May 2015

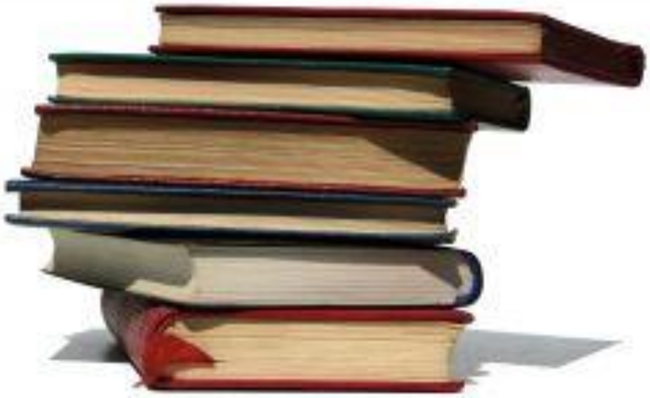
ANEC-ICT-2015-G-064

ANEC POCKET GUIDE

Consumer Representatives Guidance

Domestic Privacy and the privacy of digitally connected devices

For use when representing consumer interests on standards technical committees



Raising standards for consumers

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

Domestic Privacy Guide Contents

digg
You Tube

Bullying

SPAM

8. Personal accountability for online views

8. The principle of being accountable for views and statements made online

Annexes

Annex 1 Examples of personal information

Annex 2 Privacy by design and innovation including the use of Privacy Impact Assessments (PIA's)

Annex 3 Commentary on privacy by design or drones and mobile phone cameras

Section 1. Key privacy concepts for consumer standards guidance

1.1. Privacy standards and the law

Current Data Protection law worldwide, intended to protect consumers' privacy, is firmly established on data protection principles laid down in the 1980's when the digital presence of products and services in consumers' lives was minimal. The main concerns were about the collection and use of individuals data by organisations. The aim of the law was to provide a degree of consumer control over that use via the consent mechanism and the rights of individuals to see and correct data held about them.

Since the 1980's the presence of connected digital devices in the home and consumers' daily lives has grown to a point where digital technology can fairly be seen as pervasive. It is now present in a great many of the goods and services used by individuals in their domestic lives. This digital pervasiveness continues to grow and can be reasonably expected to increase substantially with the advent of Smart Cities and the Internet of Things.

This is one of a series of guidance papers for consumer representatives in standardisation activities, aimed at complementing existing law and supporting the development of privacy by design and market digital privacy good practice from the consumers' perspective.

1.2. Consumer Privacy Environments

1.2.1. The main environments addressed in this guide are those representing consumers' domestic environments, including:

Physical environments such as

House and home, gardens, cars, out and about in public such as in the street, shopping mall or market and public buildings.

Virtual environments such as

Online web access, multiplayer games, 'virtual' meeting places and socially shared areas like Facebook, personal e-mail, blogs

The practical aspects of privacy for domestic life focuses on consumers' digitally connected devices that are the means by which data, about domestic life, is generated, collected and communicated to others.

1.2.2. Consumer privacy beyond the domestic environment is where others, such as businesses, governments and voluntary organisations have collected personal data from individuals and then process that data for many different organisational purposes.

Outside the domestic environment data protection is the main focus for the means by which privacy is protected.

1.3. The privacy principles on which the guidance papers are based

While Data Protection principles address individuals' privacy as regards data about them that is collected by organisations, but for consumers in the 21st Century, who have many digitally-connected devices, privacy is focused on the home and domestic environment and on the precise nature of the technology. This has given rise to the following seven digital device privacy principles, which are used as a foundation for the guidance papers.

1. Security of domestic digital devices is fundamental to domestic privacy
2. Within the domestic environment consumers should have complete control over their privacy
3. When data is collected from consumers then control should be personalised allowing personal privacy preferences to be expressed and changed at any time.
4. Transparency of data sharing should be ensured when personal data is passed to others
5. Personal data analysis processes should be designed to protect individual's privacy

6. Anonymity when in public domains should be the norm

7. While protecting free speech, individuals should be accountability for statements and views made in public digital environments.

1.4. Privacy by Design (PbD)

Privacy is best served when it is designed into products and services from the beginning. Therefore one of the main objectives of the guidance papers is to support digital PbD, where providing digital technology to consumers requires privacy to be designed into products, services, processes and their governance.

This guidance paper deals with current digital design issues and market practices that relate to privacy principles 1, 2, 3, 6 and 7. The guidance is aimed at enabling consumers to live their domestic lives in a reasonably private manner where the degree of privacy and openness of their daily lives is protected and under their own control.

Additional privacy guidance applicable to consumer privacy beyond the domestic environment (see 1.2.2.) is also given in two other guidance papers on:

- Data Sharing Transparency that deals with the digital design issues and market practices that relate to privacy principle 4. These include open data sharing, and the extensive current practices, which share and trade consumers' data in very high volumes globally. Ref "Using Consumer Data: Data transfer, trading and privacy"

  http://www.anec.eu/attachments/ANEC-ICT-2015-G-040.pdf

- Using Consumer Data that deals with digital design issues and market practices that relate to privacy principle 5 where analytical processing of personal data underpins many public and private sector goods and services. This guidance on use of personal data privacy requirements for product and service standards applies also to Big Data, which is a technological step up in the scale of data analysis. Ref "Using Consumer Data Consumer Representatives Guide on Privacy" *http://www.anec.eu/attachments/ANEC-ICT-2015-G-009.pdf*

1.5. Defining Personal Data

It is not unusual to find standards committees debating what personal data is. To help with this issue a good definition of personal data has been provided by the International Standards Organisation in ISO/IEC 29100:

Personally Identifiable Information "PII is any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal"

This practical definition has wide implications on what constitutes personal data. Digitally connected devices process or collect a vast range of data from individuals that can then be used for personal processing or collected by others for other purposes. The range of data that can be considered as personal, i.e. PII, is considered next.

