In the United States, as well as in other countries, notice and consent mechanisms have become the predominant approach to consumer privacy protection. The implicit premise of such policies is simple and, at least superficially, compelling: Armed with information and control, consumers can make informed choices between different market offerings (from social networks to mobile apps) and manage their privacy in accordance with their individual preferences for privacy, without stifling innovation as a result of rigid regulation (FTC, 2012; The White House 2012). Extant research has suggested, however, that providing consumers with control does not guarantee that individuals will be able to use that control to make informed, self-interested, choices about data sharing; indeed one recent paper by two of the current authors showed that giving web-users more control encouraged them to share more information, in effect giving them more rope to hang-themselves through self-revelation (Brandimarte, Acquisti, and Loewenstein, 2012). Furthermore, and the main focus of the current paper, tools and options providing control may focus on irrelevant choices, be confusing, or be presented in a fashion that subtly but powerfully influences the consumer’s propensity to pick protective or transparent data sharing settings. For instance, across systems, services, and sites, choices surrounding sensitive collections of personal information may not be consistently presented to consumers as “privacy” choices. As a case in point, the choice to limit the use of personal information for advertising purposes is presented to Facebook users under the header of “Facebook Ads” (rather than under Facebook’s “Privacy Settings and Tools”). Similarly, on Android mobile devices, the options to limit the collection and use of location information are presented to users under the “Location Settings” header (not under “Privacy Settings”).

While those differences might seem inconsequential, findings from behavioral decision research have shown that subtle changes in a consumer’s decision frame (a decision maker’s conception of acts, outcomes, and contingencies associated with a particular choice) can significantly affect her actions.
(Tversky and Kahneman, 1981). Focusing on lesser studied but still common variations in the presentation of privacy choices, in this manuscript we investigate, and find evidence in support of, the prediction that consumer privacy decision making will be significantly impacted by subtle changes in decision frames induced by commonplace heterogeneity in the presentation of privacy choices.

We conducted three randomized experiments on Amazon’s Mechanical Turk in which we evaluated the impact on participants’ likelihood of selecting privacy protective options of altering (1) the label on privacy relevant choices, (2) the mix of high relevance and low-relevance choices, and (3) the accept vs. reject presentation of privacy relevant choices. We find that simply altering the decision frame of otherwise identical choices can have a substantial effect on individual choice. Changing the label of privacy-relevant choices from “Privacy Settings” to “Survey Settings” resulted in participants being 56% less likely to choose the privacy protective option. We also found that participants were approximately half as likely to select the privacy protective option for a high relevance choice when it was presented together within a set of low relevance choices. Finally, we found that participants were 51% less likely to select the privacy protective option when presented as a choice to allow a use of their personal information (allow frame) than when they were presented the objectively identical setting as a choice to reject a use of their personal information (prohibit frame). In all three studies presented in the paper, the set of choice frame manipulations evaluated were inspired by, and closely modeled on, the framing of privacy-relevant choices in existing contexts. The close modeling of our studies on real choice settings is intended to increase the relevance of the research findings for regulators, firms, and consumers.

This work contributes to the policy literature addressing emerging consumer privacy concerns and eliciting consumer preferences for privacy. The extant literature on consumer privacy decision making has traditionally modeled consumers as economically rational agents that make stable and consistent tradeoffs between the utility from data disclosures and privacy risks (e.g., Dinev and Hart, 2006; Fogel and Nehmad, 2009). However, a smaller but growing body of work has started to document some non-normative factors affecting people’s privacy decision making (e.g., Moon, 2001, Acquisti, John, and Loewenstein, 2012). This work contributes to this emerging stream of research and is, to our
knowledge, the first to highlight that control mechanisms, ostensibly aimed at improving consumer privacy, can themselves be fashioned in a manner that has a subtle, non-normative, and powerful influence on consumers’ propensity to pick protective data sharing settings. This suggests these mechanisms can introduce increased consumer privacy risk independent of consumers’ subsequent disclosure behavior (which has been the primary focus of prior studies; Brandimarte, Acquisti, Loewenstein, 2012). These control mechanisms are increasingly relevant in light of the ongoing shift towards indirect ways of collecting consumer personal information, not through overt requests for information (i.e. explicit consumer disclosures) but by, e.g., monitoring patterns of online browsing.

The central implication of this work is that providing consumers with greater control over privacy options may be a necessary but not sufficient policy mechanism to address privacy concerns, particularly in contexts in which firms have strong incentives to strategically leverage subtle manipulations of choice framing to solicit high rates of information sharing from consumers. These concerns are exacerbated if consumers fail to notice such subtle variation in the presentation of privacy relevant choices or significantly underestimate their impact on behavior. Such inadvertent and unaware susceptibility to framing effects is of increasing consequence to consumers, given the growing usage of personal information in commercial contexts, some of which may be particularly intrusive or even discriminatory. For instance, Sweeney (2013) finds that black-identifying names were 25% more likely to get an online ad suggestive of an arrest record relative to white-identifying names.

However, we caution that we cannot claim to know whether consumers are providing more or less personal information in the marketplace than is in their personal interest. What we can claim with greater confidence is that, if the goal of policy makers is to protect privacy, our findings suggest that the current trend in policy toward increasing choice and notification mechanisms may not necessarily achieve that intended goal. Alternative mechanisms should therefore also be considered, such as leveraging OECD fair information practice principles for baseline consumer protection against data practices perceived to be particularly intrusive or harmful. At a minimum, this could result in a more manageable set of privacy contexts that consumers are required to navigate, increasing the likelihood that they invest
in understanding the nuances and tradeoffs associated with the privacy choices presented to them. For firm data practices where choice is desirable (e.g. when significant benefit exists for consumers), additional protections could include designating uniform and consistent standards for presenting choice coupled with considerations of choice architecture (e.g. choice framing) that limit firms’ abilities to manipulate consumers in their own interests but instead empower consumers to make choices that reflect their desired balance of personal privacy and benefit from the collection and use of their personal information.

References


