Chapter 5
Safeguards

The multiplicity of threats and vulnerabilities associated with AmI will require a multiplicity of safeguards to respond to the risks and problems posed by the emerging technological systems and their applications. In some instances, a single safeguard might be sufficient to address a specified threat or vulnerability. More typically, however, a combination of safeguards will be necessary to address each threat and vulnerability. In still other instances, one safeguard might apply to numerous treats and vulnerabilities.

One could depict these combinations in a matrix or on a spreadsheet, but the spreadsheet would quickly become rather large and, perhaps, would be slightly misleading. Just as the AmI world will be dynamic, constantly changing, the applicability of safeguards should also be regarded as subject to a dynamic, i.e., different and new safeguards may need to be introduced in order to cope with changes in the threats and vulnerabilities.

For the purpose of this chapter, we have grouped safeguards into three main categories:

- Technological
- Socio-economic
- Legal and regulatory

5.1 Technological safeguards

The main privacy-protecting principles in network applications are:

- Anonymity (which is the possibility to use a resource or service without disclosure of user identity)
- Pseudonymity (the possibility to use a resource or service without disclosure of user identity, but to be still accountable for that use)
- Unlinkability (the possibility to use multiple resources or services without others being able to discover that these resources are being used by the same user)
- Unobservability (the possibility to use a resource or service without others being able to observe that the resource is being used).

D. Wright et al. (eds.), *Safeguards in a World of Ambient Intelligence*.

The main difference between existing network applications and emerging AmI applications is twofold: first, in the former case, the user has some understanding of which data about him are collected, and has some means to restrict data collection: e.g., to use a public computer anonymously to access certain Web pages; to switch off his mobile phone, to pay cash instead of using a Web service, etc. In the latter case, with the environment full of numerous invisible sensors (which might include video cameras), it is difficult (if not impossible) for users to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity. Achieving anonymity is impossible if personal data are stored in a personal device (it is obvious that the data belong to the device owner) or in a video recording, as often suggested in AmI applications.

A second important difference between existing network applications and emerging AmI applications is that neither mobile devices nor Web usage penetrates through strong privacy-protecting borders such as walls (it is rarely 100 per cent certain who sends a request from a particular IP address or uses a mobile device) and the human body, while physiological, video and audio sensors, proposed for AmI applications, will have much stronger capabilities to identify a person, to reveal personal activities and feelings and to record them for future use (e.g., as in memory aid applications, which would allow a playback of events). Today, most of us are probably happy that some things are forgotten, but in an AmI world, everything may be remembered and nothing forgotten – if not in an individual memory then somewhere in the AmI system.

Furthermore, unlike most traditional computer applications, interactions in an AmI world are often envisioned to be initiated by technology (e.g., reminding a person to do something or opening an office door after verifying a user), which could be privacy-invasive in some situations, for example, if the AmI system reminds a user to pop his Prozac at a time when the user is in an important business meeting.

Future AmI applications in personal devices and smart environments will require stronger safeguards than today, many of which are not yet fully developed. Intelligent reasoning algorithms, limiting linkability and implementing strong access control to collected data, seem a promising way to protect privacy in AmI applications. However, if laws or poor access control allow the police, intelligence agencies or family members to search through personal data, AmI applications present potential privacy threats not only to the data subject, but also to other people who just happen to be in the background, just as today when we take a friend's photo in a busy street, other passers-by are also captured in the photo. The owner of an AmI memory aid might discover some interesting facts or faces in the background to which he had not paid any attention at the time he or she was concentrating on the main subject of conversation.

Current state-of-the art privacy protection is such that most efforts are concentrated on privacy protection in networked applications in the context of *current* technology, but even today current privacy protection mechanisms are far less mature than the technologies that can collect data. The distance between privacy-protecting technologies and data-capturing technologies is only like to grow. The

PRIME project, which studied the state of the art in privacy protection in network applications in 2005, pointed out many performance problems and security weaknesses.[1] The challenges in privacy-enhancing technologies for networked applications include developing methods for users to express their wishes regarding the processing of their data in machine-readable form ("privacy policies") and developing methods to ensure that the data are indeed processed according to users' wishes and legal regulations ("licensing languages" and "privacy audits": the former check the correctness of data processing during processing, while the latter check afterwards and should allow checking even after the data are deleted).

Privacy protection research is still new, and research on privacy protection in such emerging domains as personal devices, smart environments and smart cars is especially still in its infancy.[2] Privacy protection for personal mobile devices is particularly challenging due to the devices' limited capabilities and battery life. For these domains, only generic guidelines have been developed (see Lahlou et al.[3]). Langheinrich et al. show how difficult it might be to apply fair information practices (as contained in current data protection laws) to AmI applications.

Most of the research on privacy protection is concerned with dangers of information disclosure. Other privacy aspects have not received much attention from researchers. For example, the privacy aspect known as "the right to be let alone" is rarely discussed by technology researchers, despite its importance.