A starting point in understanding the full range of data that constitutes personally identifiable information is through the types of personal information that have been identified in EN 16571: 2014 "Information technology - RFID privacy impact assessment process", a recently published European Standard from CEN. The main types of personal data in EN 16571 are:

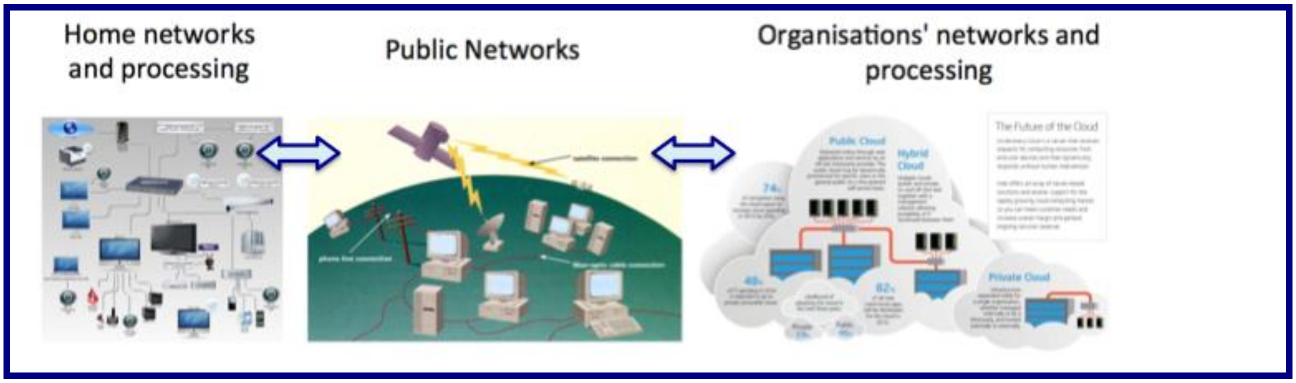
PI	Personal Identifiers
PB	Personal Behavioural data
TH	Technology and Hardware identifiers
IT	Identity of Things identifiers
RV	Residual value
TL	Time/Location data
SD	Sensor Data

Understanding what is meant by these categories is easiest from some examples, and Annex 1 gives several examples and subcategories for these seven personal information types.

1.6. Networks used by digital devices

The domestic processing environment is technically complex and typically consists of networked digital devices connecting both within the home network and externally to public networks. Figure 1 illustrates the breadth and complexity of personal processing within the home and away from it when digital devices are connected to networks.

Figure 1. 21st Century ICT Infrastructure domestic processing of personal data



note: for the purposes of this section the detail in each of the 3 domains in Figure 1 is not significant only that each is in itself complex.

All digitally connected devices have some form of internal processing, and it is the design of the software used to provide or supplement the functions of that device that determines where that processing is undertaken. It is quite possible for a simple-looking home ‘app’ to have software running on the home device, connected over a public network, then partly processed within an organisation’s ICT infrastructure, with some of that processing itself being outsourced to cloud services or similar. Put simply from the (non expert) consumer point of view, consumer domestic processing could be happening anywhere.

1.7. Data processing purposes

In the consumers’ domestic environment, individuals use devices that work using digital processing of data, and that use creates personal digital data. There are two main reasons why consumers use such devices:

i. To do something that is part of their domestic living such as using a fitness ‘app’ on a Smartphone, creating a family budget on a spread sheet, sharing photos with family and friends.

ii. To interact with an organisation in order to receive goods and services from both public and private sector providers.

Sometimes the reason why data is processed in a particular way may be a combination of both i. and ii.

In the case of i. the consumer determines the purpose of the processing while in ii. an organisation determines the purpose. Who determines the purpose of the processing plays a key part in much privacy law and standards. This usually identifies who is to be seen as the ‘controller’ of the processing.

2. Consumer privacy protection through security

2.1. Security is fundamental to privacy

Good security prevents unauthorised people from accessing personal information. For digital connected devices used by consumers 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 the security of platforms processing consumer data in the light of continuous cyber-attacks;

c. The role of the consumers in maintaining their own security, and contributing to system security of public networks and private organisations. *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*.

d. The default security settings of digital devices and network components in the home, which need to balance ease of use with protection of access to data.

2.2 Security Issues

2.2.1. Network and system security

2.2.1.1. A well researched, and informative source of security issues is provided by one of the global leaders in Internet network equipment, CISCO, in their annual security review. From the 2014 report the following should be noted:

CISCO 2014 Annual Security Report

> "Trust
>
> All organizations should be concerned about finding the right balance of trust, transparency, and privacy because much is at stake. In this area, we address three pressures that make security practitioners' attempts to help their organizations achieve this balance even more challenging:

- Greater attack surface area
- Proliferation and sophistication of the attack model
- Complexity of threats and solutions"

Continuous threats

CISCO's own network security monitoring services indicate an increase in new security alerts of between 350-400 per month. These newly exploited security vulnerabilities cumulatively mean that many thousands of known security weaknesses are being exploited globally.

