Privacy in the Global e-Village

Gregory J Pottie

Citizens of industrial nations have long become resigned to having large quantities of personal and financial information compiled by governments, insurance companies, medical practitioners, and financial institutions. Lately we have become familiar with the profiling performed in every on-line transaction, with many people growing concerned with how this data might be shared among different commercial and governmental entities. Whereas correlation of data stored in filing cabinets was a monumental and costly task, the ease of sharing electronic data over the Internet has motivated companies and governments alike to break down the walls separating data collected for different purposes. We now face the imminent expansion of cyber space into physical space, in the form of networked cameras, biometric identification devices, radio-frequency identification (RFID) tags on consumer goods, and a wide variety of sensors. The electronic networking of physical space promises wide ranging advances in basic and medical science, delivery of services, environmental well-being, industrial production, and health-monitoring of people and machines. It can also lead to new forms of social interactions, as suggested by the example of instant text-messaging [1]. However, without the appropriate architecture and regulatory controls it can also subvert democratic values. Information technology is not in fact neutral in its values; we must be intentional about designing for democracy.

Consider for example security cameras, now placed in so many locations that it is difficult to go through a day without being photographed many times. As yet however most systems are not networked, with the video erased each day. This presents few privacy concerns. On the other hand, digitally networked cameras enabled with facial recognition technology could closely track individuals. While facial ID technology, the crucial step in binding information to an individual, is so far unreliable, the day is clearly coming when all technological components will be reliable and low cost.

RF ID tags present a nearer-term means of binding diverse information collected by sensors and cameras to individual items, since the tags will each have unique identifiers. The tags may either actively emit radio signals, or more commonly, produce a resonant response when interrogated by a reader. They can be read remotely, albeit at relatively short ranges for small passive tags. Intended commercial usages include automated inventory control and retail check-out, with potentially large savings along the entire supply chain. Unfortunately, there are also significant privacy concerns. When coordinated with camera images RFID provides a recipe for automated surveillance. This is not a fanciful future scenario: already “smart shelves” have been tested such that if a tagged item is removed a picture is taken, and again when the tag is detected near checkout a second image is taken to ensure that the item was paid for. This is merely one step of many towards the deployment of means to track the behavior of individuals for commercial or governmental purposes. Moreover, having the tag ID linked to the individual in a database is not even needed for targeting of groups that attend some political event such as a demonstration. Tag readers at the venues would be sufficient to

establish that the bearer of the tag attended, allowing detection or matching of the unique ID to the individual at security checkpoints after the fact.

In recent testimony before a California senate committee [2], Beth Givens, director of the Privacy Rights Clearinghouse, enunciated seven rights that consumers should possess with respect to RF ID technology:

- To know if a tag is in a product
- To know when the tag is read
- To remove the tag when a product is purchased, to prohibit merchants' pressure tactics to coerce keeping the tag active, and to prohibit reactivation without consent
- To own and use inexpensive readers to detect tags
- To access any database that accumulates information from the tag
- Security and integrity of information transmitted from the tag and subsequently stored, with strict regulations on the use of the information by third parties, including governments
- Accountability for everyone in the tag information chain

These principles embody the incompatibility of widespread secret information collection with a free society, and as such apply to many technologies. Totalitarian states place informers in every apartment complex; democratic states should not be embedding the far more efficient electronic equivalent in every commercial transaction or stroll around the block.

It might be argued that for much of the history of civilization, most people lived in crowded villages in which there could be no reasonable expectation of privacy. However, it is also true that the great advances of civilization have taken place in the relative anonymity of cities, where divergent ideas and lifestyles have found greater space to escape the conformity of tradition. Sparta was effectively a village and left to the world little of cultural value; Athens was a city and bequeathed democracy, art, philosophy, theater, and literature.

The initially anonymous structure of the Internet promoted an explosion of self-expression, but as argued by Lessig [3] it may well evolve in unwelcome directions with pervasive profiling and monitoring by commercial and governmental interests. Indeed, the global e-village can potentially be even more intrusive than the traditional village, from which at least it was possible to escape to the city. When sensors, cameras, and tags are pervasively embedded in the environment and networked, anyone in the world who is willing to pay a fee that will exponentially decrease with time will be able to get information on anyone else. Social and political conformity is one plausible result.

Yet while the forces of economic efficiency and governmental concerns for security will drive the networking of the physical world, the outcome need not be dystopic. Information technology includes within itself the possibility for embedding privacy protection, via standards, open code, and government regulation. According to the principle of embedded responsibility [4], code should be structured from the beginning to take into account societal concerns. Historically, regulation in the United States takes

place in a reactive mode once issues have been raised by actual or imminent deployment. By incorporating such concerns as an organic part of the design, the likelihood of costly and imperfect patches is reduced, while at the same time increasing public acceptance of the technology. In this view, the public good represents an additional set of design constraints required for a successful product. Early internet design included many such concerns due to the fact that the end users were also the developers, and were interested in the reliable and open exchange of ideas. Application of embedded responsibility to embedded computing will need to be more deeply intentional with a broader set of stakeholders, but is possible since we are as yet only a small distance down the path of networking the physical world. This can be accomplished if we take the initiative in our research, in standards bodies and in advising government to ensure that these concerns are included in the design, rather than waiting for alarmed activists to propose drastic solutions. Given the largely unknowable but likely momentous societal consequences, it is our responsibility as technologists to seize this opportunity.

References

[1] Howard Rheingold. Smart Mobs: The Next Social Revolution. Perseus Publishing: Cambridge, MA, 2002.
[2] www.senate.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/08-18-03agenda.htm
[3] Lawrence Lessig. Code and Other Laws of Cyberspace. Basic Books: New York, 1999.
[4] www.ipercs.ucla.edu

Biography

Greg Pottie is the deputy director of the NSF-sponsored Center for Embedded Networked Sensing (CENS), a professor in the UCLA Electrical Engineering Department, Associate Dean for Research and Physical Resources in the Henry Samueli School of Engineering and Applied Science, and a member of the UCLA Institute of Pervasive Computing (iPERC).