Do-not-track as a driver for transparency of social networking advertisement practices?

Jens Grossklags
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA 16802

A number of different approaches have been utilized to monetize social network data and human capital. Least controversial are fan pages on social networking sites created by companies. Those efforts stimulate brand awareness, loyalty and foster a direct communication channel between a company and its potential customers. In a study of online retailers, about one-third self-reported that they maintained a Facebook page, 27% had a MySpace site and 26% created a presence on YouTube (Internet Retailer & Vovici, 2008).

However, the utilization of social network data for targeted advertisements is considered highly contentious. In a recent survey study, 66% of the surveyed adult Americans and 55% of the 18-24 year-old young adults prefer marketers to abstain from such efforts (Turow *et al.*, 2009). But behavioral and targeted advertisement is effective. 63% of the senior marketing executives report that it yields the greatest return on investment. At the same time, at least some companies are scaling back investments into related technologies as a result of consumers' privacy concerns (Ponemon Institute, 2010).

This reluctance can be explained given the state of the art of the marketing research literature: It is still hard to predict when consumers will *welcome*, *acquiesce*, or vigorously *protest* against new practices. Customers, who are burned once, may be twice as shy down the road to interact with marketers (Good *et al.*, 2005). Google and Facebook have weathered the storms that resulted from the release of Buzz and Beacon, respectively, but smaller content providers may not be so fortunate.

Indicators of consumer response may be delayed or subject to factors that are typically not accounted for in advertisement effectiveness studies. In our previous experimental work, we showed that consumers may regret their own decisions and feel betrayed even though they initially seemed to allow certain marketing practices and privacy invasions (Good *et al.*, 2007). Similarly, individuals' stated preferences may significantly differ from their eventual behaviors in marketing contexts (Spiekermann *et al.*, 2001). Related research contributes other puzzling revelations. For example, advertisements that are relevant to the website content *or* are obtrusive increase willingness to purchase. But a combination of these two factors is counterproductive (Goldfarb and Tucker, forthcoming). In another study, pop-ups were shown to increase brand awareness, but also

to reduce reservation prices (Acquisti and Spiekermann, forthcoming). These researcher groups speculate that certain practices may trigger consumers' feelings of *manipulation and deception* (Boush *et al.*, 2009).

Further, research fails to account for current practices utilizing social networking data in static and dynamic ways. In the former case, such data is frequently used as endorsements in advertisements on unrelated sites (including offline marketing efforts). New campaigns (including HP's) often include comments from Twitter and Facebook in rich banner ads (Dilworth, 2010). In the latter case, Facebook's new social plugins push user data to a wide variety of websites to offer *instant personalization* (Gannes, 2010).

It is reasonable to assume that consumers are neither fully aware of different advertisement trends nor completely understand the different means and ways of how their data is collected, shared and eventually utilized (Stein, 2011). One potential response is to aim for a higher degree of *transparency* with respect to advertisement practices involving social data.

The proposed Do Not Track Me Online Act of 2011 (H.R. 654) would not only give consumers a measure of control over data treatment, but also calls for entities that are affected by the new law to disclose their practices for collection and sharing, including the identities of data exchange affiliates. And, in anticipation of regulatory changes at least one major advertisement intermediary has started a pilot project to improve transparency and relevance (Wilson, 2011).

It is less obvious whether these trends will lead to more meaningful options for consumers and choices by consumers.

First, in the short term, the plethora of potential do-not-track implementations is likely not going to converge on a simple and effective market standard. Yu's (2010) discussion of design choices clearly highlights the problems ahead. On the one hand, the technical details of implementations can severely thwart the real-life impact of do-not-track. For example, different ways to aggregate externally provided blacklists for overly aggressive marketers in the browser can appear unintuitive for the consumer and even technologists (Clarke, 2011). On the other hand, conceptual problems are in need to be tackled by researchers. In particular, the trade-off between simplicity (e.g., a binary on/off choice) and fine-grained preference management is challenging from a variety of perspectives as evidenced by the discussions around privacy management, e.g., in the context of the Platform for Privacy Preferences (Cranor *et al.*, 2002).

