The psychology and behavioral economics of privacy

Laura Brandimarte – Carnegie Mellon University

Privacy decisions are the result of remarkably complex trade-offs. The complexity of such decisions is due to a variety of reasons: from the fact that privacy is a multi-faceted concept, quite challenging – if not impossible – to define, to the fact that continuous technological developments have made privacy-related trade-offs increasingly hard to see and resolve; from the difficulties associated with the attempt to behave as rational economic agents, when it comes to decide whether and what personal information to disclose, to the limitations and biases that every human being is naturally subject to.

A vast literature[1] has analyzed privacy decisions from the neo-classical economics perspective as, essentially, a utility maximization problem subject to certain constraints. Again, a difficult problem, but not very different from other typical economic decisions, such as how much to save or consume, whether to buy a product from the closest store or to keep on searching for a more convenient price, and so on. I come from a different school of thought, one which values the theory of the economics of privacy, but at the same time finds it somewhat unsuccessful in predicting actual privacy related choices.

The psychology and behavioral economics of privacy is an emerging field of research that, borrowing theories and methodologies from behavioral decision research, aims at understanding what are both the rational (or normative) and the non-normative factors that affect actual privacy decisions of individuals living in an ever-changing, fast-evolving world.

Among my personal interests in this area is the relationship between perceived control over personal information and willingness to disclose. Imagine you are visiting a website and are required to provide several pieces of personal information in order to proceed. The benefits you will receive if you decide to provide that information is quite clear: consumption of online contents or services provided by the website you are visiting. Calculating the costs of this operation may, on the other hand, be quite challenging. While economic rationality would impose that you consider the actual source of the risk from providing such information – namely, who will then actually access it, how they will use it, and whether they will share it with third parties – you may be subject to what we call “the control paradox.” Because you are explicitly asked to provide that information, you feel in control of that information, and you are likely to provide it because you focus your attention on the control over its original release rather than over the actual source of the risk. Many online and offline transactions are similar to the one just described. As clearly shown by the reaction of the public to the Snowden’s revelations regarding government surveillance of both American and international citizens, people tend to be averse to “silent” collection of personal information. And yet, when explicitly asked, they may very well be likely to provide it.

These findings led me to the consideration that the approach of the US self-regulated industry, focused on providing consumers with control and notice as effective instruments for privacy protection, may not be sufficient. Control can backfire, because it may lead consumers to reveal more personal information in risky situations. Similarly, notice may not be enough to communicate the risks associated with information disclosure. Work by Lorrie Cranor and colleagues has shown that privacy policies used by in websites are, most of the times, not even read by users: privacy policies are overly long, written in legal jargon, and

1 Voluntarily omitting references to relevant literature throughout the abstract. Please contact me if interested in them (lbrandim [at] andrew [dot] cmu [dot] edu).

overall incomprehensible for the average user. But even if we were to find an easier way to explain privacy policies, they may still be ineffective, because the mechanism of notification does not take into account the limitations and biases we are subject to as human beings. In a study of notice effectiveness, we provided student participants with very simple, one-line notices regarding who would be able to access the information they decided to provide: either other students, or both students and faculty (a higher risk audience if the requested information concerns academic standings and integrity). While participants responded to this experimental manipulation as expected – that is, revealing less information if the audience included faculty – we found that small mis-directions can completely mute the inhibiting effect of notices. For instance, a simple 10-second wait between the showing of the notice and the actual point of disclosure nullified the effect. Imagine how effective notices can be on multi-tasking individuals, who are likely using more than one device at a time, are interrupted by phone calls, or distracted by other activities while they are trying to decide whether to provide their personal information to a website.

This line of research led me to conclude that notice and choice, the golden standard of industry self-regulation in the US, are not the answer to consumers' privacy protection: they are necessary but not sufficient conditions. Maybe notices would be more effective if they could be "experienced" rather than cognitively processed. And maybe the difficulties with online privacy decisions lie precisely in the lack of such "visceral," sensorial notices, notifications we can see, hear, or even smell. In the physical world, sensorial stimuli alert us of the presence of dangers, and we have learned how to interpret such signals and react accordingly. But in the online world we do not experience dangers in the same way, and the current state of the art in terms of notifications has been proven to be not always effective in all environments. In a series of lab experiments, we tested the hypothesis that detection of the presence of a human being in one's surroundings, via sensorial stimuli (visual, auditory or olfactory), increases privacy concerns, not only in the physical world, but with spillovers to the online world as well, thus decreasing willingness to disclose intimate personal information in an online survey. We found that, indeed, sensorial stimuli alerting us of the presence of a human being (as compared to inanimate objects) decrease our propensity to share personal information online: we tend to write about less intimate facts, to use less words, to spend less time writing, and to simply disclose lower number of individual thoughts.

In a separate line of research, I have investigated how personal information is interpreted by others once it is disclosed. On the one hand, I have been interested in how our past information, with positive or negative valence, is weighed against more recent information: is negative information discounted at the same rate as positive information, or rather is it discounted less? In a world where digital information is so easily retrieved, our past bad deeds can haunt us forever, while, we find, the good deeds are quickly discounted, to the point that they affect the impression others will form of us only if they are very recent. On the other hand, I have been studying whether this is only a temporary or generational phenomenon, something that will disappear as more and more people post negative (embarrassing or compromising) information about themselves. After all, who will have the courage to be judgmental about a picture showing a person being drunk if we all have similar pictures on our social media profiles? In a series of studies, we actually found evidence of the opposite phenomenon. People who disclose compromising information about themselves may experience a form of cognitive dissonance when called to express judgments about others who disclosed similar information. They want to distance themselves as much as possible from such compromising information, and one way to do that is precisely to be harsh toward others with similar disclosure behaviors.

There is much to explore about privacy decision making, and behavioral economics provides effective tools for such challenging quest.