Lorrie Faith Cranor, Guest Editor

Internet Privacy

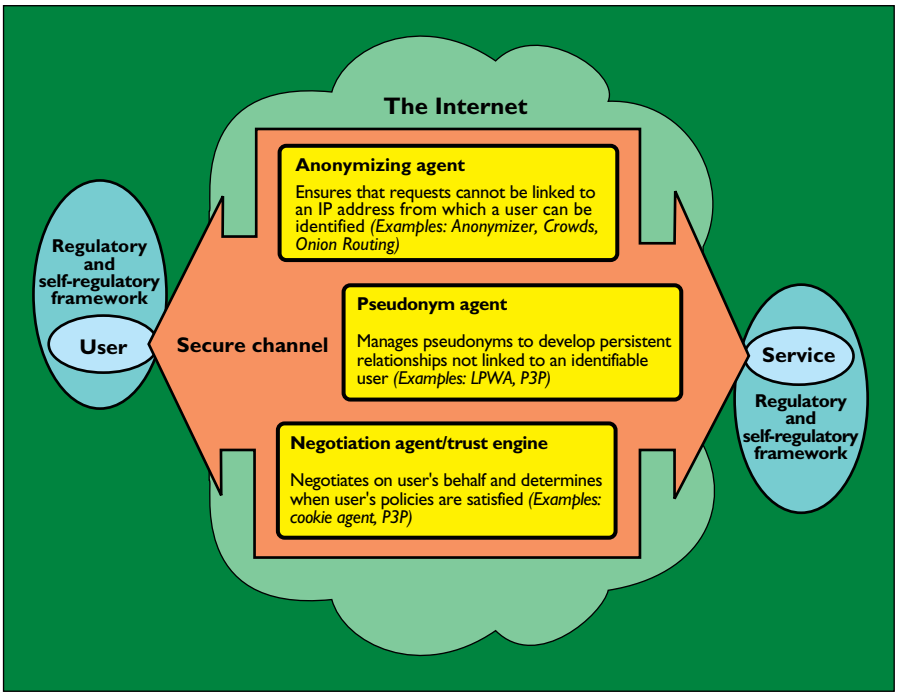
PRIVACY WAS A SENSITIVE ISSUE long before the advent of computers. Concerns have been magnified, however, by the existence and widespread use of large computer databases that make it easy to compile a dossier about an individual from many different data sources. Privacy issues are further exacerbated now that the World-Wide Web makes it easy for new data to be automatically collected and added to databases [1]. Today, data entered into forms or contained in existing databases can be combined almost effortlessly with transaction records as well as records of an individual's every click through cyberspace. As data mining tools and services become more widely available, privacy concerns will likely increase further.

In this special section we examine Internet privacy and discuss some of the tools now used to address it. We present four articles that describe technology tools that address various aspect of online privacy, one article that describes a self-regulatory program to enforce privacy claims made by Web sites, and one article that describes past regulatory and self-regulatory approaches and suggests approaches that should be taken in the future.

The figure on the next page denotes how various technology tools and regulatory and self-regulatory frameworks can work together to help protect privacy. As illustrated, a variety of technology tools help users protect their privacy during interactions with Web sites and other Internet services. Furthermore, users may receive additional privacy protections from laws and industry guidelines that may apply in their jurisdiction and/or the jurisdiction of the service. Because the Internet is global, different regulatory and self-regulatory frameworks may be in effect for the user and the service.

Illustrations By Jason Schnieder

A number of tools have been developed to help Internet users surf the Web anonymously. These anonymizing agents focus on ensuring that requests to Web sites cannot be linked to an IP address from which a user can be identified. One of the best-known Web anonymity tools is the Anonymizer,[1] a service that submits HTTP requests to Web sites on behalf of its users. Because the request is submitted by the Anonymizer rather than the user, the only IP address revealed to the Web site is that of the Anonymizer. However, users of this service are not anonymous to the Anonymizer itself, nor to their own ISPs, who may log their users' Web activities.



