Is Electronic Privacy Achievable?

Cynthia E. Irvine
Department of Computer Science
Naval Postgraduate School
Monterey, CA 93943 USA
email: irvine@cs.nps.navy.mil

Timothy E. Levin
Anteon Corporation
2600 Garden Road
Monterey, CA 93940 USA
email: levin@cs.nps.navy.mil

"You have zero privacy anyway. Get over it." [1]
-Scott McNealy, Sun Microsystems

While secrecy and integrity policies are most often crafted for protection of corporate (e.g., commercial, educational and government) information, we understand *privacy* policies to be targeted toward the protection of information for and about individuals. The purpose of this panel is to focus on how new technologies are affecting privacy.

Identification of technologies that might adversely affect privacy was made by Turn [2][3] at this Symposium, and included:

- Electronic funds transfer records (we include credit cards in 2000)
- Electronic mail monitoring tools
- Automated home services, including e-commerce and information on request
- Home monitoring services for security, health and energy management
- Use of smart cards
- Mobile computers in the transportation system
- Implanted medical and locating devices
- Linking of integrated personal information record keeping systems

Despite the historical lack of support for privacy research on the part of government, military and industry, it is encouraging to see recent developments in theory, techniques and products to support the "Privacy" part of "Security & Privacy" (e.g., see "proponent" panelists, below). However, it seems clear that the science of privacy is in its infancy, and there are more questions on the table than answers.

Privacy policies, as stated above, might be considered to be a special case of secrecy, but how do the technologies differ? We wonder whether privacy policies generally require technical support that is different in kind from those mechanisms and systems that support secrecy policies? If so, do some of the lessons learned in development of secrecy/integrity systems apply to privacy? For example, can effective privacy be designed in after the fact, or will today's systems-in-development become obsolete if they are required to rigorously enforce privacy policies? Should we consider privacy to be a fundamental component of computer security as a whole, just as are integrity, availability, etc.?

New information collection, derivation and extraction technologies are emerging which have the potential for the massive automated violation of individual privacies. We are concerned with the advancement of technology in the area of personal data acquisition without the co-development of attending assurances of privacy. Can some of the new privacy approaches be used in the responsible development of information accumulation systems?

Panel Structure

We see several camps of new/newer technology and technologists relevant to the privacy debate:

- Privacy-enhancing technology, e.g.:
  -Internet anonymity products
  -Expirable data products
  -Obfuscatable data approach
  -Anonymous e-money services
- Information accumulating technology
  - Explicit, e.g.:
    -On-line Profiling services
    -Centralized key escrow systems
    -Internet data-mining tools
  - Implicit, e.g.:
    -Ubiquitous computing "Appliances"
    -PKI (without privacy) [brands]
- Investigators, e.g.:
  -Red Teams
  -Academics
  -Security-flaw Demonstration Community
  (e.g., hackers)
  -Law Enforcement and Intelligence

For this panel, we have invited individuals from the first and third camps. Left out then, are the purveyors of information accumulation technology (e.g., "on-line profiling"), who might want to argue that their techniques are non-bypassable, or that their technology does not invade privacy, or might want to suggest technical antidotes. Alternatively these folks might want to argue that if an individual wants access to new technology, e.g. a smart refrigerator that ensures it is always stocked by invoking automatic deliveries, then he must give up his privacy, and that these new technologies are impossible without giving up privacy. In any case, we decided to frame the panel discussion without representation from this (second) camp.

The panelists have been encouraged to provide a *technical* discussion as to whether electronic privacy is achievable. While *philosophical* or *political* commentary regarding privacy can be thought provoking, we believe that a technical exploration of the effects on privacy of new technologies is a better contribution to the Symposium at this time.

We will initiate the discussion as a pseudo debate. The resolution of the debate will be: "Electronic Privacy can be Achieved." It is intended that each proponent's initial statement will narrow the resolution to a specific "proposition" regarding the privacy properties of a particular technology. We are interested in understanding how their products/techniques work. The opponents will question the effectiveness of the privacy mechanisms. We are interested in how well these technologies stand up to scrutiny.

In the end, this debate is intended to shed some light on the new privacy technologies and their ability to provide personal privacy in the information age.

Acknowledgments

We would like to thank Heather Hinton and Steve Bellovin from the program committee for their support in putting together this panel.

References

[1] Polly Sprenger, Wired News, 26 January 1999, www.wired.com/news/news/politics/story/17538.html

[2] Rein Turn, "Privacy Protection in the 1980's," Proceedings of the 1982 Symposium on Security and Privacy, Oakland, CA, April 26-28, 1982, pages 86-89

[3] Rein Turn, "Privacy Protection in the 1990's," Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May 7-9, 1990