Alessandro Acquisti Addresses ASIS&T Plenary Session

by Steve Hardin

EDITOR'S SUMMARY

During a plenary session of the 2014 ASIS&T Annual Meeting, Alessandro Acquisti explored aspects of online privacy and circumstances that heighten or relax our privacy concerns. Applying behavioral economics and considering our conflicting biases helps make sense of contradictory privacy decisions and behavior. Acquisti's research shows people surrender personal information for a small incentive but turn secretive when they know or suspect they are being observed. The personal information we readily post on social media can be easily collected and combined with other available clues to enable inferences with alarming breadth and accuracy. The need for social connection is precariously balanced with the desire for privacy. Acquisti further theorized an evolutionary link between perceived threat eliciting privacy concerns and our response to stimuli we interpret as suggesting the presence of others and potential risk. Though they may be subtle or hidden, such cues exist online, adding to the challenge of designing effective privacy technologies.

KEYWORDS

privacy

personal information

social web

Steve Hardin is reference/instruction librarian at Cunningham Memorial Library, Indiana State University. He may be reached at Steve.Hardin<at>indstate.edu.

People enjoy the connections made possible by the internet and the many social media applications it offers. But what are these connections doing to our privacy? Carnegie Mellon University professor Alessandro Acquisti addressed this situation during the second plenary session of the ASIS&T 2014 Annual Meeting in Seattle.

The decisions we make have economic consequences, Acquisti stated. When we search something on Google, we are selling some of our information.

We hear how someone hacks into a corporation's website and compromises customers' personal data. California was first to enact a breach disclosure law to force companies to reveal these attacks. The first reason for the law was to inform consumers – once there has been a breach, they can take action. But disclosure is costly. To avoid paying these costs, organizations can invest more in security and escape experiencing (and having to disclose) the breaches. Acquisti and his fellow researchers studied this situation and determined that laws that impose mandatory breach disclosures have resulted in a 6% reduction of identity theft.

Acquisti asked his audience to consider a Facebook user wondering whether he should discuss his sexual interests there. Maybe he will find a lover, but maybe his boss will see the posts. Most people do not decide rationally how much to disclose; they often use an emotional approach. A model of privacy decision making should include lessons from the behavioral economics of privacy and account for asymmetric information bounded rationality (we are not stupid, but we are not rational in the traditional economic sense either), as well as the cognitive and behavioral biases which may affect decisions.

In a 2013 study [1] Acquisti and his colleagues sent research assistants to a shopping mall where they offered people who completed a survey a $10 gift card, which they could use anonymously. Then the researchers waited 60 seconds and told participants about a $12 gift card – more valuable, but tracked. Participants were asked which card they would like. The researchers also created a second group in which subjects were given the tracked card first and then offered the untracked card second. Researchers found that in the first situation 52% of participants chose the untracked cards. In the second case only 9% chose the untracked cards. The results bring up a broader issue: How do we protect privacy when our world constantly encourages us to click items and surrender information?

In another study [2], Acquisti and colleagues did experiments in which they tried to manipulate the specific levels of control in transactions. They found that, paradoxically, more control can lead to less privacy. If people feel protected, they start taking more risks with their data.

How useful is transparency? Acquisti noted people do not read privacy policies, and if they do, they may not understand them. He and others did a study of Carnegie Mellon University (CMU) students [3]. They conducted a survey that included sensitive questions such as, "Have you ever cheated in class?" Some subjects were told that other students would see the answers; a second set of subjects was told students and faculty would see the answers. They found more persons answered the more sensitive questions when they thought only students would see their responses. However, this effect was nullified when a mere 15-second delay was inserted between the moment subjects were told who would see their answers and the moment subjects were actually asked to answer the questions. The effects of notices and transparency seem short-lived.

Acquisti has also investigated hiring discrimination via online social networks [4]. In the United States, it is risky for employers to ask interview questions about family status, religious orientation, political orientation or sexual orientation. However, many candidates put that information online. Employers say they use social media to gauge the professionalism of a candidate, although they do not say that they want to see, for example, whether a woman is pregnant. Thus, Acquisti and colleagues set up candidates who had the same professional information, but with vastly different Facebook profiles, and submitted their resumes to actual job openings in the United States. They found not too much difference in terms of callback ratios (that is, invitations to interviews) between gay and straight candidates. But for Muslims vs. Christians, fewer Muslims were being invited for interviews. It is not just what you publically put out about yourself; it is also what can be inferred from what you write.

