Theorizing the Author/Format Editor Relational Dynamic: A Study of the Manual Manuscript Review Process at Clemson University

---

A Dissertation Proposal
by
Yangyang He
Aug 2018

Submitted to the graduate faculty of the
School of Computing
In Partial Fulfillment of the Requirements
for the Dissertation Proposal
and subsequent Ph.D. in Computer Science

Approved By:

____
Dr. Bart P. Knijnenburg
Advisor/Committee Chair

____
Dr. Larry F. Hodges
Committee Member

____
Dr. Alexander Herzog
Committee Member

Author's Publications

The work in this document is partially based on the following publications.

1. He, Y., Bahirat, P., Knijnenburg, B.P. (2018): A Data Driven approach to Designing for Privacy in Household IoT. Submitted to ACM Transactions on Interactive Intelligent Systems (TiiS).

2. Bahirat, P., He, Y., Knijnenburg, B.P. (2018): Exploring Defaults and Framing effects on Privacy Decision Making in Smarthomes. To appear on Interactive Workshop on the Human aspect of Smarthome Security and Privacy, SOUPS 2018, Baltimore, U.S.A.

3. Bahirat, P., He, Y., Menon, A., Knijnenburg, B.P. (2018): A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. IUI2018, Tokyo, Japan.

4. Liu, J., Shen, H., Yu, L., Narman, H.S., Zhai, J., Hallstrom, J.O., He, Y. (2018): Characterizing Data Deliverability of Greedy Routing in Wireless Sensor Networks. IEEE Transactions on Mobile Computing (TMC) 17, 543-559.

5. Ge, R., Feng, X., He, Y., Zou, P. (2017): The Case for Cross-Component Power Coordination on Power Bounded Systems. ICPP2016, Philadelphia, PA, USA

6. Zhai, J., He, Y., Hallstrom, J.O. (2015): A Software Approach to Protecting Embedded System Memory from Single Event Upsets. EWSN2015, Porto, Portugal.

7. He, Y., Du, Y., Hughes, S., Zhai, J., Hallstrom, J.O., Sridhar, N. (2015): DESAL$^{\beta}$: A Framework For Implementing Self-stabilizing Embedded Network Applications. International Internet of Things Summit, pp. 307-312. Springer, Cham, 2015.

8. Ruffing M., He Y., Kelly, M., Hallstrom, J.O., Olariu, S., Weigle, M.C. (2014): A Retasking Framework for Wireless Sensor Networks. Military Communications Conference (MILCOM), 2014 IEEE 1066-1071.

Outline

Abstract

Internet of Things (IoT) are more widely used recently, from general industrial equipment, to household electronics, to wearable devices. With IoT systems becoming more complex, users of IoT devices are paying more attention to their privacy, bringing new challenges to the privacy-setting interface designer. In this proposed dissertation, we focus on four of the most important challenges: (i). How to design privacy-setting interfaces for general IoT devices users? (ii) How to design privacy-setting interfaces for Household IoT devices users and how exactly does the ? (iii) How to design privacy-setting interfaces for Fitness tracker devices users? (iv). How satisfied are the user when they are using these privacy-setting interfaces? In this proposal, we focus on

Chapter 1

Introduction

During the recent decade, our everyday life has been revolutionized by all kinds of ”smart” electronic equipments. These smart devices are intended to collect information directly related to the users, such as fitness/healthy information, or the environment of users, such as users’ home. They can also connect to each other, to create powerful new applications that supports our day-to-day activities.

Chapter 2

Work Completed

In this chapter, we present the work completed to date in the areas of designing for privacy for general IoT and Household IoT.

2.1 A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces

In this section, we present the data-driven design, the dataset that we use, the inspection of users' behaviors using statistical analyses, prediction of users' behaviors using machine learning techniques, and the privacy-setting prototypes that we create based on both statistical and machine learning results.

2.1.1 Data-driven design

What design process allows us to develop a usable privacy-setting interface for IoT? The development of usable privacy interfaces commonly relies on user studies with existing systems. However, this method is not possible in our IoT control scenario, because the Intel control framework has yet to be implemented [3]. We therefore develop and employ a *data-driven design* methodology, leveraging an existing dataset collected by Lee and Kobsa [9], who asked users whether they would allow or deny IoT devices in their environment to collect information about them. We use this dataset in two phases.