2.2.1.2. The report identifies as the main types of security weakness, A & B in the box below:

A – Action needed by individuals

Those security weaknesses that are dependent on the actions of individuals to lessen security threats in the CISCO report are:

- SPAM mail
- Downloaded malware
- Mobile phones and tablets for personal computing

B – Action needed by organisations

There are also in the CISCO report security weaknesses that depend on organisations addressing the security threats and providing trusted environments

- Organisations web sites and internal processing already 'invaded'
- Internet server infrastructure already invaded

Currently the ISO/IEC Security standards in the ISO 27000 series are dealing with security issues that are addressable by organisational action, "B" in the box above.

However, there is a need for considerably more standards work where the actions of individuals are required to address security weaknesses, as illustrated in by "A" in the box above. This is particularly so when individuals are consumers. Requirements guidance for domestic security protecting individual privacy is provided in the section 2.3.

2.2.2. Consumer digital devices security

2.2.2.1. Consumers' lives are already highly connected through their digital devices and the Internet of Things should be with us soon.

While many key domestic activities are in their Internet of Things (IoT) infancy, Smartphone use has already matured with approximately 2 billion in use globally[1]. Smartphones and tablets are likely to be the main, but not the only, devices used for 'apps' that collect data from sensors, provide useful consumer functionality and control in the domestic environment, thereby increasing the number of privacy threats.

To identify broader issues of security in the connected home the UK OFCOM report "*Study into the Implications of Smartphone Operating System Security*" carried out by Goode Intelligence[2] is a good source of insight.

Goode Intelligence – Security Threats

Vulnerabilities exist on every Smartphone Operating System examined in this study. A vulnerability becomes a problem when it can be exploited. Malware is an example of how a vulnerability is exploited, creating code that exploits weaknesses and bugs, in the Operating System for malicious purposes – to extract personal information or to enact financial fraud on the Smartphone owner. If the vulnerability is not remediated, fixed or patched, in a timely fashion then these exploits will continue and Smartphone owners will be exposed to security threats.

This is why it is imperative to have a robust and efficient Smartphone Operating System software update process that discovers vulnerabilities

[1] http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

[2] http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/smartphone-os/

before the bad guys do, fixes them and then pushes the resultant software update to all affected Smartphone owners before the vulnerability can be widely exploited. This is the first independent study that investigates both the Smartphone Operating System update process and vulnerability management in detail…

The greatest security risk currently for UK Smartphone owners is the threat of a lost or stolen device… In all, 10,000 mobile phones are stolen every month in London with two thirds of the victims aged between 13 and 16.

While this report covers Smartphones, the issues raised are generic and also apply to all forms of home networking and connected devices.

2.2.2.2. Key consumer activities supported by digitally connected devices

The 'apps' world is offering important functionality for consumers in

- Home health
- Childrens' security
- Online purchasing
- Home environmental control
- Home smart appliances
- ... and much more

The Goode report observations relevant to the applications and 'apps' used by consumers are given below.

Goode Intelligence – Technology Control

Mobile app stores are an important component in the Smartphone ecosystem and are the main distribution point for mobile apps…..

There is little evidence that UK consumers are effectively protecting their Smartphones using technology and that they are aware of what the main threats are. Consumers, in the main, do not take personal responsibility for the security of their Smartphones and are relying on the MNOs* to be proactive in securing both the device and ensuring the safe transport of information over the radio network.

** MNOs are Mobile Network Operators*

It should be noted that from the consumer perspective consumers are and always will be inexpert. Consumers buy or use some 700+ goods and services in their daily lives, and have neither the time nor expertise to cope with the technicalities of all 700+ as they get on with living.

When it comes to smart devices it has to be kept in mind that consumers do misunderstand information, make mistakes, forget information and take actions which seem obvious to them which may or may not be the intended action designed into the product or service.

2.3 Maintaining privacy through domestic security

2.3.1. Keeping consumer protection up to date

In order to address the continuous cyber/security attacks on digital connected devices, each element of a device and the networks they are connected to should have a security software updating capability designed in, and this should be backed up with security monitoring and action processes adapted for consumers through building on the ISO 27000 series of standards.

Note: Security updating in the past has mostly been a feature of system software such as bootstrapping BIOS, operating system software and applications/apps. It is now also applicable to network devices (e.g., Internet Routers), network peripherals (e.g., Printers) and indeed any programmable element in the network.

The security updating capability, and processes associated with that, should be easy to understand for users (consumers) and should include:

- Red security alerts
- Automated software updates, ideally with no device shutdown
- Where consumer action is required the information provided to consumers should indicate individual vulnerability and risk of attack wherever possible to motivate consumer action
- Trust in and verification of the source of the security update are absolutely essential

- Security should not be implemented in a manner that limits consumer choice for other goods and services
- Security action should include the possibility of product recall where security issues, like product safety, have generated hardware-based security risks and exploits that are serious and impossible to fix by software update
- No negative impact for the consumer on performance or utility – for example, it should not be necessary for the user to have to re-program a central heating controller with their heating schedule because the security update has deleted the original settings.

2.3.2. Sourcing trustworthy apps and applications

The software made available for consumers to buy and or use on their digital devices should be sourced from trusted suppliers and be subject to rigorous security checking and evaluation both for the software and its sources.

The consumers' digital devices should be able to automatically check that any software to be downloaded has come from valid and trusted sources.