Facial recognition software is getting better all the time. Acquisti and colleagues compared facial features on a dating site, and using facial recognition software they could identify one tenth of the people on the site [5]. Then they went further. Using photos and information from Facebook, within four attempts, they found the first five digits of 27% of subjects' Social Security numbers [6].

Advances in data accretion are continuing, Acquisti said. An anonymous face can be matched to a face from social media which can lead to a presumptive name which can lead to other information online which can lead to information that might be sensitive. Whoever is doing this process could overlay the information over the photo of a person. This process does not work quickly or correctly… yet. But algorithms keep getting better and better. In the next 10 or 15 years, inferences will keep getting more accurate. Acquisti asked his audience to consider a future in which we go around with Google glasses and know strangers' political affiliation and credit scores. Most people find that creepy.

There could be a backlash to all this information acquisition, but companies can become subtler. Acquisti discussed studies he is working on. Imagine that a company can see your Facebook wall and download a picture of your friend. The company could then create a product spokesperson using morphing to combine the features of your friends – because you act more positively toward that spokesperson who reminds you of them.

There is a paradox, Acquisti noted: people want connection, but they also want privacy. What if there is a deep psychological need for privacy and security? He made a conjecture: the need for privacy is as innate as the need for socializing and sharing. Then he made a hypothesis: if that were the case, "visceral" stimuli may elicit (unobservable) privacy concerns and reduce

CONTENTS
TOP OF ARTICLE
< PREVIOUS PAGE
NEXT PAGE >
NEXT ARTICLE >

(observable) privacy responses. He designed an experiment to investigate the hypothesis. He set up two rooms separated by a two-way mirror. Persons in one room were asked to type their sexual fantasies; some subjects were alone, but some had a guard behind them. The presence of the guard decreases how much a person is willing to write and reveal. In a second experiment, there is a noiseless fan in the room (control) and a confederate goes outside and does not interact in the second room. The decrease still happens. Another experiment checked olfactory stimuli. The researchers put oil of cloves in the control room and added a pheromone at undetectable levels for humans in the second room. They found again a decrease in willingness to reveal personal information when pheromones were added to the clove oil vial. Sensorial cues alerting us of the presence of other persons may affect our willingness to discuss sensitive and personal information by arousing privacy concerns.

Acquisti also outlined an evolutionary conjecture: our responses to threats in the physical world may be sensitive to sensorial stimuli signaling proximity and extraneous presences that we have evolved to use as cues of potential risk. So-called privacy concerns may be evolutionary by-products of those visceral responses. In cyberspace, the sensorial cues we evaluate to detect threats are absent, subdued or manipulated. This absence may help explain the paradoxical online/offline privacy behaviors – why it is so hard to protect privacy online and why the design of privacy and security technologies may need to consider visceral interventions.

Acquisti concluded that much can be inferred by what's out there about us.

People wanting more information can visit www.heinz.cmu.edu/~acquisti/economics-privacy.htm. They can also just Google or Bing economics privacy. ■

Resources Mentioned in the Article

[1] Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *Journal of Legal Studies, 42*, 249-274.

[2] Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347.

[3] Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). *Sleights of privacy: Framing, disclosures and the limits of transparency.* Paper presented at the SOUPS '13, New York, NY.

[4] Acquisti, A., & Fong, C. M. (2014). *An experiment in hiring discrimination via online social networks.* doi:10.2139/ssrn.2031979. Available at http://ssrn.com/abstract=2031979.

[5] Acquisti, A., Gross, R., and Stutzman, F. (2013). *Faces of Facebook: Privacy in the age of augmented reality [webinar slides].* Black Hat Webcast Series. Retrieved from http://marchiondelli.com/Blog/wp-content/uploads/2013/10/acquisti-face-BH-Webinar-2012-out.pdf

[6] Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *PNAS, 106*(27), 10975-10980.

CONTENTS
TOP OF ARTICLE
< PREVIOUS PAGE
NEXT PAGE >
NEXT ARTICLE >