An Introduction to Privacy on the Internet

An Internet Society Public Policy Briefing

30 October 2015

Introduction

Privacy helps reinforce user trust of online services, yet online privacy is under constant pressure of being undermined. Promoting strong, technology-neutral data-privacy laws, privacy-by-design principles, and ethical data-collection and handling principles is a key approach to protecting and fostering online privacy.

Privacy is an important right[1] and an essential enabler of an individual's autonomy, dignity, and freedom of expression. Yet, there is no universally agreed definition of privacy. In the online context, however, a common understanding of privacy is *the right to determine when, how, and to what extent personal data can be shared with others.*

In today's digital age, information gathering is fast, easy, and less expensive than ever. Progress on a variety of technological fronts contributed to this new world. For instance:

- Data storage is cheap, making data accessible online for long periods of time.
- Data sharing can be fast and distributed, enabling data to easily proliferate.
- Internet search tools can recognize images, faces, sound, voice, and movement, making it easy to track devices and individuals online over time and across locations.
- Sophisticated tools are being developed to link, correlate, and aggregate seemingly unrelated data on a vast scale.
- It is getting ever easier to identify individuals - and classes of individuals – from supposedly anonymized or deidentified data.
- There are more and more sensors in objects and mobile devices connected to the Internet.

[1] See *UN Universal Declaration of Human Rights,* http://www.un.org/en/documents/udhr/; *International Covenant on Civil and Political Rights,* http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; and *European Convention on Human Rights,* http://www.echr.coe.int/Documents/Convention_ENG.pdf.

Personal data has become a profitable commodity. Every day, users are sharing more personal data online, often unknowingly, and the Internet of Things will increase this dramatically. These factors have the potential to expose personal data and create privacy challenges on a greater scale than ever before.

With this in mind, it is important to encourage the development and application of privacy frameworks that apply an ethical approach to data collection and handling. Frameworks that incorporate, among other things, the concepts of fairness, transparency, participation, accountability, and legitimacy.

Key Considerations

Although there is no universal privacy or data protection law that applies across the Internet, a number of international and national privacy frameworks have largely converged to form a set of core, baseline privacy principles. The following principles are derived from the Organisation for Economic Co-operation and Development (OECD) *2013 Privacy Guidelines*, and are widely recognized as providing a good foundation for developing online privacy policies and practices:

- **Collection limitation.** There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data quality.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

- **Purpose specification.** The purposes for which personal data is collected should be specified. The use should be limited to those purposes or other purposes that are not incompatible.

- **Use limitation.** Personal data should not be disclosed, made available, or used for other purposes except with the consent of the individual or where authorised by law.

- **Security safeguards.** Personal data should be protected by reasonable security safeguards.

- **Openness.** There should be a general policy of openness about developments, practices, and policies with respect to personal data.

- **Individual participation.** Individuals should have the right to obtain information about personal data held by others and to have it erased, rectified, completed, or amended, as appropriate.

- **Accountability.** Those who collect personal data should be accountable for complying with the principles.

It should be noted that many of these principles imply transparency concerning who is collecting data, and what it is being used for.

Challenges

Policy developers must consider a number of key challenges when determining action related to online privacy. Some widely recognized challenges include:

1. **Determining what data needs to be protected.** Typically, privacy and data protection laws apply to personal data, also known as *personal information* in some jurisdictions. A common definition for personal data is "any information relating to an identified or identifiable individual".[2] Not all definitions are the same. In addition, it can be difficult to determine which specific types of data should be considered personal information in a particular context. Furthermore, the fast-paced evolution of services, as well as the technology used to process data, make determining what should be required to be protected an ongoing challenge.

2. **Different legal data protection requirements.** Privacy laws are not the same across all countries. This means that some data may be legally protected in one country, but not in another. Also, even where the data is covered by the laws of both countries, the protections may vary (e.g., data collection may be opt-in or opt-out). To complicate matters further, more than one country may assert that its laws apply. For example, one country may assert its data protection law applies because the personal data relates to its citizens, while another may assert that its law applies because the company collecting the data is based in its territory. Giving effect to individual's privacy rights and expectations can be especially problematic when countries' laws are in direct conflict or otherwise incompatible. In particular, recent controversies relating to mass surveillance have raised the question of whether "necessary and proportionate" clauses in legislation provide enough protection for citizens. Global debates about surveillance highlight how hard it is for nation states to agree on consistent interpretations of international conventions in the privacy sphere, such on human rights, or civil and political rights.

