Resolution
on openness of Personal Data Practices

Recalling the "Resolution on Improving the Communication of Data Protection and Privacy Information Practices" that was adopted at the 25th International Conference of Data Protection and Privacy Commissioners in 2003.

Mindful that the scale and scope of personal data being collected, the ability to analyse this data and the potential uses of this data have increased dramatically.

Noting that openness is a longstanding fair information principle that is reflected in several international instruments, including the "International Standards on the Protection of Privacy and Personal Data" (the Madrid Declaration) that was adopted at the 31st International Conference of Data Protection and Privacy Commissioners in 2009.

Recognising that effective communication of an organisation's policies and practices with respect to personal data is essential to allow individuals to make informed decisions about how their personal data will be used and to take steps to protect their privacy and enforce their rights.

Recognising that transparency about governments' policies and practices with respect to personal data is critical to create and maintain trust, foster citizen engagement and preserve democratic accountability.

The 35th International Conference of Data Protection and Privacy Commissioners therefore **resolves** to:

1. Urge organisations collecting personal data to explain the purposes for which the data are being collected; the identity of, and how to contact, the organisation or responsible individual; and the means to request access to, or correction of, the data;

2. Urge organisations to provide meaningful information about their data collection policies and practices in clear and plain language in an easily accessible format, taking into account the characteristics of the individuals to whom the data relate and the method of collection;

3. Urge organisations, data protection authorities and privacy enforcement authorities as well as governments to consider the usefulness of privacy seals, certification and trustmarks as a way of informing users and enhancing choice;

   and

The United States Federal Trade Commission abstained from voting on this resolution as far as it concerns the public sector for reasons of jurisdiction

4. Urge governments to be more open about their data collection practices, consistent with appropriate national security, public safety and public policy considerations, in order to enhance democratic accountability and to give effect to the fundamental right to privacy.

EXPLANATORY NOTE

At the international level, the principle of openness has roots in the OECD's *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* developed in the late 1970s. Today, this principle is broadly reflected in data protection and privacy laws around the world.

Individuals now expect greater accountability and transparency on the part of both private-sector organisations and their governments with respect to how they collect, use and disclose personal data. However, these expectations are not always respected. In 2013, nineteen authorities from around the globe participated in the first Global Privacy Enforcement Network (GPEN) Privacy Sweep. The participating authorities examined websites in a coordinated effort to assess the transparency of organisations' privacy practices.

The authorities found that one out of every five sites did not have a privacy policy or had a privacy policy that was buried in a lengthy Legal Notice or in Terms and Conditions. Where privacy polices did exist they often restated legal requirements in "boilerplate" language without providing individuals with clear and meaningful information about how their personal information is being used and disclosed. They also found that in a significant number of cases, the sites either did not list contact information to allow individuals to obtain additional information about the organisation's practices or the contact information was difficult to find.

Recent revelations about government surveillance programs have prompted calls for greater openness with respect to the scope of these programs, increased oversight and accountability of these programs and more transparency from the private sector organisations that are required to provide personal data to governments. The revelations have also occasioned debate about the appropriate level of transparency associated with such programs in light of relevant national security, public safety and public policy considerations.