Consentful Surveillance: Supporting User Understanding and Control

Richard Gomer
Electronics and Computer Science
University of Southampton
Southampton, SO16 7FB, UK
r.gomer@soton.ac.uk

m.c. schraefel
Electronics and Computer Science
University of Southampton
Southampton, SO16 7FB, UK
mc@ecs.soton.ac.uk

Abstract
Surveillance and surveillance-like practices are common on the free web services that we use. We argue that, although such practices can provide value to users, they should be done 'consentfully' as a way of empowering individuals and applying consumer preference to the market. Our research on this subject raises some key challenges for interaction designers and researchers to address: explanations, timing, and measurement.

Introduction: The Grey Web
Under the surface of the web-based content and services that we use every day is a largely invisible network [3] of advertisers, data brokers and analytics companies, "The Grey Web" [4]. The "trackers" that make up the Grey Web are able to track individual users through a variety of mechanisms such as browser cookies or fingerprinting [6], and to use the information that they gather about the users' web browsing history, possibly combined with information from other sources, such as social networking profiles, to create rich profiles of individual users; embodying Clarke's so-called "dataveillance" [2].

As an example of a modern commercial surveillance network, the Grey Web provides an opportunity to examine issues of surveillance more generally.

Consent & Consentfulness
The use of everyday surveillance, by or in conjunction with commercial organizations, *does* offer some value to end users, through better personalization and better insight into, for instance, their own health or behavior. Although surveillance in an adversarial context such as security is not typically conducted with the consent of the surveillee the same does not seem to be desirable of surveillance in other broader contexts. Our position is that as surveillance diversifies into new areas and

forms, there is a pressing need to do so with surveillees' *meaningful* consent. Gaining such consent is important from a values-based desire to empower individual consumers, to allow informed consumer preference to act as market force on service development and, from service providers' own perspective, in order to foster user trust in, and adoption of, new platforms and technology. The importance of consent is reflected in existing privacy and data protection regulation [8] [1].

'Consentfulness'

As a means to think about the role of consent, we propose the notion of "consentfulness"; conceptually the (inverse) degree to which a fully-informed user would choose to *undo* a particular data collection or processing practice – for instance surveillance. This could be as a result of *surprise* (at its mere existence, or at its consequences) or because inadequate control over the practice was given to begin with.

Consentful Surveillance

Today, user consent to tracking practices is typically claimed on the basis of disclosures made through devices such as privacy policies, cookie notices and terms and conditions. However, we have seen in our research that most users are unable to infer the consequences of data collection and processing by service providers, and in many cases even what is entailed by the practices themselves, based on the information provided by service providers [5].

Consentful interactions must, by definition, be intelligible to the user, and controllable. However, surveillance seems to raise a third key challenge to HCI: *Visibility*; the ability of surveillees to know *if* and *when* surveillance is taking place.

The Web Mirror

To probe user understanding of web surveillance, to improve its visibility, and to begin developing a model of how to enable consentful surveillance, we built the Web Mirror (http://mirror.websci.net/). The Web Mirror embodies many of the concepts of a "privacy mirror" [7] and reflects back to users both the extent of surveillance in their own web browsing, and the possible identities that different surveillants could have created for them.

Key Challenges

Based on user-centered research using the Web Mirror, we offer three key interaction challenges around consentful surveillance:

We need to **better explain** surveillance practices to users; explanations grounded in technical implementation details ("cookies", "pixels") do not help users to reason. Good explanations would allow the user to *relate the surveillance to their own concerns*; concerns that are often specific and based on individual social and cultural context.

We need to offer explanations, and control opportunities, at **the right time**. User inattention, of focus on a more important task, potentially leads to users making non-consentful decisions.

Finally, we may be able to develop instruments to **measure consentfulness** empirically for use as a quantifiable design metric; offering the ability to iteratively improve the consentfulness of a system as we would with reliability or performance.

Acknowledgement

Our work is supported by Research Councils UK via the *Meaningful Consent in the Digital Economy* Project; grant reference EP/K039989/1.

References

[1] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting.* 2014.

[2] Clarke, R. Information technology and dataveillance. *Communications of the ACM 31*, 5 (1988), 498–512.

[3] Gomer, R., Rodrigues, E.M., Milic-Frayling, N., and Schraefel, M.C. Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies through Search. *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, IEEE (2013), 549–556.

[4] Gomer, R.C., Milic-Frayling, N., and Schraefel, M.C. *The Grey Web: Dataveillance Vision Fulfilled through the Evolving Web.* 2014.

[5] Marreiros, H., Gomer, R., and Tonin, M. Exploring user perceptions of online privacy disclosures. *Proceedings of 14th International Conference on WWW/INTERNET 2015*, IADIS (2015).

[6] Mayer, J.R. and Mitchell, J.C. Third-Party Web Tracking : Policy and Technology. *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, (2012), 413–427.

[7] Nguyen, D.H. and Mynatt, E.D. Privacy Mirrors : Understanding and Shaping Socio-technical Ubiquitous Computing Systems. (2002), 1–18.

[8] *DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* European Union, 2009.