3. **Protecting privacy when data crosses borders.** The Internet spans national borders, yet privacy and data protection laws are based on national sovereignty. Therefore, special provisions are needed to protect personal data that leaves one country and enters another in order to ensure the continuity of data protection for users. Approaches vary, but tend to have regard to whether the receiving country has "adequate" protection. Various frameworks have emerged to facilitate transborder data flows within a region or between regions.[3]

4. **Real meaningful consent.** Privacy and data protection laws typically permit some degree of collection and use of personal data if the individual gives his or her consent. In theory, this approach empowers Internet users to have some level of control or choice over the way their data is collected and used

[2] For personal data definitions, see: OECD 2013 Revised Privacy Guidelines; Council of Europe Convention 108; EU Data Protection Directive (1995) and AU Convention on Cyber Security and Personal Data Protection.

[3] Example cross-border frameworks include: APEC Cross Border Privacy Rules (CBPR) system, US-EU Safe Harbor Framework, EU Binding Corporate Rules.

by others. However, in practice, users of online services may not read or may not understand what it is that they are agreeing to (e.g., because the terms of service are lengthy and written in complex legal language). Even if they understand the terms, users may be unable to negotiate them. The widespread use of mobile devices with sensors and small screens with which to display privacy options, and frequent secondary uses of personal data (e.g., targeted advertising) create additional challenges for users to exercise control over their personal data. One technical approach might be to encourage the development of systems that make it easier for the user to understand and manage the information that is collected by the intelligent, connected devices surrounding them.

Guiding Principles

As personal data has monetary and strategic value to others, it is a challenge to ensure that it is only collected and used appropriately. The following guiding principles promote achieving this outcome:

- **Global interoperability.** Encourage openly developed, globally interoperable privacy standards (both technical and regulatory) that facilitate transborder data flows while protecting privacy.

- **Collaboration.** Foster multistakeholder collaboration and a holistic approach that ensures value to all stakeholders.

- **Ethics.** Encourage privacy frameworks that apply an ethical approach to data collection and handling. Ethical approaches incorporate, among other things, the concepts of fairness, transparency, participation, accountability, and legitimacy in the collection and handling of data.

- **Privacy impact.** Understand the privacy impact of personal data collection and use. Consider the privacy implications of metadata. Recognize that even the mere possibility of personal data collection could interfere with the right to privacy. Further, understand that an individual's privacy may be impacted even if he or she is not identifiable, but can be singled out.

- **Anonymity and Pseudonymity.** Individuals should have the ability to communicate confidentially and anonymously on the Internet.

- **Data minimization.** Encourage data minimization practices. Insist on selective data collection and use of only the necessary data for only as long as it is needed.

- **Choice.** Empower users to be able to negotiate fair data collection and handling terms on an equal footing with data collectors, as well as be able to give meaningful consent.

- **Legal environment.** Promote strong, technology-neutral laws, compliance, and effective enforcement. These laws should focus on desired privacy outcomes, rather than specifying particular technological means to direct privacy practices.

- **Technical environment.** Encourage open environments that support the voluntary, consensus-based development of protocols and standards that support privacy-enhancing solutions.

- **Business environment.** Encourage businesses to recognise that privacy-respecting approaches can provide competitive advantages and may lower their exposure to legal risk.

- **Privacy-by-design principles.** Promote privacy-by-design throughout the development, implementation and deployment cycle. Privacy-by-design principles should also be applied to the development of standards, applications, services, and business processes.

- **Tools.** Promote the development of usable tools that empower users to express their privacy preferences and to communicate confidentially (e.g., encryption) and anonymously or pseudonymously; and enable service providers to offer choices and visibility into what is happening with user data.

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.

- Internet Society Privacy Resource Page, http://www.internetsociety.org/our-work-privacy.

- Internet Society Digital Footprint Resources, http://www.internetsociety.org/your-digital-footprint.

- Understanding your Online Identity: An Overview of Identity, http://www.internetsociety.org/understanding-your-online-identity-overview-identity.

- Understanding your Online Identity: Protecting your Privacy, http://www.internetsociety.org/understanding-your-online-identity-protecting-your-privacy.

- Understanding your Online Identity: Learning to Protect your Online Identity, http://www.internetsociety.org/understanding-your-online-identity-learning-protect-your-identity.