Perspectives on privacy in the use of online systems

Meredydd Williams
Department of Computer Science
University of Oxford, Oxford, UK
meredydd.williams@cs.ox.ac.uk

Jason R. C. Nurse
Department of Computer Science
University of Oxford, Oxford, UK
jason.nurse@cs.ox.ac.uk

Human-Computer Interaction looks to better understand the relationship between people and computers. Our work considers this relationship in the context of privacy and the privacy expectations users have when using online systems. While many surveys suggest the public care about this subject, users often act in a manner perceived contrary to their claims; a notion termed the 'Privacy Paradox'. However, research suggests privacy is inherently subjective and contextual, leading us to question: do users actually define '*private online behaviour*' in the same manner as those who study the topic? Although our exploratory survey found a general intersection between participants' perceptions and those in existing literature, opinions differed in several key areas. For example, we found users often conceptualise protection in less-technical terms and are prone to conflating privacy and security. We believe that when we expand our analyses to the general public, we will see an even greater disparity between privacy perceptions. Through this research we look to inform the development of systems and privacy-protective tools that users can actually appreciate.

Privacy, privacy paradox, user survey, online behaviour, mental models, human-computer interaction

1. INTRODUCTION

HCI explores the relationship between people and computers; an essential field in our connected world. While the benefits of technological growth are undeniable, the traditional human perceptions of privacy are placed under great pressure, particularly in online environments (Creese and Lamberts 2009).

Many opinion polls and surveys suggest that the public care about online privacy. Rainie *et al.* found that 86% claimed to protect this right (2013), while 84% in a 2015 study wished to control data disclosure (Turow, Hennessy and Draper 2015). Despite these vocal assertions, individuals are often perceived to express behaviour to the contrary. Carrascal *et al.* found participants willing to sell their browsing history for €7 (2013) and a 2016 survey saw less than 10% of respondents encrypted their emails (Morar Consulting 2016). This apparent disparity between claim and action has been termed the 'Privacy Paradox' (Brown, Mortier and Rodden 2013). However, since privacy is both highly subjective (Syverson 2003) and contextual (Nissenbaum 2004), might participants just have differing perceptions of private behaviour?

In this paper, we report on the first steps of an exploratory study concerning this paradox. We aim to understand to what extent do researchers and users agree on what comprises *'private online behaviour'*. We posit that if users undertake actions that they believe to be private, rather than just those considered by academics, then we should adapt existing mental models of privacy.

We first explain our research methodology and initial experiment design in Section 2. In Section 3 we discuss the results from this experiment, probing whether privacy perceptions differ between users and academics. We then conclude this preliminary work in Section 4 and consider how these findings, and those from our larger study, can inform the development of technologies which better match users' privacy needs.

2. METHODOLOGY AND EXPERIMENT DESIGN

Our methodology consists of two main tasks: (i) surveying existing privacy studies to understand how researchers define the topic, and (ii) soliciting the privacy perceptions of computer users. The initial experiment we present follows this structure and will be further expanded in our future research.

This paper specifically concerns the analysis of 35 well-cited privacy studies from the fields of HCI and cyberpsychology. Once literature was collected, we coded and categorised papers based on which actions their authors considered to be indicative of privacy. Next, we recruited a sample of 35 skilled

cybersecurity users for our initial study. We asserted that any discrepancy between their perceptions and those of privacy researchers might suggest a much greater disparity between academics and the opinions of the general public. To avoid biasing our respondents, we simply asked participants to list behaviours "*characteristic of being or behaving privately online*". The responses were then coded and grouped under general actions (e.g. encryption, anonymous browsing) to enable direct comparison against academic perceptions. This coding process was undertaken iteratively until our classifications reached convergence. Below we outline and discuss our initial findings.

3. INITIAL FINDINGS AND DISCUSSION

As presented below in Table 1, the perceptions of our participants frequently intersected with those of privacy researchers. In both cases we found that limiting online disclosure was considered private, as was possessing strong social-media settings. These similarities are likely due in part to the composition of our initial sample, and we expect perceptions of the general public to differ further.

Table 1: *Most frequent 'private online behaviours'*

Behaviour	Survey	Existing literature
Limiting information disclosure	23	15
Strong online privacy settings	17	9
Anonymous browsing usage	15	5
Pseudonym usage	14	6
Private browser tabs	14	-
Abstaining from services	13	5

Despite some intersection, there were a large number of reported actions that were not considered in surveyed research. Avoiding free public Wi-Fi, signing into services anonymously and using private browsing tabs were all considered to comprise acting privately. In total, participants listed 76 unique actions, compared to the 22 found in our literature review. This suggests that many 'private' behaviours undertaken by individuals are not considered by privacy researchers. This is important for HCI, as it implies users might be judged to be less private than they actually are, inhibiting our understanding of how humans and computers interact.

