

Understanding your Online Identity:

Protecting your Privacy

Laws concerning the privacy of information about you vary from country to country. Many of the world's legal frameworks have not kept up with the rapid changes in information sharing capabilities brought by the Internet, creating a regulatory gap. These two factors have created considerable uncertainty in the minds of many Internet users about how private their Internet experience really is, or should be.

This explores online identities, the privacy of your online identity, and some of the ongoing work in the Internet community to give you more control over your identity.

What are the key concerns related to online identity and privacy?

Internet users are naturally concerned about how their personal information is used. In a word, it is their *privacy* that concerns them. In addition to the problems of identity theft, users have questions about the widespread practice of information about them being shared between services.

With the increased use of the Internet for e-commerce, criminals have stepped up their own efforts to *steal user identifiers, passwords, and associated information* to impersonate other Internet users. The motivation for identity theft is often simple economic gain: by stealing your information and impersonating you, criminals may be able to order goods and services, transfer funds, or redirect existing shipments. While the technology has changed, the basic motivations and behaviors of these thieves are age-old, and there are many existing legal protections (*e.g.*, consumer protection laws) that may also apply to Internet users.

Beyond e-commerce, the *sharing of online information* also concerns many Internet users. Some of the sharing is voluntary, such as within social networks, and some is involuntary, such as the trading of information between services such as online advertising networks. For example, you may have willingly given your location, age, sex, and interests to Facebook, but you didn't intentionally disclose that information to anyone else. Yet online advertising networks may have deduced much of this information, approximately, based on the trail of web sites you visit and the searches you make. Online information sharing, though, is more difficult to discuss than outright identity theft because there are few frameworks and little agreement regarding what is proper and improper, and what is legal and illegal. Internet users are often concerned about their private information being shared and sold by third parties, even when they provided the information themselves. Users want to control the sharing of their private information, and keep it from being used in ways they didn't intend. As such, the tensions between sharing, over-sharing, privacy and commercial interests have not yet been resolved.

What kind of information about me is being collected and why?

While you pay for your home or business connection to the Internet, you're only paying for network *access*. Web sites you visit may be free to you, but each has its own costs that have to be paid somehow. The most common method of doing that is advertising, where a third party pays the web site owner for the privilege of putting their advertisement next to some information you want to see. This has made virtually every web page you visit a commercial transaction.

When you get "free" information or services from a web page, you are exposing information about yourself to the web site that they can use to show you advertising targeted more directly to you. It's a trade, in effect: you've given something valuable to the web site operator, in exchange for consuming information you consider valuable. Of course, what you expose on every page may have very little value by itself, but as this information is accumulated, a fairly significant profile—a partial identity—can be created about you. If you also consider your trusted partners, such as your bank, insurance, or health care provider, where you have explicitly provided very private information, you'll see that there's a lot of information about you on the Internet, even if it isn't necessarily connected together.

Even if you haven't explicitly given these web sites any information you normally consider "private," your Internet browsing behavior, over time, can expose more about your true identity than you might expect. For example, in 2006, when AOL released anonymized search records as part of a research project, reporters at the New York Times used those records, aggregating them together and combined them with other public information, to identify and contact one person from those searches—within days.

As you might imagine, the more information about you that can be tied together, the more complete—and the more valuable—your profile is. This creates incentives for operators of commercial web sites to work together to link large portions of your online life. As the Electronic Privacy Information Center writes: "*Search terms entered into search engines may reveal a plethora of personal information such as an individual's medical issues, religious beliefs, political preferences, sexual orientation, and investments. [...] Opaque industry practices result in consumers remaining*

largely unaware of the monitoring of their online behavior, the security of this information and the extent to which this information is kept confidential.”

When the behavioral information about an Internet user is combined with other online accessible information, such as public government records, business and personal information services, and information posted by and about them on social networking sites, there is the potential to create an in-depth online partial identity—one that may contain an uncomfortable amount of accurate and inaccurate information.

Controlling sharing of your online identity

Traditionally, the organization you are sharing information with controls access to the information. In many countries, certain types of information (such as your personal health information) and certain types of organizations (such as financial services companies) are regulated as to how your information can be shared (on-line and off-line) and used. However, other information about you may fall outside of the realm of current laws.

Before the Internet simplified the collection and sharing of information, privacy concerns were different. Now that many companies have control over vast amounts of information about Internet users, and share it among themselves for commercial purposes, the issue of control of this private personal information is attracting considerable public interest.

Three forces are working together to move the locus of control of personal information back to you. First, many countries are considering amending or introducing new laws that would require user consent for collection and use of personal information. Secondly, organizations are seeing an economic incentive in giving you more control, as doing so can increase data accuracy and reduce the costs of collecting and updating the information.

Thirdly, technology (discussed below) is being developed that will let companies share online identity information securely, while allowing Internet users to exercise greater control over who has access and what types of information can be shared.

Tell me more about the technology

Historically, technology used to control identity information started with centralized solutions, information being collected and used within a single organization for their own purposes. Over time, control has slowly shifted to federations: groups of organizations who wanted to extend services to each other's users. Through both legal and technical frameworks, these federations can use a wide variety of technologies with names like SAML (Security Assertion Markup Language), OpenID, iCards (Information Cards), and OAuth to share identity information in a controlled way. (If you'd like to learn more about these, Google's Internet Identity Research project has produced an easy-to-understand document at <http://sites.google.com/site/oauthgoog/Overlap>.) It's not the technology itself that makes up a federation, however. The value of federations is in the agreement between organizations to only share information for specific uses.

With a combination of politics, economics, divergent interests, and varying technical hurdles, there is no complete or agreed-upon solution. However, the US Government has made a significant step forward in pushing for cross-organization identity technologies after President Obama's Transparency and Open Government executive action was released on his first day in office. The result was a prototype Open Identity Exchange (OIX) that enables connections between government web sites, with participation from many Internet companies including AOL, Google, PayPal, Verisign, and Yahoo!.

An important part of the Open Government initiative is the ability for the end user to control which information is shared between their identity provider (such as AOL or Google) and various government web sites. For example, if you use your Google account to access the National Library of Medicine's PubMed site, you are able to specify exactly what information Google shares with the government web site. The supported technologies aren't necessarily complete or ready for everyone to use, but the wide scope of the Open Government initiative is giving the Internet community hands-on experience in how these technologies can be used to move the locus of control for user identity information back into the hands of the user.

As the technologies mature, enterprises and governments are engaging with each other on the topic of enabling end-user privacy controls in the online environment. International efforts, such as OECD regulatory guidance and IETF technical standards, will continue to ensure that the Internet remains a safe network for all its users. The combination of technology and public policy will increase confidence in the Internet as a reliable network for conducting public, and private, transactions. ISOC believes that this combination is the best way forward.

About the Internet Society

The Internet Society (ISOC) is a nonprofit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. We are dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world.