5.1.1 Research on overcoming the digital divide

Research is needed with regard to overcoming the digital divide in the context of AmI. The European Commission has already been sponsoring some research projects which form a foundation for needed future initiatives. Projects dealing with accessibility for all and e-Inclusion (such as COST219: "Accessibility for all to services and terminals for next generation mobile networks", ASK-IT: "Ambient intelligence system of agents for knowledge-based and integrated services for

[1] Camenisch, J. (ed.), First Annual Research Report, PRIME Deliverable D16.1, 2005. http://www.prime-project.eu.org/public/prime_products/deliverables/rsch/pub_del_D16.1.a_ec_wp16.1_V1_final.pdf

[2] Such research is, however, going on. An example is the EC-supported CONNECT project, which aims to implement a privacy management platform within pervasive mobile services, coupling research on semantic technologies and intelligent agents with wireless communications (including UMTS, WiFi and WiMAX) and context-sensitive paradigms and multimodal (voice/graphics) interfaces to provide a strong and secure framework to ensure that privacy is a feasible and desirable component of future ambient intelligence applications. The two-year project started in June 2006. http://cordis.europa.eu/search/index.cfm?fuseaction = proj.simpledocument&PJ_RCN = 8292795

[3] Lahlou, S., and F. Jegou, "European Disappearing Computer Privacy Design Guidelines V1", Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003.

mobility impaired users") are concerned with standardisation, intuitive user interfaces, personalisation, interfaces to all everyday tools (e.g., domotics,[4] home health care, computer accessibility for people with disabilities and elderly people), adaptation of contents to the channel capacity and the user terminal and so on.

Standardisation in the field of information technology (including, e.g., biometrics) is important in order to achieve interoperability between different products. However, interoperability even in fairly old technologies (such as fingerprint-based identification) has not yet been achieved.

5.1.2 Minimal data collection, transmission and storage

Minimising personal data should be factored into all stages of collection, transmission and storage.[5] The goal of the minimal data transmission principle is that data should reveal little about the user even in the event of successful eavesdropping and decryption of transmitted data. Similarly, the principle of minimal data storage requires that thieves do not benefit from stolen databases and decryption of their data. Implementation of anonymity, pseudonymity and unobservability methods helps to minimise system knowledge about users at the stages of data transmission and storage in remote databases, but not in cases involving data collection by and storage in personal devices (which collect and store mainly the device owner's data) or storage of videos.

The main goals of privacy protection during data collection are, first, to prevent linkability between diverse types of data collected about the same user and, second, to prevent surveillance by means of spyware or plugging in additional pieces of hardware transmitting raw data (as occurs in wiretapping). These goals can be achieved by:

- Careful selection of hardware (so that data are collected and transmitted only in the minimally required quality and quantity to satisfy an application's goals, and there are no easy ways to spy on raw and processed data)
- An increase of software capabilities and intelligence (so that data can be processed in real time)
- Deleting data as soon as the application allows.

In practice, it is difficult to determine what "minimally needed application data" means. Moreover, those data can be acquired by different means. Thus, we suggest that data collection technologies less capable of violating personal privacy

[4] Domotics is the application of computer and robotic technologies to domestic appliances. Information and communication technologies are expected to provide for more comfort and convenience in and around the home. See www.domotics.com.

[5] Minimisation is a goal but has to be balanced against the need for data to provide services.

expectations be chosen over those more privacy-threatening technologies even if the accuracy of collected data decreases.

Software capabilities need to be maximised in order to minimise storage of raw data and avoid storage of data with absolute time and location stamps. We suggest this safeguard in order to prevent accidental logging of sensitive data, because correlation of different kinds of data by time stamps is fairly straightforward.

These safeguards are presented below in more detail:

- In our opinion, the most privacy-threatening technologies are physiological sensors and video cameras. Physiological sensors are privacy-threatening because they reveal what's going on in the human body and, accordingly, reveal health data and even feelings. Video cameras, especially those storing raw video data, are privacy-threatening because they violate people's expectations that "nobody can see me if I am hidden behind the wall" and because playback of video data can reveal more details than most people pay attention to in normal life. We suggest that usage of these two groups of devices should be restricted to safety applications until proper artificial intelligence safeguards (see below) are implemented.
- Instead of logging raw data, only data features (i.e., a limited set of pre-selected characteristics of data, e.g., frequency and amplitude of oscillations) should be logged. This can be achieved by using either hardware filters or real-time preprocessing of data or a combination of both.
- Time and location stamping of logged data should be limited by making it relative to other application-related information or by averaging and generalising the logged data.
- Data should be deleted after an application-dependent time, e.g., when a user buys clothes, all information about the textile, price, designer, etc., should be deleted from the clothes' RFID tag. For applications that require active RFID tags (such as for finding lost objects[6]), the RFID identifier tag should be changed, so that links between the shop database and the clothes are severed.
- Applications that do not require constant monitoring should switch off automatically after a certain period of user inactivity (e.g., video cameras should automatically switch off at the end of a game).
- Anonymous identities, partial identities and pseudonyms should be used wherever possible. Using different identities with the absolute minimum of personal data for each application helps to prevent discovery of links between user identity and personal data and between different actions by the same user.