Less-technical approaches such as opting-out of data collection and sharing privacy advice were also not considered in surveyed studies. In contrast, those behaviours exclusive to existing literature included installing anti-spyware tools (Buchanan et al. 2007) and using anonymous remailers for communication (Oomen and Leenes 2008). This suggests that users might act in what they consider to be a private manner, but be discounted for not using oft-complex privacy-protective tools.

We also found that respondents frequently conflated security and privacy. We categorised each action into one of three classes: privacy, security or both. This was undertaken by considering the primary purpose of each action and comparing this against textbook definitions (Solove 2008; Gollmann 2011). This process was again undertaken in an iterative manner to increase the validity of our analyses. We found that while the main purpose of 68% of academic behaviours were privacy (15/22), only 51% of sample responses chiefly concerned the subject (39/76). While security solutions often ensure data confidentiality, the two fields should not be conflated. Although firewalls can protect against external attack, they do little when personal information is disclosed to online portals. These findings have greater implications for HCI, as security systems might be misinterpreted as a panacea, therefore placing privacy at risk.

4. CONCLUSIONS AND FUTURE WORK

Through our ongoing study we consider HCI in the context of online privacy, analysing how humans interact with computers in a private manner. We discovered that while our respondents highlighted many less-technical actions, academic literature is often preoccupied with software which might be considered complex. We also found our sample frequently conflated privacy and security; topics which can differ in important respects. We believe these issues have important ramifications for HCI, as misconceptions can inhibit our understanding of how humans and computers interact.

Since our cybersecurity sample likely understood privacy more than the general public, we will now look to survey ordinary citizens through a larger sample. We believe that perceptions will differ greatly between experts and the public, and that researchers should reconsider how they define private behaviour in the use of online systems.

We believe our ongoing research has importance for HCI for a number of reasons. Firstly, it facilitates a greater understanding of both human-computer relationships and mental models by studying real user perceptions. Secondly, findings can inform the design of systems which respect privacy in a manner individuals actually understand. Finally, results can promote protective tools, such as privacy advice-sharing platforms, which embrace the socio-technical solutions which users appear to appreciate. With individuals often having different perceptions to those who study privacy, we hope further HCI research can reduce this disconnect.

REFERENCES

Brown, Anthony, Richard Mortier and Tom Rodden (2013) MultiNet: Reducing interaction overhead in domestic wireless networks. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Paris, 27 April - 2 May 2013. New York: ACM. 1569–1578.

Buchanan, T., C. Paine, A.N. Joinson and U.D. Reips (2007) Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58(2). 157–165.

Carrascal, JP, C Riederer, V Erramilli, M Cherubini and R de Oliveira (2013) Your browsing behavior for a big mac: Economics of personal information online. In: *Proceedings of the 22nd International Conference on World Wide Web*. Rio de Janeiro, 13-17 May 2013. New York: ACM. 189–200.

Creese, S and K Lamberts (2009) Can cognitive science help us make information risk more tangible online? In *Proceedings of the WebSci'09*. Athens, 18-20 March 2009.

Gollmann, Dieter (2011) *Computer security*. Chichester: John Wiley & Sons.

Morar Consulting (2016) *The dangers of our digital lives*. Available from https://www.hidemyass.com/documents/hma-survey-summary-2-5-16.pdf (6 June 2016).

Nissenbaum, Helen (2004) Privacy as contextual integrity. *Washington Law Review* 79(1):119–158.

Oomen, I and R Leenes (2008) Privacy risk perceptions and privacy protection strategies. *Policies and Research in Identity Management in The International Federation for Information Processing* 261:121–138.

Rainie, L, S Kiesler, R Kang, M Madden, M Duggan, S Brown and L Dabbish (2013) Anonymity, privacy, and security online. *Pew Internet & American Life Project*.

Solove, Daniel J. (2008) *Understanding privacy*. Cambridge: Harvard University Press.

Syverson, P. (2003) The paradoxical value of privacy. In: *Proceedings of the 2nd Annual Workshop on Economics and Information Security*. Maryland, 29-30 May 2003.

Turow, J, M Hennessy and N Draper (2015) *The tradeoff fallacy*. University of Pennsylvania.