Taking Control of the Panopticon: Privacy Considerations in the Design of Attentive User Interfaces

Jeffrey S. Shell
Human Media Lab &
Surveillance Project
Queen's University
Kingston, ON K7L 3N6
Canada
shell@cs.queensu.ca

Introduction

Although we all have a strong sense of privacy, researchers and theorists have had a tough time agreeing on a precise and workable definition. Part of the problem is that privacy has different meanings in different contexts to different people. Clarke defines privacy most generally as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations" [1,2]. In practice, privacy can be described as a negotiation of interests between individuals, groups of individuals, and organizations [1,2]. In the context of digital devices and ubiquity, the interest of individuals is in ensuring 'informational privacy', which can be defined as the combination of communications and data privacy [1,2]. As designers, we must consider the impact of our design decisions on the members of the public who use our systems, and, at the same time, we must listen to those who spend their careers studying these issues. As social scientists, we must continue to make sure that the issues we are discussing are topical, and have a minimum amount of subject specific lingo so we can speak to, rather than about, the development and implementation of emerging technologies. By bringing together designers and social scientists to develop a common mission and vocabulary, consumers will benefit by having access to products and services more friendly to their interests, easing the transition to ubiquity.

Competing Interests

Individuals using technology want both to engage in quick, efficient transactions to complete accounting style tasks and to feel safe and secure with the ownership of information exchanged in this process. Traditionally, we have given a wealth of information to various institutions, such as banks and insurance companies, without concerning ourselves with the details of how this information will be recorded, or whether it will be sold to third parties. Recently, due to many well-documented violations of consumer trust (e.g. Doubleclick, amazon, Lotus [3]), we are increasingly sceptical of how information about us is handled, and often feel more secure when the organizations we deal with are certified by third party consumer privacy advocacy groups. One of the principle differences in our relationship with these organizations is the dominance of the spaces of flows, over the spaces of places [4]. Accountability is no longer tied to physicality – transactions are processed over the telephone from call centres, or over the internet in an electronic, disembodied form. Because corporations are larger and more detached from consumers, they engage in aggressive market research to understand prospective clients. In order to keep in touch with consumers to understand

their needs, to provide access to relevant products and services, organizations create profiles of users. Individual profiles have been traditionally assembled using factors such as home location and income. Because consumers are often treated in accordance with their constructed profiles, they are often called the 'data doubles' of consumers. The information used to constitute 'data doubles' is no longer based on transactions. It is now also based on interactions – how we surf the web, who we talk to or associate with in which chat rooms and newsgroups. Information transmitted and acquired in these less formal interactions is often what users report feeling least comfortable about. Users have a desire to be presented with products and services which they may be interested in, and not explicitly conscious of, analogous to shopping in a mall designed to cater to the users' interests and price range, but they are not comfortable with the flows of data required to create these personalized shopping arenas.

Autonomy

Because privacy has many different meanings in many different contexts to many different people, it is useful to think of the effects of profiling and data doubles in terms of the clearer concept of personal autonomy [5]. How has the automated social sorting affected our opportunities to make informed decisions over who to buy from, and what to buy? The process of constituting our data doubles is remote and secretive and it determines the stream of products we are exposed to. The specialized, direct marketing products and services we streamed has arguably made us subjects, rather than active participants in the marketplace. Can we truly consider ourselves informed consumers in this environment? If we choose from what we are shown, we negate the benefits of our access to a global market of varied goods. We give our business to those who are most successful at gathering our personal data and converting it into the most accurate data doubles.

