Article type : Research Dialogue

Corresponding author mail id : aradhna@umich.edu

Privacy is a Concern: An Introduction to the Dialogue on Privacy

Online interactions of all kinds – financial, social, informational, educational – are growing, and even more so given the lockdowns with Covid-19 in 2020. At the same time, there is also a decrease in the costs for gathering, storing and analyzing online data, related to individuals and groups -- and the rewards for doing this are enormous. Unfortunately, these are the very ingredients that make privacy a big concern.

When are consumers ready to give up privacy? When do they give up privacy because it is just too painful to wade through the "legalese"? When do they give it up because the tradeoff works in favor of giving it up? When are they fooled into giving it up? How can businesses, governments and society in general be moved in directions that protect individual and collective privacy to some "optimum level"? What is that optimum in the first place? These are just a subset of questions that we want answered – and it is apparent that we need research on the topic of privacy from a consumer psychology perspective. But, so far, research on privacy is virtually non-existent in consumer psychology.

This dialogue provides a direction for conducting such research. I invited Acquisti, Brandimarte and Loewenstein to write the target article for this dialogue, not in small part because of their very influential article on privacy that appeared in Science (2015). Their target article for this dialogue is written with a view to informing potential research by consumer psychologists.

Acquisti, Brandimarte and Loewenstein (2020, ABL) suggest that a lay belief is that "though people *say* that they care about privacy, they actually don't"—as is seen in their careless online behaviors. They argue that, in fact, consumers take many precautions for their privacy, and they provide evidence for this from surveys, field studies, and experiments. This evidence shows, that individual's try and regulate the boundaries of interactions with others, for instance by alternating between different email accounts, choosing privacy settings to limit visibility of their social media posts, or replying privately to group messages. Using experimental results, they further indicate, for example that, online shoppers in a field experiment are willing to pay a little more to keep their mobile phone number private (Jentzsch et al., 2012)".

ABL also note, though, that "*desired* privacy may not be matched by *achieved* privacy". One reason they offer is that products, software and apps may be designed to induce bad choices by consumers regarding their privacy. For instance, for immediate access to an app, one may be asked to sign a privacy agreement; and, with the present-bias that humans have (Benhabib, Bisin and Schotter 2010), consumers choose to sign off. Some other reasons offered by ABL for this divergence between desired and achieved privacy is a greater readiness to divulge information when consumer feel greater control over their privacy (and ironically, also when they feel no control), and persistence of the privacy problem leading to tolerance. They also suggest network externalities whereby "Other people's usage of privacy-intrusive services increases the cost for privacy-conscious consumers *not* to use them."

ABL end their article with looking at what can be done about the situation including using nudges to direct consumers to make the right choices regarding their privacy. One statement in their article especially resonated with me: "many Americans believe that privacy policies provide them with protections, when the reverse is more likely to be true; they provide firms with uninformed consent to use and often sell their information (Hoofnagle & Urban, 2014)."

I sought three commentaries for ABL's article – from social psychologists, lawyers/public policy scholars and computer scientists (reported in this order). Oyserman and Schwarz (OS), in their commentary, add to factors that contribute to the discrepancy between desired and achieved privacy. They point out, for instance, that the sequence in which communication occurs can make consumers sign away privacy rights (e.g., privacy questions are often asked only after the consumer is fully entrenched in the endeavor and has a sunk cost in it);

the anthropomorphic relationship one develops with devices so that they are trusted more; and playing with people's identities to make privacy issues and disinformation less of a concern. As OS state, "disinformation works best when linked to images and taglines that feel fluent because they are relevant to (one's) own identities".

OS also point out that "What people miss is that monetizing information is not just about embarrassing secrets or obtaining credit card information. The broader issue of online tracking and information linkage across many activities is for the purpose of delivering finely tuned persuasive messages".