2.3.3. Loss of digital devices

Consumer devices that may reasonably be expected to be mobile or portable should ideally include security features that ensure that :

- the device can be disabled when lost
- key consumer data on the device can be protected
- the device's location can be identified to enable retrieval

2.3.4. Security over a product lifecycle

Security design and update processes should ensure that consumer device security is maintained throughout the lifecycle of the product i.e. through design proving with early users, full launch, midlife and product withdrawal.

Note: Leaving features, such as old versions of operating systems, unsupported by consumer security maintenance processes and design updates while there is a significant number of devices at that design level in use is not good practice, and standards requirements should prohibit such practices.

2.3.5. Consumer security information

As part of continuous security and privacy review and impact assessment, consumers should be informed of:

- Residual security (and privacy) risks and a rating of the severity of those risks
- Any mitigation action that the consumer can reasonably take without incurring costs
- Wherever possible the risk assessment should be relevant to the consumer's individual situation and represented as such.

Note: Detailed technical information with respect to security should be kept easy to understand and actions to resolve difficulties easy to undertake.

3. Consumer control over their own privacy

3.1. The principle of consumer privacy control

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

Within the domestic environment the processing undertaken by individuals to help them run and manage their lives and socialise with others 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:

- Home networks and connected devices
- Cloud computing services for consumers and use of Cloud services by apps.
- Internet of Things, smart appliances including intelligent cars
- Parental monitoring and control
- Control over socially shared data
- Control over intrusive content including SPAM, porn, online bullying

3.2 EU Context for consumer control

3.2.1 EU legal rights Proposed European legislation seeks to improve consumers' control over their domestic data.

"In this fast-changing environment, individuals must retain **effective control** over their personal data. This is **a fundamental right for everyone** in the EU and must be safeguarded.[3]"

The starting point for such effective control lies in the digital devices - hardware and software – used domestically.

3.2.2 Consumer view A BEUC publication **"EU Data Protection Day - Key Messages**" strongly supports this approach too as the extracts that follow show.

"Consumers currently live in a digital 'dark room' in terms of control over the way information including their identity, daily lives, social activities, political views, hobbies, financial data and health records are collected and processed by multiple companies. Billions of euro are made each day by "flourishing" companies (ab)using our personal data....

The right to the protection of personal data should not be eroded or undermined simply because it became easier or more profitable to break it in the digital environment."

http://www.beuc.org/publications/2013-00056-01-e.pdf

3.3 US Context for consumer control

A coalition of 22 groups concerned about privacy in the USA proposed six requirements to be included in the White House's final report on Big Data and the Future of Privacy. One of the six key areas was consumers' control of their data:

"CONTROL: Individuals should be able to exercise control over the data they create or is associated with them, and decide whether the data should be collected and how it should be used if collected."

http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-tells-white-house-team-people-have-right-control-data

[3] Extract from the publication "How does the data protection reform strengthen citizens' rights?" http://ec.europa.eu/justice/data-protection/index_en.htm

Note: The 22 groups were - Advocacy for Principled Action in Government, American Association of Law Libraries, American Library Association, Association of Research Libraries, Bill of Rights Defense Committee, Center for Digital Democracy, Center for Effective Government, Center for Media Justice, Consumer Action, Consumer Federation of America, Consumer Task Force for Automotive Issues, Consumer Watchdog, Council for Responsible Genetics, Electronic Privacy Information Center (EPIC), Foolproof Initiative, OpenTheGovernment.org, National Center for Transgender Equality, Patient Privacy Rights PEN American Center, Privacy Journal, Privacy Rights Clearinghouse, Privacy Times, and Public Citizen, Inc.

The view of the US Federal Trade Commission is expressed in the following speech about the Internet of Things

FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues

International Consumer Electronics Show Las Vegas, Nevada January 6, 2015

“Today, I would like to focus on three key challenges that, in my view, the IoT poses to consumer privacy: (1) ubiquitous data collection; (2) the potential for unexpected uses of consumer data that could have adverse consequences; and (3) heightened security risks. These risks to privacy and security undermine consumer trust. And that trust is as important to the widespread consumer adoption of new IoT products and services as a network connection is to the functionality of an IoT device.

I believe there are three key steps that companies should take to enhance consumer privacy and security and thereby build consumer trust in IoT devices: (1) adopting “security by design”; (2) engaging in data minimization; and (3) increasing transparency and providing consumers with notice and choice for unexpected data uses. I believe these steps will be key to successful IoT business models and to the protection of consumer information.”

http://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf

3.4 Privacy control

3.4.1 Overview

The combination of devices and networks used to provide applications and apps that are used by consumers in their domestic lives should ensure that each individual using an application or app can apply real time control to who, socially and in the family, can access personal data from the application or app that relates to them.

3.4.2 Privacy preferences and control requirements

3.4.2.1. Privacy preference control provided by digitally connected devices should include real time control for the consumer over:

- What the personal data items are that can be accessed by others
- Who can access who's personal data
- When personal data can be accessed
- Where personal data can be accessed
- How personal data can be accessed
- Why the personal data is being accessed

The detail of how such privacy control is provided by the devices will depend on detailed design decisions within the home elements of networks and the hardware, operating systems and application software concerned. As most networking in the home and domestic environment involves equipment from many different suppliers, and, in the case of application software, many different industries, these high level privacy preference control requirements are likely to need specific interoperating standards in order to be practical.