Second, given the concentration in the advertisement industry one has to carefully observe whether the given data management options translate into meaningful consumer choices. The idea of do-not-track is inspired by regulatory efforts that are considered highly successful from a consumer protection perspective such as the do-not-call registry (Varian *et al.*, 2005). But the achievements of the do-not-call registry do not only rely on its simplicity (including the semi-permanent nature of telephone numbers) but also on the dynamics of the interactions that are concerned. Specifically, it mainly addresses unsolicited calls within the confines of the privacy of the home while consumers are engaged in their *private unrelated affairs*. In contrast, do-not-track is closely tied to interactions that are initiated by the consumer and deeply embedded in popular activities such as partaking in a social network, shopping on an ecommerce site, or information

gathering on news outlets. Companies offering these requested services have a reasonable expectation to benefit from their offerings. And consumers may feel constrained in their effective choices when they are related to services with strong network effects or market dominance. Further, these impediments will likely influence consumer behavior also on sites that do not fit these criteria.

Do-not-track will lead to more transparency in the advertisement industry, whether through regulatory actions or industry-guided efforts. However, research needs to be undertaken to understand whether this trend will help to overcome consumer privacy hurdles.

References

A. Acquisti and J. Grossklags, Privacy and rationality in decision making. *IEEE Security & Privacy*, 3(1):24–30, 2005.

A. Acquisti and S. Spiekermann, Do Pop-ups Pay Off? Economic effects of attention-consuming advertising, *Journal of Interactive Marketing*, forthcoming.

D. Boush, M. Friestad, and P. Wright (2009) *Deception in the marketplace: The psychology of deceptive persuasion and consumer self protection*, Routledge, New York, NY.

G. Clarke, Microsoft: IE9's web privacy hole? A feature, not a bug - When do-not-track lists clash, The Register, March 18, 2011.
http://www.theregister.co.uk/2011/03/18/microsoft_ie9_tpl_site_blocker/

L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, April 2002.
http://www.w3.org/TR/P3P/

L. Gannes, Facebook: The Entire Web Will Be Social, GigaOM, 2010.

A. Goldfarb and C. Tucker, Online Display Advertising: Targeting and Obtrusiveness, *Marketing Science*, in press.

N. Good, R. Dhamija, J. Grossklags, S. Aronovitz, D. Thaw, D. Mulligan and J. Konstan, Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware, *Proceedings of the Symposium On Usable Privacy and Security (SOUPS 2005)*, Pittsburgh, PA, July 6-8, 2005, pp. 43-52.

N. Good, J. Grossklags, D. Mulligan, and J. Konstan, Noticing Notice: A large-scale experiment on the timing of software license agreements, *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'07)*, San Jose, CA, April 28 - May 3, 2007, pp. 607-616.

Internet Retailer & Vovici, 2008. Emerging Technologies. Market study.

Ponemon Institute, 2010. Fear and Loathing in Online Advertising, Research Report.

S. Spiekermann, J. Grossklags, and B. Berendt (2001) E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior, *Proceedings of the Third ACM Conference on Electronic Commerce (ACM EC'01)*, pp. 38-47.

J. Stein, Data Mining: How companies now know everything about you, *Time*, March 10, 2011. http://www.time.com/time/printout/0,8816,2058114,00.html

J. Turow, J. King, C. Hoofnagle, A. Bleakley and M. Hennessy, Americans Reject Tailored Advertising and Three Activities that Enable It, University of Pennsylvania and University of California, Berkeley, report, 2009.

H. Varian, G. Woroch and F. Wallenberg, The demographics of the do not call list. *IEEE Security and Privacy*, 3(1):34-39, 2005.

D. Wilson, Yahoo launches a transparent advertising scheme: Claims it's a better consumer experience, *The Inquirer*, March 18, 2011. http://www.theinquirer.net/inquirer/news/2035321/yahoo-launches-transparent-advertising

H. Yu, Do Not Track: Not as Simple as it Sounds, *Freedom to Tinker (Blog)*, Princeton University, August 10, 2010. http://www.freedom-to-tinker.com/blog/harlanyu/do-not-track-not-simple-it-sounds