Understanding your Online Identity

Protecting Your Privacy

Not only do laws concerning the privacy of your personal information vary from country to country, but many of the world's legal frameworks have not kept up with the rapid changes in information sharing brought on 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 paper explores online identities, the privacy of your online identity, and some of the ongoing work within the Internet community that will 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 having information about them shared among services.

As more and more people use the Internet for e-commerce, criminals have stepped up their efforts to *steal user identifiers, passwords, and associated information,* information that makes it possible 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, redirect existing shipments, or transfer funds. While the technology has changed, the basic motivations and behaviours of these types of thieves are age-old, and there are many existing legal protections, such as consumer-protection laws, that may also apply to Internet users.

Beyond e-commerce, the simple act of *sharing online information* is a source of concern for many Internet users. Some of the sharing is voluntary, such as within social networks, and some is involuntary, such as when your information is traded by online advertising networks. For example, you may have willingly shared your location, age, gender, and personal interests on your Facebook page, but you did not intentionally disclose that information to anyone other than your Facebook friends. Yet, online advertising networks may have deduced much of this information, approximately, based on the trail of websites you visit and the searches you make. Unlike outright identity theft, online information sharing is a more difficult issue to address because there are few frameworks and little agreement regarding what is proper and improper, and what is legal and illegal. Internet users often express concern about their personal information being shared and sometimes sold, even when they provide the information themselves. They want to be able to decide what information is private and control what is shared, and they want to keep their information from being used in ways they did not 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 may pay each month for a home- or business-based Internet connection, in reality you are only paying for network access, not for the content you find on websites. The websites 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 through advertising, wherein a third party pays the website owner for the privilege of putting advertisements near information they believe you want to see. This has turned virtually every Web page you visit into a commercial transaction.

Just by viewing or clicking through free information or services on a website, you are divulging information about yourself that can be used to determine what types of products or services might interest you. It is, in effect, a trade: you have given the website operator something of value (your attention) in exchange for being able to view information you consider valuable. Of course, what you divulge about yourself on a Web page may have very little value on its own, but as information about you is accumulated, a fairly significant profile—a partial identity—can be created. If you combine that with the information you have shared with your trusted partners, such as a bank, insurance company, or healthcare provider, you will see that there is a lot of potentially valuable information about you on the Internet, even if the pieces of information are not connected.

Even if you have not explicitly given any of the websites you normally visit any specific information about you that you would consider private, your Internet-browsing behaviour, over time, can reveal more about

your true identity than you might expect. Consider, for example, what happened in 2006, when AOL inadvertently released anonymized search records that were being used as part of a research project. By cross-referencing those anonymized search records with phonebook listings, reporters at the *New York Times* were able to identify and locate an individual within days.

As you might imagine, the more information about you that can be pulled together, the more complete—and the more valuable—is your profile. This creates incentives for operators of commercial websites to work together to connect 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 behavioural information about an Internet user is combined with other information that is available online, 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 a disquieting blend of accurate and inaccurate information.

Controlling sharing of your online identity

Traditionally, the organizations you are sharing information with control access to that information. In many countries, certain types of information (such as your personal health information) and certain types of organizations (such as financial-services companies) must comply with regulations about how your information can be shared (both online and offline) and used. However, other information about you may fall outside 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 that information among themselves for commercial purposes) the issue of who controls private personal information is attracting considerable public interest.

Three forces are at work to return control of your personal information to you. First, many countries are considering amending or introducing new laws that would require user consent for the collection and use of personal information. Second, businesses and organizations are seeing an economic incentive in giving you more control over your personal information, as doing so can increase data accuracy and reduce the costs of collecting and updating the information. Third, there are new technologies being developed (as discussed later) that will allow companies to share information about users' identities securely, while allowing users to exercise greater control over who has access to their information and what types of information can be shared.

Tell me more about the technology

Originally, the technology used to control identity information was based on centralized solutions; that is, the information being collected remained within a single organization and was used only for that organization's purposes. Over time, however, control of identity information shifted to federations; groups of organizations that wanted to extend services to each other's users. Through both legal and technical frameworks, those federations are able to 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 want to know more about these technologies, Google's Internet Identity Research project has produced an easy-to-understand document that can be found at http://sites.google.com/site/oauthgoog/Overlap.) The value of federations is not just in the technology, it is also in the agreement among organizations that they will only share information for specific uses.

Whether it is because of politics, economics, divergent interests, or varying technical hurdles, or a combination of those factors, there is no complete or agreed-upon solution. However, the U.S. 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 among government websites, 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 websites. For example, if you use your Google account to access the National Library of Medicine's PubMed site, you are now able to specify exactly what information Google shares with a government website. The supported technologies are not 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 over 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 Organisation for Economic Co-operation and Development (OECD) regulatory guidance and the technical standards that come out of the Internet Engineering Task Force (IETF), 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. The Internet Society 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.

Internet Society™