In our first phase, we develop a "layered" settings interface, where users make a decision on a less granular level (e.g., whether a certain recipient is allowed to collect their personal information or not), and only move to a more granular decision (e.g., what types of information this recipient is allowed to collect) when they desire more detailed control. This reduces the complexity of the decisions users have to make, without reducing the amount of control available to them. We use statistical analysis of the Lee and Kobsa dataset to decide which aspect should be presented at the highest layer of our IoT privacy-setting interface, and which aspects are relegated to subsequently lower layers.

In our second phase, we develop a "smart" default setting, which preempts the need for many users to manually change their settings [17]. However, since people differ extensively in their privacy preferences [11], it is not possible to achieve an optimal default that is the same for everyone. Instead, different people may require different settings. Outside the field of IoT, researchers have been able to establish distinct clusters or "profiles" based on user behavioral data [8, 11, 20]. We perform machine learning analysis on the Lee and Kobsa dataset to create a similar set of "smart profiles" for our IoT privacy-setting interface.

The remainder of this paper is structured as follows: We first summarize previous work on privacy in IoT scenarios, and describe the structure of the Lee and Kobsa [9] dataset. We then *inspect* users' behaviors using statistical analysis. Next, we *predict* users' behaviors using machine learning methods. We subsequently present a set of prototypes for an IoT privacy-setting interface. Finally, we conclude with a summary of our proposed procedure and the results of our analysis.

2.1.2 Dataset

This study is based on a dataset collected by Lee and Kobsa [9]. A total of 2800 scenarios were presented to 200 participants (100 male, 99 female, 1 undisclosed) through Amazon Mechanical Turk. Four participants were aged between 18 and 20, 75 aged 20–30, 68 aged 30–40, 31 aged 40–50, 20 aged 50–60, and 2 aged > 60.

Each participant was presented with 14 scenarios describing a situation where an IoT device would collect information about the participant. Each scenario was a combination of five contextual parameters (Table 2.1), manipulated at several levels using a mixed fractional factorial design that allowed us to test main effects and two-way interactions between all parameters.

For every scenario, participants were asked a total of 9 questions. Our study focuses on the **allow/reject** question: “If you had a choice to allow/reject this, what would you choose?”, with options “I would allow it” and “I would reject it”. We also used participants’ answers to three attitudinal questions regarding the scenario:

- **Risk:** How risky or safe is this situation? (7pt scale from “very risky” to “very safe”)
- **Comfort:** How comfortable or uncomfortable do you feel about this situation? (7pt scale)
- **Appropriateness:** How appropriate do you consider this situation? (7pt scale)

2.1.3 Inspecting users’ behaviors

In this section we analyze how users’ behavioral intentions to allow or reject the information collection described in the scenario are influenced by the scenario parameters. In line with classic attitude-behavior models [1], we also investigate whether users’ attitudes regarding the scenario—their judgment of risk, comfort, and appropriateness—mediate these effects. This mediation analysis [2] involves the following test:

- **Test 1:** The effect of the scenario parameters (who, what, where, reason, persistence) on participants’ attitudes (risk, comfort, appropriateness).
- **Test 2:** The effect of participants’ attitudes on their behavioral intentions (the allow/reject decision).
- **Test 3:** The effect of the parameters on behavioral intentions, controlling for attitudes.

If tests 1 and 2 are significant, and test 3 reveals a substantial reduction in conditional direct effect (compared to the marginal effect), then we can say that the effects of the scenario parameters on participants’ behavioral intention are mediated by their attitudes. Moreover, if the conditional direct effect is (close to) zero, then the effects are fully (rather than partially) mediated.

2.1.3.1 Scenario Parameters and Attitude

ANOVA Test of Main Effects: To understand the effect of the scenario parameters on participants’ attitudes, we created a separate *linear mixed effects regression* (*lmer*) model with a random intercept (to account for repeated measures on the same participant) for each dependent variable (risk, comfort, appropriateness), using the scenario parameters as independent variables. We

Table 2.1: Parameters used in the experiment. Example scenarios:
"A device of a friend records your video to detect your presence. This happens continuously, while you are at someone else's place, for your safety."
"A government device reads your phone ID to detect your identity. This happens once, while you are in a public place (e.g. on the street), for health-related purposes."