The Panopticon

In the late 18th century, to improve the efficiency of prisons, Jeremy Bentham developed panoptic design. In a panopticon, as the name implies, everything is visible in one view from everywhere. Bentham used this technique to affect social responses. By hiding prison guards in tall inspection towers, and building one-way observation systems, prisoners assumed that they were always being observed by prison guards. Therefore, they adjusted their behaviour regardless of whether they were being monitored, reducing the need for actual prison guards [8]. This automated the disciplinary system, coercing micro policing among prisoners. This is an early example of what we now call risk management, a process in which actuarial style decision making practices based on probabilities, and assumed cost of failure, dominate decision making. Although there were fewer prison guards, and their collective ability to cope with altercations was lowered, the probability of an incident requiring intervention was greatly reduced. The net result is a gain in operational efficiency and effectiveness of the prison. Foucault revisited the concept of the Panopticon in the mid twentieth century. At this time, from his perspective, the power of the central authority of nation states had extended itself to stifle individual autonomy and freedom of action [6]. Recently, Mark Poster has extended the concept of the Panopticon to apply to the information technology revolution [9]. Large databases are utilized to apply risk management processes to governance,

crime prevention and marketing, judging people and affecting their opportunities, often without their knowledge or consent. This Superpanopticon, like Bentham's prisons, has the ability to affect our behaviour. We all know that we have centralized and shared credit reports, which constrain and regulate our financial opportunities, but yet we have little control over what information they obtain, and how they use this information to rank us.

Attentive User Interfaces

Attentive User Interfaces aim to recognize a user's attention space in order to optimize the information processing resources of user and devices. This is accomplished by measuring and modeling the users' past, present and future attention for tasks, devices or people. Key features of AUIs include:

1) *Sensing attention*: By monitoring users' physical proximity, body orientation and eye fixations, AUIs can determine what device, person or task the user is attending to.
2) *Reasoning about Attention*: By modeling user attention, AUIs can estimate task prioritization and predict attentive focus.
3) *Graceful Negotiation of Turns*: Before taking the foreground, AUIs a) determine whether the user is available for interruption given the priority of the request; b) signal the user via a non-intrusive peripheral channel; c) sense user acknowledgement of the request.
4) *Communicating Attention*: To encourage efficient turn taking AUIs communicate their attention to users, and communicate the attentive focus of the user to other AUIs and remote people that request the user's attention.
5) *Augmenting Attentive Resources*: Analogous to the Cocktail Party Effect, AUIs may optimize the use of the user's attentive resources by magnifying information in the estimated focus of user activity, while attenuating peripheral detail.

Attentive User Interfaces are aware of both the context in which the user is operating her digital device and the presence and attention of the user outside of this interaction, in her non-mediated environment. They are personalized and automated assistants that help the user manage information overload by regulating their attention space, attenuating unimportant distractions and interruptions as part of a holistic approach to improving the quality of interactions with digital devices in the context of ubiquity [10].

A Little Technological Determinism

Computers are everywhere. They are imbedded in virtually every device with which we interact. They are wireless, they are fast, they are invisible and they are even making their way into our appliances. They also are unaware of what we are doing, and how we're doing it. Computers *will* become aware of these issues in order to be more usable. They need to understand, one way or another, what is occupying our attention, and whether we are willing to be interrupted, what it will take, and how they should do it. It is not unreasonable to proceed under the assumption that Attentive User Interfaces are on their way. They will initially be used by wealthy, computer enthusiasts, and like mobile phones, will proliferate across most groups to enable them to manage conflicting demands on their attention.

Gatekeeper versus Facilitator

Based on our design decisions, Attentive User Interfaces can either exacerbate the panoptic effect and widen the scope and net of surveillance, or give us an opportunity to take control of informational privacy, and manage our own data doubles. An Attentive User Interface (abbreviated AUI), is not only going to contain information as to what purchases we made, and where we surf when a particular cookie is active. It will know when, how, where and what occupies our attention in both mediated and non-mediated worlds. It will know our buying preferences, our affiliations with organizations, and who our friends and foes are. It will know exactly what our priorities are, and how we like them sorted. AUIs will also have information about what is accessible to whom within our households, including private files and secrets that we keep from each other within our family. Who we talk to and when we talk to them will be recorded to inform future prioritization of the caller. This could potentially be used to conduct surveillance on each other within the household. If we provide privacy controls on information within the household and among the family, restricting access to a resource can imply deceitfulness. In short, the surveillance required to facilitate such a system can produce accurate data doubles based on much more personal information than the current database and cookie enabled systems, and could affect interpersonal dynamics among friends and family.