3.4.2.2. Furthermore as discussed in section 1.6, detailed design determines exactly where domestic processing is undertaken, usually in a way that the consumer is unaware of. In such cases real time privacy control should be extended across all the ICT infrastructure involved in the domestic processing no matter where that processing is undertaken.

It is not the intent of this guidance to address the interoperability requirements needed for privacy control purposes in detail, however, such interoperability standards do represent a key element in good practice standards and should be prioritised as such.

3.4.3. Cloud computing services for consumers and use of cloud services by apps

Cloud computing is one of the main examples of distributed processing described in section 1.6. In such cases cloud computing is used to complete the processing required for a consumer's use of an application or app for domestic activities.

As some hundreds of thousands of apps are provided by third parties to consumers with no direct contractual relationship for the consumer with cloud service providers, it is essential to apply both commercial and technical standards that ensure the privacy control elements for domestic use of digital devices (as in 3.4.2.1) are extended into the processing undertaken in the Cloud; and further that Cloud security measures are extended into the processing undertaken by the apps and digitally connected devices.

3.4.4. Internet of Things, smart appliances including intelligent cars

Many possibilities lie ahead with the implementation of smart devices in the home environment and in the extension of that domestic environment within the car.

Two aspects of these developing markets that are addressed elsewhere in this paper are:

- The use of remote control of devices in the home and domestic environment to 'instruct' things to undertake actions; see section 3.4.5
- The concerns of industry, that consumer privacy worries will slow the rate of innovation that is possible; see Annex 3

Note: Industry concerns about innovation being slowed by privacy concerns apply to other ICT technology areas too such as Big Data.

3.4.5. Remote control requirements

Secure access to remote control facilities should be under the direct real time control of the consumer, so that access to remote control is only possible for those allowed by that consumer. An example in the social context could be allowing house monitoring and false alarm shut down by friends when the consumer is on holiday.

When authorisation for remote control by other people is offered in a product or service, then the consumer should have complete real time control over any control instructions issued by those people to the consumer’s equipment s. A commercial example of this could be smart grid instructions to turn off devices in the home to manage electricity demand, where the consumer, and not the electricity company, should have overriding control of which devices may be turned off.

3.4.6. Responsible persons and personal privacy

3.4.6.1 There are some key consumer contexts where a responsible third party may be involved in privacy control. Examples include parents or guardians of children, and those with responsibility for looking after people who may not have, or are losing adequate capability to take such decisions.

Outlined in the following sub-sections are two aspects for which standards need to be developed carefully:

- Non-technical processes and advice;
- Technical shared control capabilities to be implemented to enable a sharing of privacy control between the person whose privacy it is (the PII Principal) and those recognised as having a legitimate role in their upbringing and or care.

The following two boxes give some current perspectives concerning children and mental health issues.

Example 1. UK Children’s charity the NSPCC

Talking to your child – openly, and regularly – is the best way to help keep them safe online.

You might find it helpful to start with a family discussion to set boundaries and agree what's appropriate. Or you might need a more specific conversation about an app or website your child wants to use or something you're worried about.

If you're not sure where to start then here's the advice you need – great ways to begin conversations to keep your child safe online.

The risks and dangers of being online

- Inappropriate content, including pornography
- Ignoring age restrictions
- Friending or communicating with people they don't know
- Grooming and sexual abuse
- Sharing personal information
- Gambling or running up debts

http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Example 2: The Royal College of Psychiatrists: Carers and confidentiality in mental health

"consent: for the professionals, the most important issue is the agreement of the patient to the disclosure of information to the carer. Many patients and carers are unaware of this and do not realise that the patient must give consent before any information can be shared. Complex issues can arise when the patient is unable to give 'informed consent', for example at certain times during an acute episode or when the patient has dementia."

http://www.rcpsych.ac.uk/healthadvice/partnersincarecampaign/carersandconfidentiality.aspx

3.4.6.2 Non-technical processes and advice

Standards in this sensitive area need to ensure that there is good governance of the processes involved to provide someone else with shared privacy control provided via a digitally connected device. Also there should be advice to the consumers involved about good practice within families or by voluntary carers.

3.4.6.3 Technical requirements for shared privacy control

- The person to whom the data relates should provide consent to someone else having control over their privacy and data collection. The parent or 3rd party assigned detailed privacy control should be provided with the same level of privacy control as normally provided to consumers. (see 3.4.2).

- The person to whom the data relates should be able to remove consent to shared privacy control.
- As people's decision taking capability varies over time, governance of the overall shared privacy control process should allow for the on-going level of decision taking capability that the person (PII Principal). For example, young children grow up and take on more responsibility for their own lives while some elderly may become less capable over time.
- Parents should be able to monitor their children's use of apps and online services as a technical facility but subject to the overall agreement and consent of the child, taking account of his/her development and reasoning capabilities.

4. Control over socially-shared information

4.1. Overview

There are two main areas of concern about social sharing, illustrated by A and B in the box below:

A "Aware and Obama (2009) state: Far too many users believe that their postings on the Internet are private between them and the recipient. The reality, however, is that once the statement is typed, it can be copied, saved and forwarded. In addition, the user no longer owns all the information posted to social networks…."