Parameter	**Levels**
Who *The entity collecting the data*	1. Unknown 2. Colleague 3. Friend 4. Own device 5. Business 6. Employer 7. Government
What *The type of data collected and (optionally) the knowledge extracted from this data*	1. PhoneID 2. PhoneID>identity 3. Location 4. Location>presence 5. Voice 6. Voice>gender 7. Voice> age 8. Voice>identity 9. Voice>presence 10. Voice>mood 11. Photo 12. Photo>gender 13. Photo>age 14. Photo>identity 15. Photo>presence 16. Photo>mood 17. Video 18. Video>gender 19. Video>age 20. Video>presence 21. Video>mood 22. Video>looking at 23. Gaze 24. Gaze>looking at
Where *The location of the data collection*	1. Your place 2. Someone else's place 3. Semi-public place (e.g. restaurant) 4. Public space (e.g. street)
Reason *The reason for collecting this data*	1. Safety 2. Commercial 3. Social-related 4. Convenience 5. Health-related 6. None
Persistence *Whether data is collected once or continuously*	1. Once 2. Continuously

Table 2.2: Effect of scenario on attitudes. Each model builds upon and is tested against the previous.

Model	χ^2	*df*	*p*-value
$risk \sim (1\|sid)$			
+who	315.37	6	$< .0001$
+what	67.74	23	$< .0001$
+reason	15.65	5	.0079
+persistence	9.95	1	.0016
+where	7.47	3	.0586
+who:what	166.47	138	.0050
Model	χ^2	*df*	*p*-value
$comfort \sim (1\|sid)$			
+who	334.06	6	$< .0001$
+what	83.24	23	$< .0001$
+reason	18.68	5	.0022
+persistence	14.73	1	.0001
+where	3.25	3	.3544
+who:what	195.07	138	.0001
Model	χ^2	*df*	*p*-value
$appropriateness \sim (1\|sid)$			
+who	315.77	6	$< .0001$
+what	72.87	23	$< .0001$
+reason	23.27	5	.0003
+persistence	8.97	1	.0027
+where	5.46	3	.1411
+who:what	214.61	138	$< .0001$

employed a forward stepwise procedure, adding the strongest remaining parameter into the model at each step and comparing it against the previous model. Table 2.2 shows that all parameters except **where** have a significant effect on each of the attitudes.

Post-hoc Comparisons: We also conducted Tukey post hoc analyses to better understand how the various values of each parameter influenced the attitudes. **Where** was excluded from these analyses, as it did not have an overall significant effect. Some key findings of these post hoc analyses are:

Who: Participants perceive more *risk* when the recipient of the information is 'unknown' than for any other recipient (d range = [0.640, 1.450] and all ps $< .001$, except for 'government': $d = 0.286$, $p < .05$). 'Government' is the next most risky recipient (d range = [0.440, 1.190], all ps $< .001$). Participants consider their 'own device' the least risky (d range = [0.510, 1.450], all ps $< .001$). Similar patterns were found for *comfort* and *appropriateness*.

Reason: Participants were more *comfortable* disclosing information for the purpose of 'safety' than for any other reason except 'health' (d range = [0.230, 0.355], all ps $< .05$). They also believe that disclosing information for the purpose of 'health' or 'safety' is more *appropriate* than for 'social' or 'commercial' purposes (d range = [0.270, 0.310], all ps $< .05$).

Persistence: Participants were more *comfortable*, found it more *appropriate*, and less *risky* to disclose their information 'once' rather than 'continuously' ($d = 0.146$, $p < .01$).

What: This parameter has a large number of values, so we decided to selectively test planned contrasts instead of post-hoc tests. We first compared different mediums (voice, photo, video) regardless of what is being inferred:

- Participants were significantly more *comfortable* with 'voice' than 'video' ($d = 0.260$, $p = .005$), and found 'voice' less *risky* ($d = -0.239$, $p = .005$) and more *appropriate* ($d = 0.217$, $p = .015$) than 'video'.

