Identity on the Internet

An Internet Society Public Policy Briefing

On the Internet, your digital identity is not just a name, it is who you are and your key to online interactions. Digital identities help users protect their privacy; segregate personal, social, and professional online presences; and engage in trusted transactions with storefronts, banks, medical providers, and governments. Identity-driven innovation can encourage a more secure banking sector, more trusted digital trade (e.g., electronic signatures and mobile payments), and a more efficient e-government sector (e.g., electronic tax returns and e-voting). For these reasons, digital identity is a key aspect of many Internet policy issues, including privacy, consumer protection goals, e-government services, digital trade, and trust in the digital economy. In short, a trusted digital-identity ecosystem is a critical component of a trusted Internet.

The Internet Society believes that governments should continue to encourage the open development and use of identity choices on the Internet, whether identified, pseudonymous, or anonymous. This policy brief is designed to help policy makers understand the benefits of online identity solutions for services, economic efficiency and growth, and citizen empowerment.

Introduction

Some people think of their digital identity as a passport for the Internet. In reality, the concept of identity on the Internet is much richer: we adapt our identity depending on the context. For example, we likely reveal our “real” identity to access e-government services, but use a fictitious name or pseudonym on social media, and anonymously access public websites for medical information.

There are five main types of digital identities, each used in different contexts.

1. **Electronic identities.** Some governments issue their citizens electronic identities for online use. In some cases, the issuing entity, or identity provider, is an approved organization (e.g., a post office).
2. **Attribute-based identities.** Some interactions do not require identification. Instead, it is enough that an individual possesses a specific attribute (e.g., is at least 18 years old or is a student).
3. **Authentication-based identities.** Many providers of online services, such as Facebook and Gmail, provide users access to their accounts via a username and password (also known as login credentials). These identities are both how customers identify themselves to service providers and how service providers authenticate or verify that users are who they say they are. Unlike government-issued electronic

identities, login credentials can be anonymous or pseudonymous. Second-generation authentication mechanisms, such as “single sign-on”, allow users to login to multiple services from one access point.

4. **Electronic signatures.** Many countries have enacted laws to recognize the legal effect of electronic signatures. In addition to being a means of identification, electronic signatures may have consequences, such as confirmation or acceptance of a contract.

5. **Identifiers.** All Internet interactions involve the use of identifiers. Some help the Internet function (e.g., IP addresses), others identify or recognize a device and/or user (e.g., security at financial institutions), and still others track users’ online interactions (e.g., targeted advertising). There is no definitive list of identifiers: in theory, identifiers are any data that identifies information about a device and/or a user. Information about a device may include type of device, operating system, browser version, browser plug-ins, and so forth. Information about a user may include preferences, such as font size, screen colours, and contrast, and the like.

Key Considerations

Specific use cases and privacy considerations exist for each of the main digital identities.

- **Electronic identities.** To obtain a government-issued electronic identity, citizens typically must prove who they are by presenting a government-issued passport, identity card, or other form of government-issued identification. As a result, the two types of identity are linked. Typically, the primary use of government-issued electronic identities is government services (e.g., filing tax returns and claiming benefits). Secondary uses are typically services that require a high degree of certainty or assurance that an individual is who he or she claims to be (e.g., banking and medical records). Government-issued electronic identities frequently serve multiple purposes, such as identification, two-factor authentication to access online services (e.g., e-government services), electronic proof-of-passport information to allow access to personal data, and a legally effective electronic signature.

- **Attribute-based identities.** While one attribute (e.g., age) might not indicate an individual’s actual identity, a combination of attributes can (e.g., date of birth, zip code, and gender).

- **Authentication-based identities.** For a variety of reasons, authentication mechanisms that require only a username and a password are notoriously insecure. Often, the username is an email address or other obvious identifier (e.g., a name or nickname); people frequently reuse passwords or use easily guessed passwords (e.g., 12345); and when users forget their passwords, sites typically reset them using the email address stored in the profile, thereby leaving the account even more-poorly protected. Today, many service providers offer additional access-control protection via two-factor authentication. This type of authentication requires a combination of something a user obtains (e.g., a one-use time-sensitive code sent to the user’s smartphone) and something the user knows (e.g., username or password). Single-sign-on mechanisms offer users greater convenience, but may expose users to tracking across the connected services.