If we design AUIs to serve as local surveillance systems that keep the information repository local, then we can benefit from improved communication among ubiquitous devices that respond to our attention without sacrificing informational privacy. These systems can be our own personalized information facilitators that will accommodate our needs and preferences to improve our interaction with technology. If we are worried that our external communication will be monitored by our service providers, we can also include the facility to trick these systems by making queries we are not interested in during offline time, such as when we are eating a meal, taking a bath, or sleeping. Control of our external data double can finally be in our hands. Our personal AUI will make requests, actively engaging the useful resources, rather than passively being subjected to personalized direct marketing information streams. However, if our AUIs are stored and managed externally, the resources that pop up will certainly be relayed with more than our own interests in mind. AUIs and similar systems have great potential to gather both transactional and interactional information to construct externally managed personal profiles. Therefore, rather than being information facilitators that act solely on our behalf they might be information gatekeepers with motives that differ from simply improving the quality of our lives with and among technology. This would produce a panoptic effect in which we would adjust our behavior on the assumption that we are always monitored by external interests.

We must be conscious of how access restrictions will affect our interpersonal relationships, by conducting experiments on prototypes, situated within a household. We should strive for ecological validity so we learn about how these systems will be really be used, not just how we think they will be used, and what the impact of their use might be. This will be very important research that will require social scientists to conduct properly. Designers must partner with social researchers to make use of the wealth of knowledge they possess and social scientists must continue to take an active role in the development

of new technology, in order to influence and improve technologies that are changing the way that we live.

References and Important Works in the Field

1. Clarke, R. Introduction to Dataveillance and Information Privacy, and Definition of Terms. ANU. http://www.anu.edu/people/Roger.Clarke/DV/Intro.html, 2002
2. Clarke, R. Information Technology and Dataveillance. Communications of the ACM, 31, 5, 1988, pp. 498-512
3. Clarke, R. Why Would M-Marketing be Trusted by Consumers and Small Enterprises ??. http://www.anu.edu.au/people/Roger.Clarke/EC/AMTA01.ppt, AMTA Congress, Sydney, 27 February 2001
4. Castells, M. 1996. The Rise of Network Society. Oxford: Blackwell
5. Lyon, D. 1994. The Electronic Eye – The Rise of Surveillance Society. Minneapolis: University of Minneapolis Press
6. Rule, J. 1996. High-Tech Workplace Surveillance: What's Really New? In Lyon and Zureik (ed.) Computers, Surveillance & Privacy. Minneapolis: University of Minneapolis Press
7. Perrolle, J. 1996. Privacy and Surveillance in Computer-Supported Cooperative Work. In Lyon and Zureik (ed.) Computers, Surveillance & Privacy. Minneapolis: University of Minneapolis Press
8. Lyon, D. 2001. Surveillance Society – Monitoring Everyday Life. Philadelphia: Open University Press
9. Poster, M. 1995. The Second Media Age. Blackwell Great Britain: Polity Press
10. Shell, J., Selker, T, Vertegaal, R. Interacting With Groups of Computers. In Special Issue on Attentive User Interfaces, Communications of the ACM 46(3).
11. Bellotti, V. and Sellen, A. Designing for Privacy in Ubiquitous Computing Environments. in Proceeds of ACM Conference on Computer-Supported Cooperative Work ECSCW '93, Milano, Italy.
12. Dourish, P. Culture and Control in a Media Space. in Proceeds of ACM Conference on Computer-Supported Cooperative Work ECSCW '93, Milano, Italy.