agency (TSA) used a PIA to analyze the potential impact of airport security whole body imaging systems. Using the FIPs, the PIA conceptualized privacy as control over personal data. The assessment found that while the system captured naked-like images of persons' bodies, the images would be deleted and faces were blurred so that images were not personally identifiable [15]. Nevertheless, many people cited privacy concerns about increased visibility and exposure to the TSA. Simply put, the privacy invasion arose from TSA agents *viewing images of naked bodies*, not from *identifying individuals* in the images. The PIA's focus on privacy risks from data collection and identification did not match people's concerns of closed-booth ogling by TSA agents, leading to expensive redesigns.

While a useful range of privacy engineering and compliance approaches have been developed, many attempt to translate definitions or theories of privacy into implementable requirements or into privacy impact assessments [1,4]. However, these top-down approaches assume that the "correct" conception of privacy is known at the outset of a design process, and may enshrine a specific concept of privacy that is not applicable in all cases [4] (see sidebar). In many situations, designers and engineers may not know what conceptions of privacy might be at play at the outset. A more open ended theoretical framework can be used with bottom-up approaches to surface what conceptions of privacy might be at play in a given situation.

A Multidimensional Privacy Analytic

Building on a contextual and bottom-up approach to privacy, Mulligan, Koopman, and Doty put forth that privacy is an "essentially contested concept"; that rather than seeing multiple conceptions of privacy as evidence of "disarray", they argue that "contests about privacy and the ambiguity of meaning that they simultaneously beget are battles for its core and essential to its functioning." [8:3]. Rather than argue for a particular conception of privacy, they propose an analytic for mapping multiple dimensions privacy that can be applied in specific situations when privacy arises, to give a shared way to articulate what aspects of privacy are at play. This analytic consists of five meta-dimensions of privacy [8:11]:

1. **Theory** (why there should be privacy). For instance, privacy might be thought of as control over personal information, or to provide dignity, or to provide individual liberty. Mulligan et al. also suggest identifying what is seen in contrast to or opposite of privacy in the situation being analyzed; for example being public, open, or transparent.
2. **Protection** (what and who is protected by privacy). Examples of things that privacy might protect include personal information, specific data types, one's body or likeness, or physical private spaces. Who gets protected might include individuals, groups, or roles such as: myself, my child, users, teens, students, or patients.
3. **Harm** (actions that violate privacy, who violates them, and from whom privacy was expected). Examples of actions that might violate privacy include Solove's taxonomy of harms [14], including data collection, processing, dissemination, and invasion. Who violates privacy and from whom privacy was expected may not necessarily be the same. For instance, if a company releases customers' credit card information, the action causing the harm is the dissemination or breach; the company releasing the information is the actor that violated privacy; while credit card thieves are from whom privacy was expected.
4. **Provision** (what provides privacy protection). This includes asking how is privacy provided, and who is supposed to provide privacy. For instance, is privacy protected by legal regulations, technical design, social norms, etc.? Does responsibility for providing privacy lie with governments, technology producers, third party groups, individual responsibility, etc.?
5. **Scope** (how broadly does privacy apply). This includes thinking about the social boundaries and context (e.g. a hospital, a workplace, a specific country); the temporal scale (e.g. does privacy apply for a few minutes, for years, or forever?);

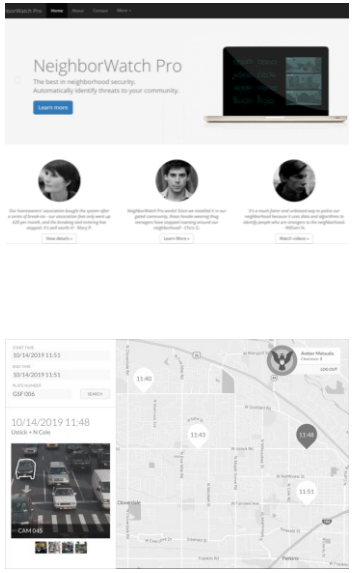

Figure 1. Two conceptual designs using the same imagined camera analytic system. The top version is advertised as a community neighborhood surveillance product; the bottom version is advertised as a criminal tracking product for police use. Using the analytic, we find that the conceptions of privacy at play in these two designs differ.

and how often (e.g. does privacy always apply, or a case by case basis?)

Mulligan et al. suggest that the analytic can be used to generate a more useful conversation about what privacy means, grounded in a particular context or situation, allowing one to engage with *multiple* theories and conceptions of privacy. Rather than seeing privacy as a static or universal property, privacy arises within particular assemblages of social, organizational, and technical components as emphasized by asking "privacy for what/whom," "privacy from what/whom," and "where/when does privacy apply."