Various technology tools can work together along with regulatory and self-regulatory frameworks to provide online privacy protection

We present two anonymity tools in this section that do not require users to trust a single third-party to maintain anonymity. Reiter and Rubin discuss Crowds—an anonymity agent based on the idea that people can be anonymous when they blend into a crowd. Rather than submitting HTTP requests through a single third-party, Crowds users submit their requests through a crowd, that is, a group of Web surfers running the Crowds software. Crowds users forward HTTP requests to a randomly selected member of their crowd. Neither the end server nor any of the crowd members can determine where the request originated. Syverson, Goldschlag, and Reed discuss an anonymity agent called Onion Routing, in which users submit encrypted HTTP requests using an onion, that is, a layered data structure that specifies symmetric cryptographic algorithms and keys to be used as data is transported to the intended recipient. As the data passes through each onion-router along the way, one layer of encryption is removed according to the recipe contained in the onion. The request arrives at the recipient in plain text, with only the IP address of the last onion-router on the path.

While Internet users may often wish to remain unidentified, they may sometimes wish to establish persistent—albeit anonymous—relationships with Web sites, for example to take advantage of customized services. Gabber et al. present the Lucent Personalized Web Assistant (LPWA), a pseudonym agent that helps users build such persistent anonymous relationships. LPWA can be used to insert pseudonyms into Web forms that request a user's name or email address. It is designed to use the same pseudonyms consistently every time a particular user returns to the same site, but use a different pseudonym at each site. It works in conjunction with an anonymizing proxy server, but it could also be used with other anonymity agents such as Crowds or Onion Routing.

Anonymity agents and pseudonym agents are useful for Web surfing in which users have no need or desire to be identified. However, when users wish to make online credit card purchases and have merchandise delivered to their doorsteps, they need to provide some identifying information. Negotiation agents and trust engines can assist users in reviewing a service's request and determining whether or not to provide the

[1] www.anonymizer.com

requested data or access. For example, many Web browsers include tools that allow users to specify their preferences regarding HTTP cookies. Users can specify that they should be prompted whenever a site asks to set a cookie, that all cookie requests should be automatically accepted or rejected, or that cookie requests should be accepted under a limited set of conditions. Reagle and Cranor describe the Platform for Privacy Preferences Project (P3P) which provides a rich vocabulary for services to express their information practices and for users to express their privacy preferences. Thus, P3P helps users make informed decisions about when to release their data. But P3P does not protect data in and of itself. Users must be assured that when they release their data, services will use it only as they have promised. Regulatory and self-regulatory frameworks can help provide such assurances.

Benassi describes TRUSTe, a self-regulatory privacy initiative dedicated to building consumers' trust and confidence on the Internet through a program in which Web sites can be licensed to display a privacy seal or "trustmark" on their sites. Trustmarks provide consumers with up-front assurance that a Web site's policies accurately reflect their practices and that there will be a means of recourse if the site does not abide by its stated policies. Other organizations are developing similar privacy assurance seal programs that place a variety of requirements on licensees including entering into contractual agreements, undergoing third-party audits, and agreeing to enter into an arbitration process if a complaint is filed against the licensee. So far these organizations are offering only visual seals that licensees can place on their Web sites. However, these seals could also come in the form of digitally signed certificates that could be processed by negotiation agents and trust engines.

Clarke discusses a variety of privacy inititatives that address the multiple dimensions of privacy. He also outlines a "co-regulatory privacy protection regime." He argues that while self-regulation and privacy-enhancing technologies are welcome developments, they are not sufficient by themselves and should be accompanied by legislative provisions, a privacy watchdog agency, enforcements, and sanctions. He further argues the principles around which the co-regulatory regime revolves must extend beyond the outdated set codified in the 1980 OECD Guidelines in order to cope with the last quarter-century's dramatic enhancements to the capabilities and capacity of information technology.

IT IS IMPORTANT TO NOTE THAT FOR ONLINE PRIVACY INITIATIVES to be successful, they must be accompanied by tools and procedures to provide strong security.

Finally, it is important to note that for online privacy initiatives to be successful, they must be accompanied by tools and procedures to provide strong security. Whenever sensitive information is exchanged, it should be transmitted over a secure channel and stored securely. Encryption technology such as SSL can protect data as it is transmitted during Web interactions. File encryption, firewalls, and access control systems can protect stored data. A general discussion of encryption or security is beyond the scope of this issue. Interested readers might review recent survey articles on Web security [2, 3]. C

References

1. Cranor, L. Internet privacy: A public concern. *netWorker 2*, 3 (June/July 1998), 13–18.
2. Oppliger, R. Internet security: firewalls and beyond. *Commun. ACM 40*, 5 (May 1997), 92–102.
3. Rubin, A. and Greer, D. A survey of World Wide Web security. *IEEE Computer 31*, 9 (Sept. 1998), 34–41.