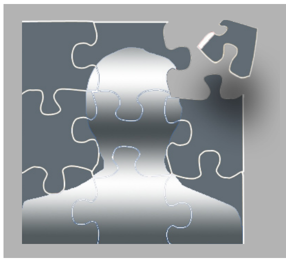

Privacy Policies, Perceptions and Trade-offs

Overview

Privacy has long been a key aspect of cybersecurity but is often over-shadowed by other pressing security concerns. Indeed, perceptions of privacy can vary widely. Some people consider privacy a basic human right, as reflected in some countries' laws giving people ownership of the data that describe them. Others see it as an archaic holdover from an analog world; here, privacy is viewed as an impediment to trading in the growing marketplace for personal data. Still others see privacy as an impediment to "real" security, which requires sharing data about the people being tracked. What remains undisputed, however, is that both the amount and type of personal information circling in cyberspace are increasing exponentially, fueled by the tracking and data capture done by social networking sites, search engines, smart phones, GPS systems, shared databases, and even copy machines.

With support from the Institute for Information Infrastructure Protection (I3P), researchers from five academic institutions are engaged in a sweeping effort to understand privacy in the digital era. Over the course of 18 months, this research project will take a multi-disciplinary look at privacy, examining the roles of human behavior, data exposure, and policy expression on the way people understand and protect their privacy.

I3P

Institute for Information
Infrastructure Protection

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded laboratories and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States.

Project Goals

The project addresses three key research areas, with the following objectives:

Perception and Awareness

- Better understand how privacy is viewed cross-culturally and contextually.
- Construct a framework for making privacy controls more effective (taking into account cultural differences).
- Investigate models of data ownership, particularly those that enable an owner to track third party usage of his or her data.

Policy

- Identify the elements of an effective privacy policy, one that takes into account the initial context and any subsequent changes to it.
- Improve ways for the average user to compare or combine two privacy policies.
- Model the impact of privacy policy on commerce, public health and welfare.

Privacy Metrics

- Understand the value that privacy measurements (such as an individual's data exposure) would provide to an individual and to society. For example, what might various levels of privacy look like, and how might their application affect discourse or practice?
- Suggest how levels of privacy could be reported and enforced.
- Determine the differences between actual and perceived privacy.

Team Members

Carnegie Mellon University
Dartmouth College
Georgia Tech
Indiana University
University of California, Berkeley

For more info visit http://www.thei3p.org/.
The I3P is managed by Dartmouth College.

The Team

This multi-institutional, multi-disciplinary investigation brings together legal experts, behavioral scientists, sociologists and computer scientists from five I3P member institutions: Carnegie Mellon University, Dartmouth College, Georgia Tech, Indiana University and the University of California, Berkeley.

Impact

Over the course of the 18-month project, researchers will interact with industry, government and academia, to ensure that their analysis and findings reflect the realities of privacy in today's digital age. The project team will disseminate its findings in peer-reviewed publications and at workshops involving all constituencies.

Advisory Committee

To ensure that the project reflects the needs of all constituencies, the project team will work closely with an external set of advisors drawn from the federal government, private enterprise and a non-governmental organization.

For More Information

Please contact Shari Lawrence Pfleeger, Research Director of the I3P: shari.l.pfleeger@dartmouth.edu for more information.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.