- Participants were significantly more *comfortable* with 'voice' than 'photo' ($d = 0.201$, $p = .007$) and found 'voice' more *appropriate* than 'photo' ($d = 0.157$, $p = .028$). There was no significant difference in terms of *risk* ($p = .118$).

- No differences were found between 'photo' and 'video' in terms of *risk* ($p = .24$), *comfort* ($p = .35$) and *appropriateness* ($p = .26$).

We also compared different inferences (e.g. age, gender, mood, identity) across mediums. The following planned contrasts were significant (all others were not):

- Participants were significantly more *comfortable* ($d = 0.363$, $p = .028$) and found it more *appropriate* ($d = 0.371$, $p = .018$) to reveal their 'age' rather than their 'identity'.

- Participants were significantly more *comfortable* ($d = 0.363$, $p = .008$) and found it more *appropriate* ($d = 0.308$, $p = .024$) to reveal their 'presence' rather than their 'identity'.

Interaction effects: We also checked for two-way interactions between the scenario parameters. The only significant interaction effect observed was between **who** and **what**. The last line of each section in Table 2.2 shows the results of adding this interaction to the model. Due to space concerns, we choose not to address the post-hoc analysis of the $7 * 24 = 168$ specific combinations of who and what.

Table 2.3: Effect of attitudes and scenario on allow/reject.

Model	OR	χ^2	*df*	*p*-value
$allow \sim (1\|sid)$				
+risk	0.25	1005.24	1	$< .0001$
+comfort	5.04	723.27	1	$< .0001$
+appropriateness	3.47	128.17	1	$< .0001$
+who		8.80	6	.1851
+what		26.07	23	.2976
+reason		19.33	5	.0017
+persistence		12.69	1	.0004

Table 2.4: Effect of scenario on allow/reject, *not* controlling for attitudes.

Model	χ^2	*df*	*p*-value
$allow \sim (1\|sid)$			
+who	221.36	6	$< .0001$
+what	78.55	23	$< .0001$
+reason	21.95	5	.0005
+persistence	20.64	1	$< .0001$

2.1.3.2 Attitude and Behavioral intention

To test the effects of participants' attitudes on their allow/reject decision, we ran a *generalized linear mixed effects regression* (*glmer*) with a random intercept and a logit link function to account for the binary dependent variable. We found significant effects of all the three attitudes on participants' allow/reject decision (see Table 2.3). Each 1-point increase in **risk** results in a 4.04-fold decrease in the odds that the scenario will be allowed ($p < .0001$). Each 1-point increase in **comfort** results in a 5.04-fold increase ($p < .0001$), and each 1-point increase in **appropriateness** results in a 3.47-fold increase ($p < .0001$).

Mediation Analysis: The bottom half of Table 2.3 shows the *conditional* effects of the significant parameters (who, what, reason, persistance) on participants' allow/reject decision, controlling for attitude. **Who** and **what** are no longer significant; these effects are thus fully mediated by attitude. The effects of **reason** and **persistance** are still significant, but smaller than the marginal effects (i.e., without controlling for attitude, see Table 2.4)—their χ^2s are reduced by 12% and 39%, respectively. This means that the mediation effect was substantial in all cases. The final mediation model is displayed in Figure 2.1.

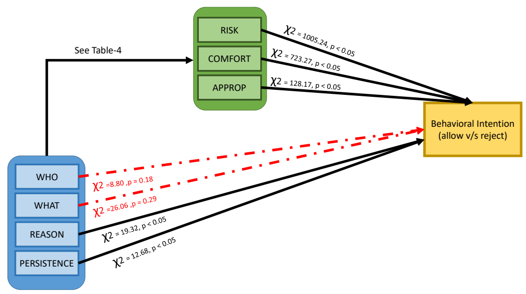

Figure 2.1: Mediation model of the effect of scenario parameters on participants' intention to allow/reject the scenario, mediated by attitudinal factors

2.1.3.3 Discussion of Statistical Results

Our statistical results show several patterns that can inform the development of an IoT privacy-setting interface. We find that **who** is the most important scenario parameter, and should thus end up at the top layer of our interface. People are generally concerned about IoT scenarios involving unknown and government devices, but less concerned about about data collected by their own devices. Mistrust of government data collection is in line with Li et al.'s finding regarding US audiences [10].