Applying the Analytic

In our prior and ongoing work, we have applied Mulligan et al.'s privacy analytic to connect privacy theory with research and design practices in several ways, which we briefly describe below.

(1) Exploring a Privacy Problem Space with Conceptual Design Workbooks

In one project we created a set of conceptual design workbooks to try to explore the "privacy problem space" around new and emerging ubiquitous computing and human biosensing technologies. We used four initial technologies, and created a set of conceptual products that used those technologies in a range of different social and cultural situations to explore how the theoretical construct of privacy might emerge differently in each of the conceptual designs [17]. We completed three iterations or rounds of creating designs. Using Mulligan et al.'s privacy analytic as a framework to interpret our design fictions after each round of designs, we ended our design process after finding we explored a wide variety of combinations of dimensions of privacy.

For instance, we envisioned a camera and analytics system as a neighborhood surveillance product, as a police criminal tracking product (Figure 1). Using the analytic helped us think about how even though these conceptual products used the same technical systems, privacy from whom, who causes privacy harms, what gets protected, and where we might look to provide privacy protection might differ in each case. For instance, the neighborhood surveillance product highlights issues about privacy *from* one's neighbors (and protection from their neighbors' social, economic, and racial biases which might inform the system's analytics), and home security is seen in opposition (the product suggests that for less privacy, one gains security). Privacy in this case might also be about being let alone and be about receiving equal treatment. In contrast, the police tracking product raises questions about privacy *from* the government, 4th Amendment protections, potential use restrictions, and police power. Privacy is about a right as a U.S. citizen. Our analysis suggested that the privacy analytic could be a useful way to help guide and map a design exploration space as well as the privacy problem space.

(2) Analyzing and Coding Research Participants' Discussions of Privacy

We have also used the analytic's dimensions as a way to code qualitative data in privacy research. In a follow up qualitative interview study to the design project described above, we presented the workbooks of conceptual designs to a range of technologists to see how they might use the designs to discuss privacy [16]. One of the ways we coded the interview data was to

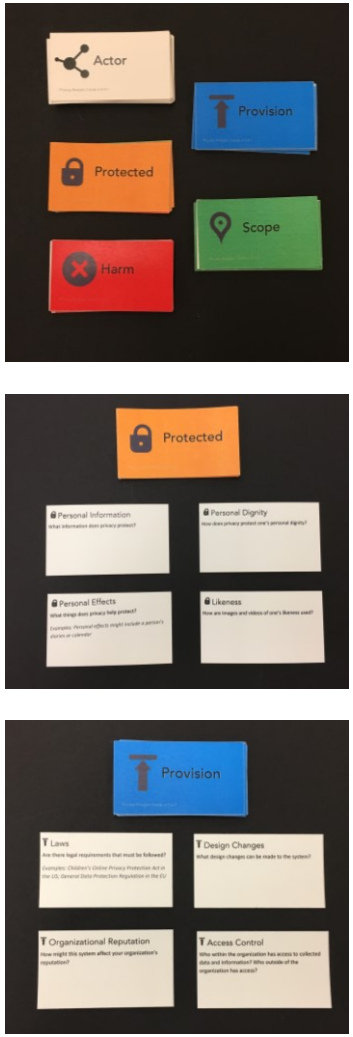

Figure 2. A set of Privacy Design Cards

use the analytic to understand how these technologists were conceptualizing privacy. Whenever a participant discussed privacy, we would code their discussion of privacy along the analytic's 5 meta-dimensions. We found the *protection, harm,* and *scope* dimensions useful in understanding how participants were conceptualizing privacy. We found the *provision* dimension useful to understand ways in which technologists placed responsibility for addressing privacy—ranging from technical design to organizational policies that they could affect, to laws, regulations, or other sources.

Notably, the use of the analytic helped us highlight the complexity of provisioning privacy. One participant felt strongly that physical prominent notices about data collection needed to be posted for the conceptual designs that depicted sensing in public spaces, but she also worried that the notices would not be seen, not provide enough information for meaningful consent, or not provide a meaningful opt-out choice for users, feeling conflicted about it. This highlighted how privacy-related values can be expressed in multiple and conflicting ways, representing a gray area of complex and entangled issues where it can be difficult to address issues with simplistic rules or solutions.

(3) Creating Privacy Design Cards

We have prototyped a set of privacy design cards based on the analytic (Figure 2), inspired by IDEO's method cards, and card activities used to think about values in design [3,6,10]. Our cards include 5 "suits": *actors* (people, groups, and institutions that might need or threaten privacy); *protected* (what gets protected by privacy); *harm* (actions that violate privacy); *provision* (approaches to providing privacy); and *scope* (places and times where privacy might exist). Putting together different combinations of cards suggest different theories of privacy that might be at play. Through a set of activities, the cards can be used in classrooms to educate about privacy, used in design ideation activities, or be used with a case study to try to describe what conceptions of privacy are at play.

