Developing for Privacy: Civility Frameworks and Technical Design

Mark S. Ackerman
Computing, Organizations, Policy, and Society
Information and Computer Science
University of California, Irvine
Irvine, CA 92697 USA
ackerman@ics.uci.edu
http://www.ics.uci.edu/CORPS/ackerman.html

The Sunday Boston Globe of January 30, 2000 was very representative of current newspapers. In addition to the usual mayhem, fires, weather, traffic accidents, and sports, the newspaper contained a number of Internet related stories, all roughly on a similar topic. A page one story discussed Internet gambling. Even though it is illegal in US, Internet gambling has merely moved offshore. Another story reports the widow of Frank Malina, an artist, has been sued over the word "Leonardo." Malina founded an academic journal called "Leonardo" in 1968, but a French corporation is claiming trademark damages because the journal shows up in Web searches for their site "Leonardo". Another story tells people how to avoid auction scams on e-bay and similar Web sites.

Even Miss Manners, an etiquette column, wades in. Judith Martin, its author, admonishes people not to spread idle gossip in Internet forums. She notes: "Where once people could count on mobility as a way of escaping disapproval, cyberspace gives them nowhere to hide. [Martin 2000]"

All of these stories are recent indications of the changing geographical nature of our social space. These issues have been revisited again and again through history. Taxation in the 13th century meant that tax collectors needed to distinguish all of the John's in a parish and brought a requirement for last names. The growth of urban areas in the 19th century brought the threat of large-scale fires, and the requirement that fire departments be organized and be able to quickly find urban buildings. This brought the standardization of street names and address. (Standardization for other urban services, such as mail, was also important, but fire was critical.)

One of the changes, present only in the Boston Globe on page F8 in a story about DoubleClick, is privacy. Today, the ability to collect personal information across many different boundaries - organizational, institutional, and geopolitical - has grown to a crisis. (Perhaps the key indicator of this crisis is that the public actually is beginning to be concerned about its privacy.)

Privacy is a lead indicator of many future issues. To understand the effect of current technologies on privacy, we need to step back and examine some underlying social issues. These social issues suggest certain technical steps are extremely important.

Civility and the new technologies of the Internet

As has occurred in many periods of social change, a new civility is being forged. The term "civility" has an old-fashioned air, connoting antiquated etiquette, manners, and politeness. However, by "civility", I mean merely understanding the reciprocating set of social connections that binds an individual to his or her social groupings and vice versa. All social-historical situations have their own form of civility.

It can be argued that technology and civility are deeply intertwined. On one hand, technology affects civility in two ways. First, technology allows new possibilities for social activities. The railroad in the US nineteenth century brought additional food to cities, and allowed them to grow. The railroad also brought additional mobility, and increased the economic umbrella of specific cities. (For example, Columbus Ohio became the financial center for southeastern Ohio, and therefore continued to grow at the expense of similarly sized cities.) For individuals, their use of technology, by technology's changing of the basic infrastructure of social (as well as political and economic) interaction slowly affects the social structures surrounding the technology's use. A second effect of technology on civility is that technology increases the scope of geopolitical regulation. Railroads brought a larger need for national regulation of key industries that had expanded past the ability of states to regulate them. With the new communication devices in the late nineteenth century, organizations could become national. The federal government also increased its scope. For an individual, it is important to note, technology brings new possibilities, freedom, and mobility, but it also dissolves traditional social structures that permit the individual to judge what will happen socially and to expect whatever form of justice is required.

On the other hand, civility is not formed merely by technology. Technology is formed by the social and political expectations of its designers and users. Kling [1991] pointed out that financial systems and by extension other computational systems, reflect political value orientations "...each resting on its own assumptions about which social goods should be maximized... (p. 427)." Kling identifies the private enterprise, statist, libertarian, neo-populist, and systems models. Designers take these ideological models and necessarily incorporate them into their designs. Moreover, all of the various stakeholders in a computerization project incorporate these political stances into the design of the entire social-technical system.

Political ideologies, then, underlay both technology development and changes in civility. One could argue, in fact, that crystallizations in civility are connoted by political labels – for example, Whigs in the 18th Century, Know-Nothings in the 19th, Socialists in the 20th, Greens in the 21st.

As noted, privacy, as protection of oneself, is part of civility. One can argue whether privacy is an inalienable right or to stretch an example, a privilege conferred by an all-powerful divine monarchy. In any case, the possibilities for privacy (and indeed the assumptions underlying its social definition) is clearly dependent on the ideological stances possible within that society.

Privacy within the current US civility

Any privacy technology for US use must exist within the US' combined private enterprise and libertarian model. This model usually promotes corporations over individual citizens, removes government from a central social control position, and relegates social obligations to the sidelines.

If one accepts that liberal or leftist ideological regimes within the US are difficult or impossible

to instantiate within regulatory structures, then as such, two issues are critical: Individuals need knowledge in the markets for their private data, and they need technical help in fending for themselves. One might argue whether this is best privacy environment, and indeed it is not. The argument here is merely that these capabilities are needed within the current US political environment. In detail, these two issues are:

- *Providing sufficient information to individuals about their privacy concerns.* Some mechanism needs to be provided to tell individuals what is being requested (or taken) and the effect of that provision. The Platform for Privacy Preferences Project (P3P), a World Wide Web Consortium proposed protocol, is one such effort to provide this information.[1] While some privacy advocates misdiagnose P3P as leading individuals into selling their privacy, it could also be argued that P3P provides individuals with labeling information that is not obtainable today. P3P reduces or eliminates the current non-symmetric barter for private information - the individual can at least determine what is desired and what will be done with the data. P3P does this by labeling Web pages with metadata about the data requested and the actions taken with that data.
- *Providing help in determining what to do with that labeling information.* Relatively few people will understand the full implications of data transfer; this is especially true as the Web world begins. A new civility, with shared assumptions about social obligations and relationships, will take some time to come together. In the meantime, however, it is necessary to provide people with some tools that allow them to weigh the truthfulness and the consequences of privacy statements.

