The Accountability Perspective

Lalana Kagal and Hal Abelson
MIT Computer Science and Artificial Intelligence Lab
32 Vassar Street Cambridge MA 02139
{lkagal, hal}@csail.mit.edu

Extended Abstract

Attempts to address issues of personal privacy in a world of computerized databases and information networks typically proceed from the perspective of controlling or preventing access to information. The ease of sharing and copying data and of aggregating and searching across multiple databases, to reveal private information from public sources have made this perspective inadequate for addressing information misuse on the Internet [1]. In addition, an exclusive reliance on access restriction leads to technology and policy strategies in which information, once revealed, is completely uncontrolled.

We propose alternate strategies to access control, ones that are similar to how legal and social rules work in democratic societies. Vast majority of these rules are not enforced perfectly or automatically, yet most of us follow the majority of the rules because social systems built up over thousands of years encourage us to do so and often make compliance easier than violation. For example, when trying to find parking on the street even if there is no traffic police around to give me a fine or a ticket, most people will still obey the parking signs because of the way social and legal norms have been built into our societies. They've made it easier to meet the norms than violate them, risk getting caught and getting punished. The set of legal or social norms govern what we can or cannot do, and they have been ingrained into our way of thinking such that most people go through life without any problems. When problems occur, there are mechanisms that ensure that violators are reprimanded.

From a technology perspective, this requires supplementing legal and technical mechanisms for access control with new mechanisms for transparency and accountability of *data use*. We suggest focussing on helping users conform to policies by making them aware of the usage restrictions associated with the data and to understand the implications of their actions and of violating the policy, and a technology infrastructure that supports privacy through provable accountability to usage rules rather than merely data access restrictions.

In order to support the responsible use of private data, we believe information systems should be engineered to have the characteristics described below

- Give users due notice: Both in the case of collecting their data and using it, information systems must give users due notice. This will give users the opportunity to respond appropriately - to either take action to protect their privacy or voluntarily give it up in exchange for better service.

- Don't rely just on upfront authorization, also support accountability: A-priori authorization provides a way to restrict access to sensitive data but has several problems [1]. A supporting approach is to provide post-facto accountability, which requires the system to have mechanisms in place to identify misuse of data [2]. This requires (i) tracking the data as it flows through the system and to maintain detailed provenance information, (ii) machine processable usage policies, (iii) policy tools that reason over policies and provenance to identify violations.

- Privacy-enabling interface design: As we want to encourage appropriate use not only by information systems but also by users, system interfaces should provide hints or signs describing optimal behavior for users with respect to data. Some approaches include (i) policy-awareness which provides all participants with accessible and understandable views of the policies associated with information resources including the consequences of misuse, and (ii) tools for helping users understand the consequences of their actions (such as posting a picture on their social network or sending an email) on the Web, some of which will have privacy implications.

Most online businesses today leverage user data to provide more customization and so privacy can be seen as a tradeoff between value-added services and loss of personal data. As preventing access to personal data is no longer an option and as sensitive data can be easily inferred from public sources, we believe the future of privacy protection lies in developing frameworks that ensure the responsible collection and use of data and in educating users on good privacy practices.

References

[1] L. Kagal and H. Abelson. Access control is an inadequate framework for privacy protection. In *W3C Privacy Workshop*, 2010.

[2] D. Weitzner, H. Abelson, T. Berners-Lee, C. Hanson, J. Hendler, L. Kagal, D. McGuinness, G. Sussman, and K. K. Waterman. Transparent accountable inferencing for privacy risk management. In *AAAI Spring Symposium on The Semantic Web meets eGovernment*, March 2006.