Conclusion

Using Mulligan et al.'s privacy analytic in our research has allowed us to grapple with a diverse range of theoretical notions of privacy in our work. Moreover, the analytic helps view privacy as a *sociotechnical* phenomenon. For instance, the protection, harm, provision, scope dimensions encourage thinking about technical features of systems in relation to social and institutional norms and practices. It also helps broaden the privacy "solution space" by thinking about the provision of privacy in a sociotechnical way: in some cases it might be preferable or desirable to provide privacy via design of hardware, software, interfaces, or interactions; while in other cases it might be preferable to provide privacy via law, regulation, organizational processes, or social norms. In most cases, addressing privacy will likely take some combination of those approaches. Thinking about these methods of provision together, rather than defaulting to purely technological solutions, can better enable us to address privacy in more holistic ways. Future work might expand on our uses of the privacy analytic, such as utilizing it in a literature review to understand dominant conceptions of privacy in CSCW and HCI, as a way to analyze or assess privacy risk in design proposals, as a design ideation tool, or using the dimensions as the basis for quantitative survey questions.

References

1. Adam Barth, Anupam Datta, J.C. Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: framework and applications. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, 15 pp.-pp.198. https://doi.org/10.1109/SP.2006.32
2. Christopher A. Le Dantec, Erika Shehan Poole, and Susan P. Wyche. 2009. Values as lived experience: Evolving value sensitive design in support of value discovery. In *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, 1141. https://doi.org/10.1145/1518701.1518875
3. Batya Friedman and David Hendry. 2012. The envisioning cards: a toolkit for catalyzing humanistic and technical imaginations. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems (CHI '12)*, 1145–1148. https://doi.org/10.1145/2207676.2208562
4. Seda Gürses, Carmela Troncoso, and Claudia Diaz. 2011. Engineering Privacy by Design. In *International Conference on Privacy and Data Protection*.
5. Lara Houston, Steven J Jackson, Daniela K Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in Repair. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 1403–1414. https://doi.org/10.1145/2858036.2858470
6. IDEO. 2003. Method Cards. *ideo.com*. Retrieved January 15, 2017 from https://www.ideo.com/us/post/method-cards
7. Nassim JafariNaimi, Lisa Nathan, and Ian Hargraves. 2015. Values as Hypotheses: Design, Inquiry, and the Service of Values. *Design Issues* 31, 4: 91–104. https://doi.org/10.1162/DESI_a_00354
8. Deirdre K. Mulligan, Colin Koopman, and Nick Doty. 2016. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, 2083. https://doi.org/10.1098/rsta.2016.0118
9. Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, California.
10. Katie O'Leary, Tao Dong, Julia Katherine Haines, Michael Gilbert, Elizabeth F Churchill, and Jeffrey Nichols. 2017. The Moving Context Kit: Designing for Context Shifts in Multi-Device Experiences. In *Proceedings of the 2017 Conference on Designing Interactive Systems (DIS '17)*, 309–320. https://doi.org/10.1145/3064663.3064768
11. Katie Shilton, Jes A. Koepfler, and Kenneth R. Fleischmann. 2014. How to see values in social computing: Methods for Studying Values Dimensions. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '14)*, 426–435. https://doi.org/10.1145/2531602.2531625
12. Daniel J Solove. 2008. Privacy: A Concept in Disarray. In *Understanding privacy*. Harvard University Press, Cambridge, Massachusetts.
13. Daniel J. Solove. 2002. Conceptualizing privacy. *California Law Review* 90: 1087–1155. https://doi.org/10.1145/1929609.1929610
14. Daniel J. Solove. 2003. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 477: 477–560.
15. U.S. Department of Homeland Security. 2008. *Privacy Impact Assessment for TSA Whole Body Imaging*. Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-wbi-jan2008.pdf
16. Richmond Y. Wong, Deirdre K Mulligan, Ellen Van Wyk,

James Pierce, and John Chuang. 2017. Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks. *Proceedings of the ACM on Human Computer Interaction* 1, CSCW. https://doi.org/10.1145/3134746

17. Richmond Y. Wong, Ellen Van Wyk, and James Pierce. 2017. Real - Fictional Entanglements: Using Science Fiction and Design Fiction to Interrogate Sensing Technologies. In *Proceedings of the 2017 ACM Conference on Designing Interactive Systems (DIS '17)*. https://doi.org/10.1145/3064663.3064682