Below I describe some potential intelligent agents that can help consumers. The discussion below summarizes Ackerman and Cranor [1999].

Privacy critics

Currently Internet users do not know how information they release online will be used. Unfortunately they have little choice but to provide data; users who wish to engage in electronic commerce must often release personal information to complete transactions.

Users could benefit from systems that assist them in identifying situations where their privacy might be at risk. *Privacy critics* are agents that help users protect their privacy online. These critics currently work with P3P, but any other labelling protocol would work.

Critic-based architectures were first introduced by Fischer et al. [1990]. A critic, as a type of intelligent agent, provides feedback and suggestions as users go about their ordinary tasks. For example, the HYDRA critics [Fischer et al. 1993] provided design feedback for kitchen architects as they laid out kitchens.

Two features of critics are important to this discussion. First, critics provide only feedback to users - they do not take action on their own. Privacy critics would help (rather than attempt to automate) the user's control over private information. Critics might offer suggestions or warnings to users, watching over their shoulders as they go about their normal Web-based business.

Second, a critic-based environment might have hundreds of different critics. Each critic would check on a different facet of a problem domain and user goal. The independent nature of numerous critics allows an ecology of critics, from many different vendors or sources. This allows users to mix types of protection and protection levels. Users are, of course, free to turn these critics off and on, set threshold levels, and decide what aspects of privacy they wish to guard most closely.

Sample privacy critics

Privacy critics, then, are agents that watch the user's actions and make privacy suggestions. We have implemented prototypes of six sample critics; two are presented here. These six are merely the beginning of what can be done.

The first critic checks a simulated CyberPrivacy Advocacy Group's database for consumer complaints about a Web site. This critic assumes a number of third-party databases collecting claims or problems about different kinds of sites. For example, a Better Business Bureau database could report that sites have had privacy complaints against them; other databases might report sites participating in data scams. This critic does not currently learn to categorize sites or learn about user preferences; these would be potential extensions.

The second critic watches the type of information being released and warns users when a P3P proposal requests data elements that can be used in combination to identify the user. For example, many consumers do not appear to know that specific demographic data (e.g., race, birth date) can be used with zip code to uniquely identify individuals or households.

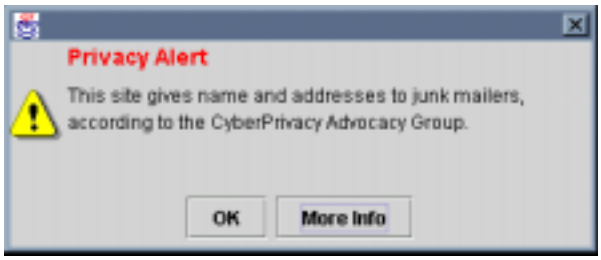

Figure 1: A privacy critic that warns users about data scams.

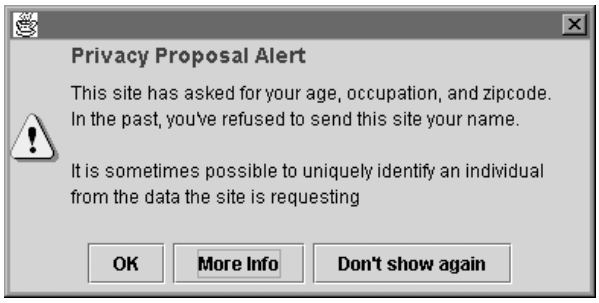

Figure 2: A privacy critic that warns users about giving away data that can be assembled into identifying data.

Conclusions and future work

To be completely effective, current browsers must support privacy critics by opening up their "trust" engines, whereby decisions are made on behalf of the user. However, privacy critics are quite simple to implement (even as client proxies), and therefore their introduction can be easily staged for users. Current research includes the necessary support services for these critics within a user environment and the types of metadata that would usefully augment P3P statements for the user.

As an important caveat, this work considers only the current ideological regimes in constructing aids for individuals' privacy. Certainly, other regulatory, technical, and political initatives are needed for full privacy protection. Nonetheless, within the present regulatory and political constraints, privacy critics offer important assistance to users.

References

Ackerman, Mark S., and Lorrie Cranor. 1999. Privacy Critics: UI Components to Safeguard Users' Privacy. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'99)* : 258-259.

Cranor, Lorrie, and Joseph Reagle. 1998. The Platform for Privacy Preferences. *Communications of the ACM*.

Fischer, Gerhard, Andreas C. Lemke, Thomas Mastaglio, and Anders I. Morch. 1990. Using Critics to Empower Users. In *Proceedings of ACM CHI'90 Conference on Human Factors in Computing System:* 337-347.

Fischer, Gerhard, Kumiyo Nakakoji, Jonathan Ostwald, Gerry Stahl, and Tamara Sumner. 1993. Embedding Computer-Based Critics in the Contexts of Design. In *Proceedings of ACM INTERCHI'93 Conference on Human Factors in Computing System:* 157-164.

Kling, Rob. 1991. Value Conflicts in the Design and Organization of EFT Systems. In *Computerization and Controversy* (Edited by C. Dunlop and R. Kling): 421-435. Boston: Academic Press.

Martin, Judith. 2000. Gossip poison in cyberspace. *Boston Globe*, January 30, 2000, C8.

[1]P3P allows Web sites to make statements ("proposals") about their privacy policies and request data using a standardized vocabulary and protocol. See [Cranor and Reagle 1998] for more information.