Selected Papers of AoIR 2016:
The 17th Annual Conference of the
Association of Internet Researchers
Berlin, Germany / 5-8 October 2016

STRATEGIES OF INFORMATION DISCLOSURE

Nili Steinfeld
Ariel University

Abstract
How do users react when they are requested to provide personal information?

The paper presents findings from two experiments conducted in distinct online environments, in which users were presented with a trade offer from an unfamiliar research body: Access to their personal Facebook profile in exchange for a monetary reward. The two experiments illustrate and characterize several strategies employed by participants in response to the trade offer.

Literature Review
The Freemium model, the currently preferred business model for online services (Hoofnagle and Whittington, 2014), is based on free services which are often exchanged for personal information subsequently traded by the service provider. The model is, however, profoundly flawed: The service may be presented as free, but is effectively a trade of service for data, disguising users' information disclosure costs (Hoofnagle and Whittington, 2014), which are impossible to calculate for several reasons. First, information is different from other traded goods in that the value of a piece of information is subjective and difficult to calculate (Papacharissi and Gibson, 2011). Second, individuals requested to disclose information usually lack complete and relevant information about the market, which is needed to make a rational decision (Hoofnagle and Whittington, 2014). They are unaware of what will be done with the information they disclose, and when the information is being distributed to third parties, they are no longer part of the deal (Acquisti and Grossklags, 2005), even though the information, unlike other goods, remains linked to them (Papacharissi and Gibson, 2011), and they are still affected by the distribution of that information. In addition, the price of avoidance of participating in some social or commercial processes for reasons of privacy protection is sometimes high enough as to call into question how freely these choices are made (Nissenbaum, 2011).

Suggested Citation (APA): Steinfeld, N. (2016, October 5-8**).** *Strategies Of Information Disclosure*. Paper presented at AoIR 2016: The 17th Annual Conference of the Association of Internet Researchers. Berlin, Germany: AoIR. Retrieved from http://spir.aoir.org.

As a way to cope with the trend of personal information collection over the internet, security experts and privacy scholars advise users to lie at every opportunity (Fogarty, 2012; Jentzsch et al., 2012; Rosencrance, 2012). Users lie online for a variety of reasons, mostly related to identity play and presenting an ideal self (Caspi and Gorsky, 2006; Hooi and Cho, 2013; Ellison et al., 2012). But users also lie to protect their privacy and maintain boundaries between the offline and the online world, thus deception becomes a privacy protection, or privacy management strategy (Caspi and Gorsky, 2006; Page et al., 2013).

Research Aims and Methodology

In two distinct experiments, users of online environments were presented with a trade offer from a research body: Access to their personal Facebook profile in exchange for a monetary reward. One experiment took place in the online anonymous virtual world of Second Life, while the other was a panel survey conducted among a representative sample of Israeli internet users. The request and method were identical: In exchange for participants' compliance, they were offered a monetary reward in variable sums. To verify a successful connection, participants were requested to connect to Facebook from a website created for that purpose and linked from the survey, and permit access to the institute's Facebook application through their user profile in Facebook. Participants who refused to connect were asked to state the reason for their refusal. Options included "I wish to protect my privacy", or "I would login for a greater sum" (followed by a request to state the desired sum). The Facebook profiles of participants who allowed access were later inspected by the researcher, and profiles which were created on the same day of the experiment and presented no user activity were judged to be fake.

Findings

A review of the findings from both studies reveals several groups of users who employ different strategies in response to the trade offer, which undermines users' privacy and anonymity online.

Traders were participants who accepted the trade offer. Tendency to accept the trade offer correlates with the sum of money offered, and several other characteristics related to online habits and behavior. Men were also more willing to accept the trade offer in one experiment.

Abstainers, who rejected the trade offer, were mostly driven by their desire to protect their privacy, although a sub-group of abstainers, which may be referred to as **negotiators**, expressed their willingness to trade for a greater amount of money.

A third and most intriguing group are **deceivers**. Users in this group employed a strategy of "tricking the system," which allowed them to enjoy the benefits of the trade without paying the costs and risking their privacy. These users accepted the offer, but instead of trading with their authentic Facebook profile- they opened a fake account and logged in with the account made for the purpose of the trade. Most noteworthy with respect to this group is the overwhelming difference between the two environments in

the use of deception: While more than half of the profiles submitted by participants in the Second Life experiment were fake, not one of the profiles submitted by users in the general survey was judged to be fake. This difference between populations in the use of deception as a way to protect users' privacy suggests that the strategy of deception is the practice of digital savvy, and highly sophisticated and experienced internet users, such as users of Second Life tend to be in comparison with a general representative sample of internet users.
The paper explores the various strategies and characterizes users of each group. Moral consequences of deception as a privacy protection strategy are also discussed.

References

Acquisti, A. and Grossklags, J. (2005), "Privacy and rationality in individual decision making", IEEE Security and Privacy, Vol. 3 No. 1, pp. 26-33.

Caspi, A. and Gorsky, P. (2006), "Online deception: prevalence, motivation, and emotion", CyberPsychology & Behavior, Vol. 9 No. 1, pp. 54-59.

Ellison, N.B., Hancock, J.T. and Toma, C.L. (2012), "Profile as promise: a framework for conceptualizing veracity in online dating self-presentations", New Media & Society, Vol. 14 No. 1, pp. 45-62.

Fogarty, K. (2012), "Protect your online privacy: lie", PCWorld, March 1, available at: www.pcworld.com/article/251121/protect_your_online_privacy_lie.html (accessed July 12, 2012).

Hoofnagle, C.J. and Whittington, J. (2014), "Free: accounting for the costs of the internet's most popular price", UCLA Law Review, Vol. 61 No. 3, pp. 606-670.

Hooi, R. and Cho, H. (2013), "Deception in avatar-mediated virtual environment", Computers in Human Behavior, Vol. 29 No. 1, pp. 276-284.

Jentzsch, N., Preibusch, S. and Harasser, A. (2012), "Study on monetising privacy: an economic model for pricing personal information", available at: www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy (accessed March 3, 2013).

Nissenbaum, H. (2011), "A contextual approach to privacy online", Daedalus-US, Vol. 140 No. 4, pp. 32-48.

Page, X., Knijnenburg, B.P. and Kobsa, A. (2013), "What a tangled web we weave: lying backfires in location-sharing social media", Proceedings of the 16th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW), ACM, New York, NY, pp. 273-284.

Papacharissi, Z. and Gibson, P.L. (2011), "Fifteen minutes of privacy: privacy, sociality, and publicity on social network sites", in Trepte, S. and Reinecke, L. (Eds), Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web, Springer-Verlag, Berlin, pp. 75-89.

Rosencrance, L. (2012), "How online dishonesty protects your identity", NBC News, July 18, available at: www.nbcnews.com/id/48232403/ns/technology_and_science-security/t/how-online-dishonesty-protects-your-identity/ (accessed March 12, 2014).