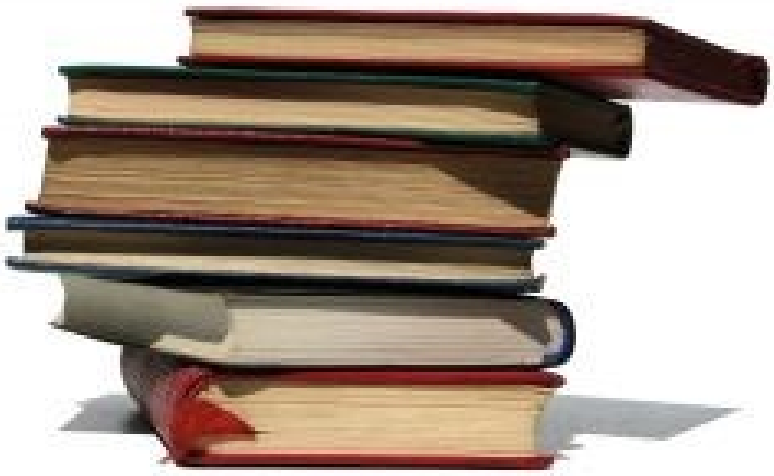
ANEC POCKET GUIDE

Overview of Privacy Guidance for Consumer Representatives in standards technical committees

Key Principles



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 principles that are the basis for the detailed design and good practice requirements as provided in the three detailed guidance documents outlined in section 2 of this overview.

1. Consumer standards representatives

1. Security is fundamental to privacy

Good security prevents unauthorised people from accessing personal information. This principle impinges on

a. The security of processing platforms used by consumers such as smartphones and tablets as well as home networks
b. Maintaining consumer processing platforms security in the light of continuous cyber attacks.
c. The role of the consumer in maintaining their own security and contributing to the public network and private organisation system security. *For example how to avoid picking up malware and spreading it and also getting rid of malware that has embedded itself in the domestic ICT infrastructure*.

2. Within the domestic environment consumers should have complete control over their privacy

Within the domestic environment the processing undertaken by individuals to help them socialise, run and manage their lives should be secure and under their control wherever the processing is undertaken within the global ICT architecture. For example: fitness apps, home environmental control, travel planning etc.

This principle impinges on

a. Home networks and connected devices
b. Cloud computing services for consumers and use of Cloud services by apps.
c. Intelligent cars
d. Parental monitoring and control
e. Control over socially shared data

f. Control over intrusive content including SPAM, Porn, online bullying (see also principle 7), nuisance telephone calls and more

3. When data is collected from consumers then control should be personalised allowing personal privacy preferences to be expressed and changed at any time.

Where consumers consent to data collection as an ongoing process from domestic activities then real time control over their own privacy preferences is needed. This principle impinges on the data collection for

a. Home health
b. Home environmental control
c. Smart meters and smart grid
d. Traffic and navigation systems
e. Smart Cities
f. The Internet of Things and much more

4. Transparency of data sharing

Transparency of data use shall be ensured when personal data is passed to others.

This should apply when individuals have consented to data collection from domestic activities by

- explicitly consenting to their data being passed to and used by others,
- accepting a service where it is necessary to share personal data as part of that service delivery,

Then transparency should be technically implemented to enable the individual to determine easily who the data has been passed to and for what reason(s).

5. Personal data analysis processes should be designed to protect individuals privacy

Where personal data is processed in a manner that it is analysed to inform or influence decisions then precautions are needed to protect privacy. This principle impinges on

a. Governance
b. Identifiability
c. Creation of large data sets that collectively represent much more sensitive personal data than individual data items do by themselves
d. Accuracy of analysis, especially false positives and false negatives which impact individuals
e. Use of personal data analysis for personal risk management within health, finance and many other types of service
f. Big data applications

6. Anonymity when in public domains should be the norm

When in public environments both physical where sensors are used (including cameras) and in virtual environments such as multi-player games, or using the web, individuals should be able to expect their identifiability to be limited to those they already know or the individual has agreed to be identified by, otherwise anonymity should be the norm except where national laws require otherwise.

7. Accountability for statements and views made in public

In public environments individuals should expect to be held legally accountable for the accuracy of their public statements and any harm caused to others as determined by national laws. This principle impinges on

a. Freedom to express personal opinions, which should be maintained
b. Freedom to organise, which should be maintained
c. Cyber bullying
d. Online libel and slander issues

e. Incitement to hatred

f. Twitter trolls and so on

2. Guidance papers based on these principles

Guidance with respect to detailed standards requirements for privacy derived from these seven principles are to be given in 3 papers:

i. Domestic privacy good practice requirements guide

This deals with requirements that support principles 1, 2, 3 as well as the privacy aspects of public domains for principles 6 and 7.

ii. Personal data sharing transparency requirements guide

This deals with requirements that support principle 4.

iii. Personal data analysis privacy requirements guide

This deals with requirements that support principle 5.

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