In the second commentary, Mulligan, Regan and King (MRK) expand beyond ABL's focus on the individual, to a focus on the collective social value of privacy. In doing so, they employ Altman's (1975) central contribution, that privacy is a constantly negotiated social construct, not a preexisting individually oriented right or preference. They pick up on ABL's concern that "companies employ 'dark patterns'—design choices intended to manipulate people into making decisions against their best interests—to divest individuals of their data", but contend that these practices extend way beyond what is suggested by ABL. They state that ABL seem to focus on "notice and consent" regimes, whereas companies use more nefarious methods to evade privacy concerns, such as the imposition of 'clickwraps' (an accept or decline agreement before a person can access a website), or even appealing to individuals' social motivations (e.g., suggesting that the individual can "Become part of something bigger").

This second point plays into the larger issue MRK address, that privacy may be demonized "as the refuge of free-riders, parasites, and criminals", resulting in "the impossibility of extracting the behavior of individuals, including research participants, from the society that has constructed their understanding of what is not only possible but desirable"

MRK therefore suggest that "successful legislative efforts to protect privacy are those that frame privacy as instrumental to realizing other socially desirable ends" (I would like to the reader to note the use of "other" in this sentence, implying that "protecting privacy for the sake of privacy alone will not fly"). And, given their expertise on algorithms and privacy law, they also indicate that "Congress is considering imposing algorithmic audit requirements on companies to address concerns with bias, extending campaign finance laws to the Internet to address political filter bubbles, and revising existing frameworks that limit platform liability for various kinds of information".

In the third commentary, Jagadish adds another perspective, from a technological angle (Jagadish is an expert on data science ethics). He introduces the notion of "circle of privacy" and suggests that there are different circles of shared knowledge that we have with different groups of friends/firms, e.g., with our group of school friends, with our work colleagues, with our siblings, with our Facebook friends, with an app (e.g., an app we use for weekly food deliveries, like Imperfect Foods). He then indicates that while some of these circles have symmetric relationships in terms of information knowledge and control over privacy (generally inter-personal relationships with groups of humans), relationships that involve firms are not typically symmetric. Here, firms may have more power over our information than we want and they may want to share our information more than we desire. The only way to reign them in is through policy (as MLK say) which is facilitated through technology.

Besides "circles of privacy", Jagadish also introduces many other constructs which can be informative to consumer psychology research, such as the third party doctrine whereby sharing information voluntarily with a third party implies complete loss of control (and privacy) for that information. He also introduces the reader to new techniques being used to protect individuals' privacy, like "differential privacy", where a small amount of noise is intentionally added to computed aggregates, so that reverse engineering of data to the individual level is rendered extremely difficult.

In their rejoinder to the three commentaries, ABL highlight many questions for future researchers to contemplate, with the hope that "research in this area may ultimately change the frame of the public debate surrounding privacy: Rather than unquestionably accepting the premise that loss of privacy is necessary to enjoy the benefits of data, or at the opposite extreme calling for radical privacy protections whatever their cost, we should ask: are there approaches to the regulation of privacy that could enable society to realize the greatest benefits from data sharing while simultaneously protecting privacy in the ways that matter most?". I hope that this dialogue facilitates responses to this call.

Privacy matters. Consumers' privacy, in their interaction with firms, is central to this discussion. Regulation for privacy has begun in Europe, California and elsewhere. More regulation is coming. We, as experts in consumer psychology need to play a leading role in developing rules that are effective, but not unduly burdensome. Furthermore, we may need to do

this for issues that go beyond privacy. As MLK say, “privacy is becoming a flashpoint in the surveillance economy, yet the concerns causing the fire go well beyond privacy”.

References

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

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. United States: Brooks/Cole Publishing Company.

Benhabib, J., Bisin, A., & Schotter, A. (2010). Present-bias, quasi-hyperbolic discounting, and fixed costs. *Games and Economic Behavior*, *69*(2), 205-223.

Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy. an economic model for pricing personal information.* European Network and information Security Agency (ENISA).