B "However social sharing networks do not only raise privacy issues regarding the people sharing content about them. Lipton (2009: 4) claims:"We are witnessing the emergence of a worrying new trend: peers intruding into each other's privacy and anonymity with video and multi-media files in ways that harm the subjects of the digital files." There are no rules or regulations to protect individuals from accidentally having an embarrassing photo or video taken of them and then posted on the web for others to see. Using the words of Lipton (2009) again: "While copyright law has proved extremely effective in protecting property rights online, it is of little assistance to those seeking to protect privacy."

http://social-networks-privacy.wikidot.com/

It is helpful to be clear that sharing comprises a number of different roles for consumers:

- Providers of the shared information

- Receivers of the shared information

- Other people with personal information contained within the shared information

4.2. Data sharing requirements (with respect to A in the box above)

As things stand, usually sharing systems do not control who can receive the shared information, and so that shared information received can be made available to (as with social networking) or passed to (as with e mail systems) others with whom the originator may well wish not to share that information.

To address this lack of sharing control for the consumer (PII Principal) as personal information provider, standards should include the ability to provide personalised control over who, what why when and how information is shared.

Depending on the degree of control an individual wishes to exercise this may involve:

- Distribution lists for mail and social networks that limit distribution to only those identified by the PII Principal ie removal of forwarding or further sharing facilities
- Controls for the provider that remove the ability to copy their shared information that apply once the information is shared
- Notification to the provider of who else can see or has accessed to shared information passed on by others
- The ability for those receiving shared information to request permission from the PII Principal provider for further sharing of information beyond existing limitations
- The ability for the PII Principal to grant permissions for wider sharing than that arising from initial sharing constraints
- In order to address 'oversharing', especially by children, the ability should be included for the PII Principal, or their responsible third party, to remove or limit initial permissions with

access to the previously shared information being removed for those who have been excluded by the change in permissions.

4.3. Requirements for personal information-sharing receivers (with respect to B in the box above)

When shared information from one individual contains personal information pertinent to another, then standards should include the ability to provide:

- Notification from the individual to whom the personal information is pertinent to the original PII Principal sharer to remove, obscure or limit the availability of that content pertinent to the requesting individual.
-
- Escalation processes, should requests to act have not been addressed by information sharers, whereby those who have requested some limitation on the visibility of that information pertinent to themselves can request action by service providers to remove, obscure or limit availability of the information that is their own PII.
-
- Good governance processes to ensure that such action to remove, obscure or limit availability of an affected individual’s PII is only exercised when justified against clearly understood and transparent criteria.

4.4. Privacy when an individual is identifiable in someone else’s shared data (with respect to B in the box above)

Currently this section of the guidance relates to digital pictures, videos and multimedia content containing information about individuals that has been digitally captured by others, who then share that content with others.

There is a need for guidance for consumers who have captured such images in dealing with requests from “captured” individuals to remove or obscure images of that individual from shared data.

Some of the technical issues relating to this issue are commented on in Annex 3.

5. Privacy and intrusive content

5.1. Overview

For the consumer, intrusive content includes SPAM, online pop-up advertisements, porn, online bullying (see also section 8), nuisance telephone calls and more. Such intrusion can be made through direct communication with the individual, and also by use of other mechanisms such as social media. Many of the intrusive types of content reach consumers with their source concealed (or at least not obvious).

For many types of intrusive content, only those on the receiving end of the content can identify whether it is unwanted and so intrusive.

The following guidance for standards is aimed at addressing generically the many technical means by which intrusive content may reach consumers for example:

- search engines returning porn sites from global searches where such sites look to be non-porn until accessed;
- marketing telephone calls targeted at individuals;
- bullying on social media.
- proliferation of unwanted pop-up and other advertising content which degrades the value and utility of the information the user is seeking

5.2. Privacy requirements for intrusive content

5.2.1. Privacy by design should be supported by standards that provide the ability for the consumer to notify service providers that the particular communication received has been intrusive and unwanted.

- This notification should be automated as much as possible through a digital process supported by the digitally connected devices that receive the intrusive content.

Note: The practical reason for this guidance is to support privacy design for digital devices whereby automatic technical data capture is possible that may assist with identification of the source of the content.

- Where such capability is available then such data should be automatically forwarded to the service provider with the report of intrusion.

Note: ideally the relevant service provider will be the originator of the content, but on occasions that may be the intermediate digital service provider like an Internet Service Provider or Social media web site because the identify and location of the originator is concealed therefore requiring further investigation.

5.2.2. Privacy by design should be supported by standards that provide for

- Blocking by service providers of further intrusive content to individuals once the source has been identified. An example of this is lists of porn sites as unsuitable for children within ISPs which are activated as filters by parental controls.
- Blocking of or diversion of intrusive content identified by an individual at the digital connected device. An example of this are SPAM filters on e-mail systems.

5.3. Intrusive (false) control commands protection

The first line of defence against unwanted control instructions coming from outside the domestic environment to control devices in the home, car or about the body, as part of the Internet of Things, has to be the security access control, and especially security software updates designed into the digitally connected devices (see section 2.3.)

Additional intrusive control instructions requirements for Privacy by Design.

- In addition to the guidance in section 2.3 digitally connected devices that can be controlled remotely should assist in protecting privacy by including control instruction monitoring capability that can be easily used by consumers to check whether unwanted device control instructions have entered the domestic environment.

Note In the case of legitimate remote control incoming control instructions see section 3.4. on privacy controls.

