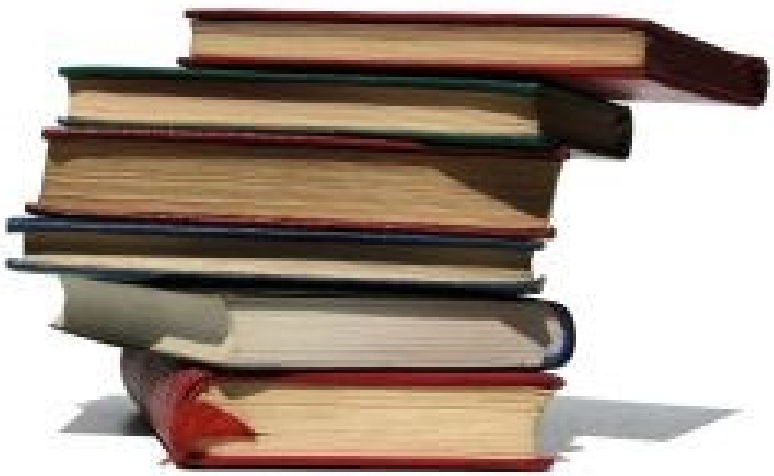
ANEC POCKET GUIDE

Overview of Privacy Guidance for members of standards technical committees who are Consumer Representatives

Key Principles for Digital Device Privacy Impact Assessment



Raising standards for consumers

Disclaimer: this pocket guide is intended for ANEC membership and ANEC representatives in particular.

The following document sets out the consumer and public interest privacy assessment principles that are the basis for consumer digital device and application privacy impact assessment.

1. Remote control over device power

The privacy implications of any remote ability to cause any digital device used by consumers to power up or power down should be evaluated.

The ability for others to turn devices on or off without the user's knowledge or control is fundamental to digital privacy. This principle impinges on for example:

a) Devices connected to systems that can control power to individual devices such as smartphone apps for home electrical power control
b) Future capabilities of smart grid
c) Radio Frequency Identification (RFID) devices including smart cards

2. Eavesdropping digital radio emissions from devices

The privacy implications of eavesdropping radio emissions when a device is powered up and in operation should be evaluated.

When electronic devices are powered up they emit radio waves

- From their own internal operations that can be intercepted and eavesdropped (as an example see Government TEMPEST testing for highly secure installations)
- When connected by radio technology for interoperation with other parts of an ICT infrastructure

This principle impinges on all radio connected devices and radio connection technologies like

a) Wi-Fi,
b) Bluetooth,
c) Mobile phone transmission
d) RFID.

3. Data transmission to and from the connected device (security)

The privacy implications of the device and network security, and any mismatch of security configuration between device and network, should be evaluated.

Digital devices can exchange data with other parts of the ICT infrastructure they are connected to. The evaluation of security to protect privacy should apply whether the data exchange is part of the internal operation of an application where processing is performed beyond the device, or whether it is data collection by another application.

This principle impinges on for example:

a) Home networking
b) Smartphone apps that use cloud services to complete their processing
c) Online games
d) RFID
e) Wifi access to the Internet for home computing and in public places
f) Smart meters

4. User control of data types passed over networks and remote processing of that data

The default when data types are unknown should be evaluation of the most sensitive of personal information being processed and transmitted in both directions.

Where users control the data types (e.g. free text content) passed over the network and processed remotely then the default evaluation should be that the most sensitive of personal information is being transmitted in both directions and processed remotely.

This principle impinges on for example:

a) Consumer use of the Internet
b) Cloud computing services used directly by consumers or as part of distributed processing within consumer solutions and services

5. User personal data sensitivity

The privacy implications of the sensitivity of the data types processed and collected should be evaluated.

Data is held on and collected from domestic activities, whether that collection is inherent within a service being provided by others through the connected digital device, or inherent to the user's own domestic processing. If the data held on or sent across the network by the digital connected device is of low sensitivity then the impact of loss of privacy is lower for some risks.

6. User control over personal privacy preferences

The privacy implications for the degree of privacy preference control available to the user should be evaluated.

Privacy is affected by the degree of control that users have over their own privacy preferences with respect to data collection and data sharing. Past practice was for consent to be given to collection, and then all data types that had been consented to were collected unless consent was withdrawn. This is control that is either on or off. In practice the user sees privacy as much more refined and contextual. Real time privacy controls on devices are beginning to recognise this characteristic of privacy, for example the privacy controls on Apple iPhones.

There are risks of loss of privacy through

- parties with whom data is shared
- consented to real time data collection including data that the user wishes temporarily not to be collected.

This principle impinges on for example:

a) Location data used in applications
b) Frequency and detail in smart meter data collection
c) Information shared through social networks
d) Personal data trading for commercial purposes

7. User behaviours

The privacy implications of user behaviour and their use of digital devices should be evaluated to identify privacy risks brought about by how the device is used in domestic life.

This principle impinges on for example

a) Consumer updating of operating system security on processing devices
b) Propensity to lose mobile devices and smart cards
c) Propensity to misoperate or misunderstand devices in a manner that can increase privacy risks
d) The degree of illicit activity in the market place that utilises features of the technology to trick consumers into loss of privacy / security. Examples: e mails embedding malware or trick links in e mails to spoof web sites to elicit key personal details or security information, fake optical codes added to physical advertising routing consumer's smartphone optical code recognition apps to false web sites.
e) Reduction of privacy risks through user behaviour guided by Privacy Impact Assessment summary information with respect to risks and user mitigation action

8. User privacy exposure arising from organisational security breaches

The risk to privacy should be evaluated for personal data lost or stolen from an organisation leading to the linking of that data to an individual either through

- the data itself
- linking to the device used by the individual

Prepared by Peter Eisenegger

ANEC ICT Working Group

ANEC in Brief

ANEC is the European consumer voice in standardisation, representing and defending consumer interests in the development of technical standards, in the application of conformity assessment schemes to standards, and in the creation or revision of legislation on products and services. ANEC receives funding from the European Commission and the EFTA Secretariat.

ANEC, the European Association for the Co-ordination of Consumer Representation in Standardisation

Avenue de Tervueren 32, box 27 – 1040 Brussels – +32 (0)2 743 24 70

anec@anec.eu - www.anec.eu

http://twitter.com/#!/anectweet

http://companies.to/anec