

Usable Privacy and Security for Personal Information Management

The goal is a policy workbench enabling users to create and transform natural language policies into machine-readable code for enforcement and compliance audits.

Usable privacy and security technology is a critical and unmet need in the management of personal information. Computer professionals can contribute significant business and social value by focusing on practical solutions. In today's online environment, personal information is improperly disclosed in ways that enable identity theft and other negative consequences for individuals and organizations alike. For example, phishers are increasingly sophisticated. Viruses are a constant threat. No one who interacts electronically is immune from these risks. A vast amount of personal information is constantly being collected, transferred, stored, and shared by organizations in the health care, banking/finance, government, travel, entertainment, and communications domains.

How can computer professionals address this challenge? Making systems secure and giving appropriate attention to privacy issues require more than just technology. The 2003 Computing Research Association Conference on Grand Research Challenges in Information Security and Assurance identified the ability to "give end users security controls they can

understand and privacy they can control for the dynamic, pervasive computing environments of the future" as a major research challenge [1]. This goal reinforced [6], which stated that "Security mechanisms are only effective when used correctly," though such use is often not possible due to usability issues with security software. Usable privacy and security management must be part of the initial design considerations for technology applications, systems, and devices that involve personal information collection, access, and communication.

Privacy, which depends on security systems, involves complex social issues that concern our right to know what information about us is collected, who might see it, and how it might be used. Privacy protection involves more than just protecting personal information (such as credit card numbers or other identifiers). In isolation, one data element might not identify the individual to whom it relates. But data-aggregation techniques are changing the playing field. Research demonstrates that minimal amounts of information believed to be anonymous can be used to personally identify an individual [4].

While there is considerable international consensus around a set of high-level principles regarding the protection of privacy in information technology [5], little has been done to implement privacy policies through technology. Privacy enforcement remains largely a human process, and the policies that organizations present to their customers, patients, citizens, and employees are generally vague (such as "Customer service representatives will use your personal information only for the efficient conduct of our

business”). Emerging standards for privacy policies on Web sites [2] involve XML schemas of policy content but do not specify how the policy might be created or implemented. The reality is that little capability is available for getting the technology to actually implement the access and use limitations we might expect from a policy statement like “We will not share your information with a third party without your consent.” While much privacy-related research and development focuses on the end user’s control of information on Web sites and pervasive devices, some privacy research is being conducted at the organizational level needed for complete privacy policy [3].

Our work on the Server Privacy ARchitecture and CapabiLity Enablement, or SPARCLE, policy workbench at the IBM T.J. Watson Research Center in Hawthorne, NY, focuses on the design and development of policy authoring and transformation tools that enable organizations to create machine-readable policies for real-time enforcement decisions, along with the ability to verify the operational policy decisions through compliance audits of enforcement logs (www.research.ibm.com/privacy) [3]. SPARCLE will enable individuals to be informed participants when interacting with many types of organizations and for the organizations to be able to know that the policies they espouse are indeed being enforced within the organizations by their own processes, thus lowering the risk for all parties.

In 2003, we identified customer requirements for privacy technology in North America, Europe, and Asia, then built and tested them with users in 2004 Wizard-of-Oz prototypes (looks and feels real, though no functional code) for privacy policy creation, implementation, and transformation, as well as for compliance auditing. In 2005 the SPARCLE team completed a functional policy workbench prototype of the authoring and transformation capabilities that enable organizations to establish implementable rules covering how they collect and use personal information, transfer it within and outside the organization, and dispose of it. The prototype workbench transforms natural language rules through the use of natural language parsing technology into machine-readable XML code for use by enforcement engines. Future research will complete additional components necessary for end-to-end commercial solutions.

Professionals in the fields of human-computer interaction, computer architecture, security, and privacy can

aim to create systems and interaction methods that reduce the complexity in defining, implementing, and managing privacy and security policies for everyone’s benefit. As technological tools become available to help organizations establish and enforce privacy policies implemented through technology, the quality of these policies and new privacy legislation will improve. Challenges that remain include simplifying the mapping of rule elements to data fields and applications in system configurations. The tools promise to help give organizations a verifiable path from the written form of a privacy rule to real-time enforcement decisions regarding access to personal information.

People interacting with organizations as patients, customers, students, citizens, or employees will be able to understand and verify who has access to their personal information and for what purposes it might be used. The result is increased user trust and their use of e-government services, e-healthcare, and a range of e-commerce products and services, demonstrating that what a particular organization says is indeed what it verifiably does regarding the personal information in its care. **C**

REFERENCES

1. Computer Research Association Conference on Grand Research Challenges in Information Security and Assurance (Warrenton, VA, Nov. 16–19, 2003); www.cra.org/Activities/grand.challenges/security/.
2. Cranor, L. *Web Privacy with P3P*. O’Reilly Media, Cambridge, MA, 2002.
3. Karat, J., Karat, C., Brodie, C., and Feng, J., Eds. Special Section: Privacy in information technology: Designing to enable privacy policy management in organizations. *International Journal of Human Computer Studies* 63, 1–2 (July 2005), 153–174.
4. Malin, B. and Sweeney, L. How (not) to protect genomic data privacy in a distributed network: Using trail re-identification to evaluate and design anonymity protection systems. *Journal of Biomedical Informatics* 37, 3 (2004), 179–192.
5. Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, France, 1980; www.oecd.org/home/.
6. Whitten, A. and Tygar J. Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the Ninth Usenix Security Symposium* (Washington, D.C., Aug. 23–26). Wiley Publishing, Berkeley, CA, 1999, 167–184.

CLARE-MARIE KARAT (ckarat@us.ibm.com) is a research staff member in the security and privacy area of the IBM T.J. Watson Research Center, Hawthorne, NY.

CAROLYN BRODIE (brodiec@us.ibm.com) is a research staff member in the security and privacy area of the IBM T.J. Watson Research Center, Hawthorne, NY.

JOHN KARAT (jkarat@watson.ibm.com) is a research staff member in the security and privacy area of the IBM T.J. Watson Research Center, Hawthorne, NY.