6. Privacy control over data collection

6.1. The principle of consumer data collection privacy control

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 part of their own domestic activities, then real time control over their own privacy preferences is needed. This principle impinges on data collection for

- **a.** Home health
- **b.** Home environmental control
- **c.** Smart meters and smart grids
- **d.** Traffic and navigation systems
- **e.** Smart cities
- **f.** "Big Data"
- **g.** The Internet of Things and much more

The impact of this principle is very similar to that of Principle 2, whereby complete privacy control should be provided, but with a refinement. If a consumer limits data collection for privacy reasons then that may mean that some of the data collecting organisation's ability to provide service may be reduced too.

6.2. Commentary on data protection and data minimisation

The current situation with respect to consumer data collection is illustrated in the following box:

> "**Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer**: Data brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction. Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new

records each month to its databases. Most importantly, data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers has 3000 data segments for nearly every U.S. consumer."

http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Although Data Protection law requires data minimisation the guidance in this paper has been formulated around the practicalities that apply in very many data collection situations. In reality:

- many consumers will not appreciate what is being collected or the significance of that to their privacy when initial consent is given;
- many organisations will struggle to minimise data collection in practice;
- currently, collection is out of control due to embedded consent in terms and conditions, that have to be agreed to in order to obtain goods or services.

So the requirements guidance is aimed at providing a pragmatic approach, which assumes a great deal of personal data will be collected. Much of this will not always be relevant to the prime processing purpose, even though it is collected by an application run by a given organisation.

Note: The approach outlined in this section 6.2, while enabling individuals to exercise a high degree of privacy control if they so choose, enables better use of data to improve consumers and citizens lives as being proposed for smart cities, big data applications and open data initiatives.

6.3 Privacy requirements for data collection

6.3.1. Data collection control requirements

It is recommended that the overarching requirements guidance to apply privacy control of real time on-going data collection is as given in section 3.4.2

6.3.2. Service impacts

Should a consumer choose to reduce data collection through privacy preference control, then that reduced data collection may impact on the service levels that can be provided to consumers. There are three categories of potential service reduction need to be considered for the purposes of this guidance:

a) **Peripheral** to service delivery

This means that core service can be provided without the data being collected. An example would be detailed grocery purchases data on a supermarket loyalty card. Disabling the relevant data collection represents a temporary withdrawal of consent via the privacy control and it can be expected to affect 'fringe benefits'.

The privacy control may be temporary or longer term and what peripheral benefits are impacted may change with the length of time that data collection is disabled by the consumer.

b) **Important** to service delivery

This means that service can continue to be delivered but with some reduction in features and facilities available during the period that privacy control has disabled data collection.

For example, a home security system can detect intruders and transmit video; disabling the video transmission for privacy leaves the system working but with reduced utility.

c) **Essential** to service delivery

This means that core service cannot be delivered and the consumer has to acknowledge that service will not be available while that particular data collection element is disabled. An example would be using privacy control to disable location data collection for a 'find a place to eat' app.

6.3.3. Consumer privacy/service interaction

Good practice standards should include feedback mechanisms to the consumer when a privacy control would impact on the level of service being received to allow the consumer to review and confirm or rescind the privacy preference expressed.

7. Privacy in public places

7.1. The principle of anonymity

Anonymity should be the norm when consumer information is in the public domain.

When in public environments - both physical where sensors are used (including cameras) and in virtual, such as in multi-player games, or in using the web, individuals should be able to expect their identifiability to be limited to people they already know, or cases where they have agreed to be identifiable. Otherwise, anonymity should be the norm except where the law requires it.

The need to support this principle is illustrated by the boxed quotation below from the Electronic Freedom Federation in their comments submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression.

> "Almost all international conventions on human rights protect the right to privacy.[1] Article 17 of the International Covenant on Civil and Political Rights, one of the most important international instruments, provides that:
>
> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
>
> *https://www.eff.org/files/filenode/unspecialrapporteurfoe2011-final_3.pdf*

7.2. Anonymity good and bad

This area of guidance on requirements deals with possibly the most sensitive privacy issues where the needs of countries' security and law enforcement directly clash with the need for individual's privacy.

Anonymity has many beneficial effects when individuals face major organisations' and countries' oppressive practices, but equally anonymity can protect those carrying out horrendous crimes. Both aspects of anonymity are illustrated by the web links in the box below:

The Onion Router (TOR) - good

"Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by the military, journalists, law enforcement officers, activists, and many others"

https://www.torproject.org/about/torusers.html.en

The Onion Router (TOR) - bad

Tor's most visited hidden sites host child abuse images

http://www.bbc.co.uk/news/technology-30637010

7.3. Personal Data Analysis that removes anonymity

Individuals can only be identified digitally if some of their personal information (PII) has been collected and processed (analysed) to identify them. The standards requirements guidance for such collected data processing is provided in the guidance on use of consumer data in the section on analysis whose purpose is to identify individuals. Ref: Using Consumer Data Consumer Representatives Guide on Privacy *http://www.anec.eu/attachments/ANEC-ICT-2015-G-009.pdf*

The main aspect addressed in that guidance for this issue is the need for transparent and fair governance of the identification process and analysis.

7.4. Anonymity when personal data is obtained from sensors

Currently this mainly applies to cameras and in time, as the Internet of Things develops, other types of sensor too. Sensors are not currently designed to discriminate in a way that supports privacy and so the practical way of addressing this is via the approach in section 5.2.2. above when the sensors are used by organisations and section 4.4. when private individuals have captured camera and sensing data about others.