What is the next most important scenario parameter, and its significant interaction with **who** suggests that some users may want to allow/reject the collection of different types of data by different types of recipients. Privacy concerns are higher for photo and video than for voice, arguably because photos and videos are more likely to reveal the identity of a person. Moreover, people are less concerned with revealing their age and presence, and most concerned with revealing their identity.

The **reason** for the data collection may be used as the next layer in the interface. Health and safety are generally seen as acceptable reasons. **Persistence** is less important, although one-time collection is more acceptable than continuous collection. **Where** the data is being collected does not influence intention at all. This could be an artifact of the dataset: location is arguably less prominent when reading a scenario than it is in real life.

Finally, participants' attitudes significantly (and in some cases fully) mediated the effect of scenario parameters on behavioral intentions. This means that these attitudes may be used as a valuable source for classifying people into distinct groups. Such attitudinal clustering could capture a significant amount of the variation in participants in terms of their preferred privacy settings, espcially with respect to the **who** and **what** dimensions.

Chapter 3

Proposed Work

Chapter 4

Related Work

4.1 A Data Driven approach to Designing for Privacy in Household IoT

Our goal is to develop intuitive interfaces for IoT privacy settings, using a data-driven approach. In this section we therefore discuss existing research on privacy-setting interfaces and on privacy prediction.

4.1.1 Existing privacy control schemes

Smartphones give users control over their privacy settings in the form of prompts that ask whether the user allows or denies a certain app access to a certain type of information. Such prompts are problematic for IoT, because IoT devices are supposed to operate in the background. Moreover, as the penetration of IoT devices in our homes continues to increase, prompts would become a constant noise which users will soon start to ignore, like software EULAs [6] or privacy policies [7].

In [**?**], Pejovic and Musolesi presented the design and implementation of an efficient online learner that can serve as a basis for recognizing opportune moments for interruption. The design of the library is based on an in-depth study of human interruptibility. Comparatively, our work tries to find the most suitable privacy-setting profile for each user based on their privacy preference on different household IoT scenarios.

4.1.2 Privacy-Setting Interfaces

Beyond prompts, one can regulate privacy with global settings. The most basic privacy-setting interface is the traditional "access control matrix", which allows users to indicate which entity gets to access what type of information [16]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [18]. Taking a step further, Raber et al. [13] proposed *Privacy Wedges* to manipulate privacy settings. Privacy Wedges allow users to make privacy decisions using a combination of semantic categorization (the various wedges) and inter-personal distance (the position of a person on the wedge). Users can decide who gets to see various posts or personal information by "coloring" parts of each wedge.

Privacy wedges have been tested on limited numbers of friends, and in the case of household IoT they are likely to be insufficient, due to the complexity of the decision space. To wit, IoT privacy decisions involve a large selection of devices, each with various sensors that collect data for a range of different purposes. This makes it complicated to design an interface that covers every possible setting [19]. A wedge-based interface will arguably not be able to succinctly represent such complexity, and therefore either be impossible, or still lead to a significant amount of information and choice overload.

We propose a data-driven approach to solve this problem: statistical analysis informs the construction of a layered settings interface, while machine learning-based privacy prediction helps us find smart privacy profiles.

4.1.3 Privacy Prediction

Several researchers have proposed privacy prediction as a solution to the privacy settings complexity problem. Sadeh et al. used a k-nearest neighbor algorithm and a random forest algorithm to predict users' privacy preferences in a location-sharing system [15], based on the type of recipient and the time and location of the request. They demonstrated that users had difficulties setting their privacy preferences, and that the applied machine learning techniques can help users to choose more accurate disclosure preferences. Similarly, Pallapa et al. [12] present a system which can determine the required privacy level in new situations based on the history of interaction between users. Their system can efficiently deal with the rise of privacy concerns and help users in a pervasive system full of dynamic interactions.

Dong et al. [4] use a binary classification algorithms to give users personalized advice regarding their privacy decision-making practices on online social networks. They found that J48 decision trees provided the best results. Li and et al. [10] similarly use J48 to demonstrate that taking the user's cultural background into account when making privacy predictions improves the prediction accuracy. Our data stems from a culturally homogeneous population (U.S. Mechanical Turk workers), so cultural variables are outside the scope of our study. We do however follow these previous works in using J48 decision trees in our prediction approach.