  Note that even if users choose pseudonymous login credentials, the content of their accounts (e.g., email text or photos) may reveal their real identities.

- **Electronic signatures.** Electronic signatures can serve two purposes: confirming that a user adopts the contents of a document and confirming who wrote the communication. Cross-border legal recognition of electronic signatures is critical to efficient global trade.

- **Identifiers.** Identifiers can be used to identify a specific device or user[1] or track a device or device user's online interactions. Some identifiers are easily observable (e.g., browser features), others are deliberately placed within a device to make tracking easier (e.g., cookies). Identifiers can be aggregated, linked, and used to infer connections.

Challenges

Privacy is one of the biggest challenges regarding identity on the Internet. It is no longer true that "On the Internet, nobody knows you are dog" to quote the famous cartoon from *The New Yorker* (1993). Despite the countless ways that trusted, verifiable digital identities are employed, today most Internet users are more-easily identified than ever before. In many cases, although a user's actual identity may not immediately be known, it can be inferred by someone with enough access to either their data or their attributes (e.g., Facebook friends, geolocation data, Internet time and date stamps).

Guiding Principles

Following are guiding principles for governments and citizens to consider:

- **Individuals should be able to use pseudonymous and anonymous digital identities, depending on the context and with whom they are interacting.** They should have access to reliable, secure, privacy-by-design, trustworthy digital identities for online transactions, particularly those involving sensitive data (e.g., medical and financial data) or private content. At a fundamental level, these are the characteristics that will support a secure, reliable, and protective consumer environment.
- **Digital identities needn't be government-issued to be trustworthy.** However, governments should consider offering electronic identification for more-secure access to e-government services and commercial transactions (e.g., banking) that require a high level of authentication. This would contribute to transactional security for all parties.

Governments that already issue electronic identification (identity providers) should take the following steps:

- Consider what form(s) of electronic identity are most useful for their projected uses; and identify the economic, social, or other issues that could hinder their deployment or use.
- Ensure that their electronic-identity system is technically interoperable and legally compatible with the identity systems deployed by other governments, so their electronic identities can be used for cross-border transactions.
- Prevent the government and other relying parties from tracking the use of electronic identities across services and institutions, unless absolutely necessary. It is good privacy and security practice to quarantine the use of digital identities and the data they are used to access.
- Throughout the lifecycle of the electronic identity, collect and use only the data that is necessary. Applying the principle of data minimization in this way enhances consumer trust and choice.
- Make electronic identities revocable when necessary (e.g., in the event of compromise).
- Conduct a thorough risk-benefit analysis before considering the use of biometric data for electronic identities. In the event of compromise, biometric data cannot be revoked (e.g., a person cannot change his or her fingerprint). For this reason, it should be avoided, unless absolutely necessary.

[1] See Panopticlick, an Electronic Frontier Foundation research project on the uniqueness of browsers, https://panopticlick.eff.org/.

Governments should ensure that citizens without government-issued electronic identities are not excluded from government services.

Conclusion

Effective digital identities facilitate trusted Internet communications. For this reason, it is critical that governments (1) continue to encourage the open development and use of new technologies to express identity on the Internet, whether they are identified, pseudonyms, or anonymous; and (2) refrain from activities that might stifle innovation or economic and social progress, such as mandating the level of identification required to access the Internet or social media.

Additional Resources

The Internet Society has published a number of papers and additional content related to this issue. These are available for free access on the Internet Society website.

- Understanding your Online Identity: An Overview of Identity, 2011, http://www.internetsociety.org/understanding-your-online-identity-overview-identity
- Understanding Your Online Identity: Protecting Your Privacy, 2012, http://www.internetsociety.org/understanding-your-online-identity-protecting-your-privacy-0
- R. Wilton, *Have you chosen an Identity Provider Lately?*, 2014, http://www.internetsociety.org/doc/have-you-chosen-identity-provider-lately

More information about digital identity is available online.

- *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, Organisation for Economic Co-Operation and Development, 2011, http://www.oecd.org/sti/interneteconomy/49338380.pdf
- E. Birrell and F.B. Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization," *Security & Privacy, IEEE,* vol. 11, no. 5, Sept.–Oct. 2013, pp. 36–48, https://www.cs.cornell.edu/fbs/publications/idMgmt.SP.pdf

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444 • Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tel: +1 703 439 2120 • Fax: +1 703 326 9881
Email: info@isoc.org