8. The principle of being accountability for statements and views made online

In public, socially shared, and personal environments, individuals should expect to be held legally accountable for any harm caused to others as determined by national laws and the accuracy of their public statements. 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

This aspect of privacy and other individual’s impact on a consumer’s privacy are addressed by use of section 5.2. whereby individuals can identify content that they consider intrusive, and the subsequent governance and processes applied to intrusive content by the service organisation to whom that ‘intrusion signal’ has been sent.

Annex 1 – Examples of personal information (Personally Identifiable Information)

Type PI - Personal identifiers

Identity data *:*

Name

Address

E mail address

Identity confirmation data

Birth certificates

Pictures

Biometrics

Identity characteristics data

Blood group

Date of birth/age

Nationality

Married status

Sex

Service reference data

Account codes

Invoice references

Patient reference number

Tax reference number

Passport number

Type PB – Personal Behaviour identifiers

Long term behaviours

Sexual orientation

Religion

Union membership

Political views

Short term/transient/ variable behaviours

Domestic use of services data

Smart utility bills

Bank account statements

Credit and debit card use

Other personal finance information

Professional service data

Service record of an individual

Medical records

Wage and salary records

Court offences and spent convictions

Complaints

Professional opinions

Diagnosis

Analysis

Books from library

Grocery/product purchases

School homework *Friends and family e-mail content*	
Communication data *Web sites visited* *Telephone numbers called* *E mails sent/received (end addresses not content)*	
Domestic data *:* *My notes* *My contacts* *My photos* *My budget* *My views and opinions*	*My letters and mails (content)* *My fitness and diet* *My diary* *Telephone records* *My travel details*
Types TH and IT Technology and Hardware codes, Identities of Things *IP addresses* *RFID chip codes* *Mobile phone ID* *Product codes*	**Type RV – Value/Residual Value data** *Value on travel card* *Value on payments card* *Value of product* *Bank account balance*
Type TL - Time / Location data *Time* *Location* *Note these can also be given with sensor data too*	**Sensor data** *Camera images (still and video)* *Medical measurements* *Movement* *Temperatures* *Pressures* *Fault alarms* *Biometrics readers*

Annex 2 Privacy by Design and innovation including the use of Privacy Impact Assessments

A2.1 Consumer involvement in development

There are many good reasons for involving consumers directly in new product and service development.

In order to reduce the factors in early design that may impact on privacy early user trails and feedback should be incorporated in the innovation and development process. Such early user involvement should bring out a number of operational and design issues including any significant privacy issues.

A2.2 The role of Privacy Impact Assessments (PIA's)

Privacy by design, as outlined in 1.4, should make use of Privacy Impact Assessments undertaken during the design process for products or services that consist of, or incorporate a digital consumer device. Privacy assessment should iterate with the development process to ensure privacy protection and control is built into the design.

In the last phases of design a PIA should be used to provide the basic information needed by consumers once the product or service is launched. This information includes any level of residual privacy risk as well as any mitigation actions that needs to be taken by users to achieve that level of residual risk.

As the PIA is the source of key consumer privacy information it is important that a consistent privacy risk assessment approach should be used for all digitally connected consumer devices. This would help consumer choice and enable a reasonably level playing field for all the industries involved in consumer markets.

To this end wherever possible the same privacy risk assessment framework developed in the EU for peripheral technology should be used. There is now a European Standard on the RFID privacy impact process - EN 16571:2014 which incorporates a risk rating framework adapted from an ISO/IEC 27005 security risk assessment methodology.

In this approach to achieve a PIA risk assessment the rating of three factors are added together to provide an overall score. These are:

- A rating of the sensitivity of the personal data that might be at risk rated from 0-4
- A rating of how vulnerable the design is to privacy threats rated from 0-3
- A rating of how likely it is that the vulnerability would be exploited rated from 0-3

Of these three factors the one that often gives rise to most contentious debate is how likely it is that privacy vulnerabilities will be exploited.

Assessing the reality of risks

The European Standard on the RFID privacy impact process - EN 16571:2014 has adopted a useful approach to this key risk factor in that PIA process which is based on :

Privacy Risk likelihood rating

0 = not an exploit that is physically possible within the design and hence no theoretical risk

1 = a theoretical risk that has been demonstrated in research papers from reputable sources

2 = proof of concept (ie a practical demonstration) that has been demonstrated by acknowledged security and privacy researchers

3 = privacy /security breaches that have occurred in practice in the market place

More guidance for Privacy Impact Assessment is available in the guide on the “Key Principles for Digital Device Privacy Impact Assessment” paper.

Ref: Key Principles for Digital Device Privacy Impact Assessment

http://www.anec.eu/attachments/ANEC-ICT-2015-G-008.pdf

Annex 3 A commentary on privacy by design for drones and mobile phones cameras

For there to be a technological solution to consumers taking pictures of other consumers when that is not wanted, then considerably more development would be needed than is visible in the market at the moment.

For example, and only as an illustration of technical approaches that might be considered:

- Mobile phones might be given the capability to sense other mobile phones nearby and their owner's privacy setting for being observed by others, and then the camera, when pointing in that direction, would edit the image.

- Drones and their controlling apps might be equipped with map information showing residential areas that could be linked to on board GPS and direction sensors to turn the camera off when flying over domestic premises.

Such "thought experimentation" is a significant step up on current designed-in capabilities and would require new sets of standards to be developed to allow such capabilities to be widely used.

Author Pete Eisenegger

p.eisenegger@btinternet.com

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

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

facebook http://companies.to/anec