We further extend our approach using *clustering* to find several smart default policies ("profiles"). This is in line with Fang et al. [5], who present an active learning algorithm that comes up with privacy profiles for users in real time. Since our approach is based on an existing dataset, our algorithm does not classify users in real time, but instead creates a static set of profiles 'offline', from which users can subsequently choose. This avoids cold start problems, and does not rely on the availability of continuous real-time behaviors. This is beneficial for household IoT privacy settings, because users often specify their settings in these systems in a "single shot", leaving the settings interface alone afterwards.

Ravichandran et al. [14] employ an approach similar to ours, using k-means clustering on users' contextualized location sharing decisions to come up with several default policies. They showed that a small number of policies could accurately reflect a large part of the location sharing preferences. We extend their approach to find the best profiles based on various novel clustering approaches, and take the additional step of designing user interfaces that incorporate the best solutions.

Chapter 5

Conclusion

Appendices

Bibliography

[1] Icek Ajzen and Martin Fishbein. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological bulletin*, 84(5), 1977.

[2] Reuben M Baron and David A Kenny. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology*, 51(6):1173–1182, 1986.

[3] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. HCI in Business: A Collaboration with Academia in IoT Privacy. In Fiona Fui-Hoon Nah and Chuan-Hoo Tan, editors, *HCI in Business*, number 9191 in Lecture Notes on Computer Science. Springer, 2015.

[4] Cailing Dong, Hongxia Jin, and Bart P Knijnenburg. Ppm: A privacy prediction model for online social networks. In *International Conference on Social Informatics*, pages 400–420, 2016.

[5] Lujun Fang and Kristen LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web*, pages 351–360, 2010.

[6] Nathaniel Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan. Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, pages 43–52, 2005.

[7] Carlos Jensen and Colin Potts. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In *2004 Conference on Human Factors in Computing Systems*, pages 471–478, 2004.

[8] Bart P Knijnenburg, Alfred Kobsa, and Hongxia Jin. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, 71(12):1144–1162, 2013.

[9] Hosub Lee and Alfred Kobsa. Understanding user privacy in internet of things environments. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, 2016.

[10] Yao Li, Alfred Kobsa, Bart P Knijnenburg, and MH Carolyn Nguyen. Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies*, 2:93–112, 2017.

[11] Judith S Olson, Jonathan Grudin, and Eric Horvitz. A study of preferences for sharing and privacy. In *CHI'05 extended abstracts on Human factors in computing systems*, pages 1985–1988, 2005.

[12] Gautham Pallapa, Sajal K Das, Mario Di Francesco, and Tuomas Aura. Adaptive and context-aware privacy preservation exploiting user interactions in smart environments. *Pervasive and Mobile Computing*, 12:232–243, 2014.

[13] Frederic Raber, Alexander De Luca, and Moritz Graus. Privacy wedges: Area-based audience selection for social network posts. In *Proceedings of the 2016 Symposium on Usable Privacy and Security*, 2016.

[14] Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M Sadeh. Capturing social networking privacy preferences. In *Proceedings of the 2009 Symposium on Usable Privacy and Security*, pages 1–18, 2009.

[15] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing peoples privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009.

[16] R. S. Sandhu and P. Samarati. Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48, 1994.

[17] N. Craig Smith, Daniel G. Goldstein, and Eric J. Johnson. Choice Without Awareness: Ethical and Policy Implications of Defaults. *Journal of Public Policy & Marketing*, 32(2):159–172, 2013.

[18] Jason Watson, Andrew Besmer, and Heather Richter Lipford. +Your circles: sharing behavior on Google+. In *Proceedings of the 8th Symposium on Usable Privacy and Security*, pages 12:1–12:10, 2012.

[19] Meredydd Williams, Jason RC Nurse, and Sadie Creese. The perfect storm: The privacy paradox and the internet-of-things. In *11th International Conference on Availability, Reliability and Security*, pages 644–652, 2016.

[20] Pamela J Wisniewski, Bart P Knijnenburg, and Heather Richter Lipford. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, 98:95–108, 2017.