[6] Orr, R.J., R. Raymond, J. Berman and F. Seay, "A System for Finding Frequently Lost Objects in the Home", *Technical Report* 99-24, Graphics, Visualization, and Usability Center, Georgia Tech, 1999.

5.1.3 Data and software security

Data and software protection from malicious actions should be implemented by intrusion prevention and by recovery from its consequences. Intrusion prevention can be active (such as antivirus software, which removes viruses) or passive (such as encryption, which makes it more difficult to understand the contents of stolen data).

At all stages of data collection, storage and transmission, malicious actions should be hindered by countermeasures such as the following:

- Cryptography
- Watermarking: a method to conceal a message in such a way that the very existence of the embedded message is undetectable
- Antivirus software and firewalls
- User-friendly updates of antivirus and firewall software
- Self-healing methods for personal devices, e.g., switching to redundant functionalities in the event of suspicious execution delays or spyware detection
- Detection of changes in hardware configuration
- Usage of trusted hardware modules
- Secure establishing of ad hoc communications.

5.1.4 Privacy protection in networking (transfer of identity and personal data)

Privacy protection in networking includes providing anonymity, pseudonymity and unobservability whenever possible. When data are transferred over long distances, anonymity, pseudonymity and unobservability can be provided by the following methods: first, methods to prove user authorisation locally and to transmit over the network only a confirmation of authorisation; second, methods of hiding relations between user identity and actions by, for example, distributing this knowledge over many network nodes. For providing anonymity, it is also necessary to use special communication protocols which do not use device IDs or which hide them. It is also necessary to implement authorisation for accessing the device ID: currently, most RFID tags and Bluetooth devices provide their IDs upon any request, no matter who actually asked for the ID. Another problem to solve is that devices can be distinguished by their analogue radio signals, and this can hinder achieving anonymity. Additionally, by analysing radio signals and communication protocols of a personal object, one can estimate the capabilities of embedded hardware and guess whether this is a new and expensive thing or old and inexpensive, which is an undesirable feature.

Unobservability can be implemented to some extent in smart spaces and personal area networks (PANs) by limiting the communication range so that signals do not penetrate the walls of a smart space or a car, unlike the current situation when two owners of Bluetooth-enabled phones are aware of each other's presence in neighbouring apartments.

Methods of privacy protection in network applications (mainly long-distance applications) include the following:

- Anonymous credentials (methods to hide user identity while proving the user's authorisation).
- A trusted third party: to preserve the relationships between the user's true identity and his or her pseudonym.
- Zero-knowledge techniques that allow one to prove the knowledge of something without actually providing the secret.
- Secret-sharing schemes: that allow any subset of participants to reconstruct the message provided that the subset size is larger than a predefined threshold.
- Special communication protocols and networks such as:
  - Onion routing: messages are sent from one node to another so that each node removes one encryption layer, gets the address of the next node and sends the message there. The next node does the same, and so on until some node decrypts the real user address.
  - Mix networks and crowds that hide the relationship between senders and receivers by having many intermediate nodes between them.
- Communication protocols that do not use permanent IDs of a personal device or object; instead, IDs are assigned only for the current communication session. Communication protocols that provide anonymity at the network layer, as stated in the PRIME deliverable,[7] are not suitable for large-scale applications: there is no evaluation on the desired security level, and performance is a hard problem.

5.1.5 Authentication and access control

Strong access control methods are needed in AmI applications. Physical access control is required in applications such as border control, airport check-ins and office access. Reliable user authentication is required for logging on to computers and personal devices as well as network applications such as mobile commerce, mobile voting and so on. Reliable authentication should have low error rates *and* strong anti-spoofing protection. Work on anti-spoofing protection of iris and fingerprint recognition is going on, but spoofing is still possible.

We suggest that really reliable authentication should be unobtrusive, continuous (i.e., several times during an application-dependent time period) and multimodal. So far, there has been limited research on continuous multimodal access control systems.

Authentication methods include the following:

[7] Camenish, 2005.

5.1.5.1 Biometrics

Some experts don't believe that biometrics should be the focus of the security approach in an AmI world, since the identification and authentication of individuals by biometrics will always be approximate, is like publishing passwords, can be spoofed and cannot be revoked after an incident.[8]

5.1.5.2 Tokens

Tokens are portable physical devices given to users who keep them in their possession.

5.1.5.3 Implants

Implants are small physical devices, embedded into a human body (nowadays they are inserted with a syringe under the skin). Implants are used for identification by unique ID number, and some research aims to add a GPS positioning module in order to detect the user's location at any time.

5.1.5.4 Multimodal fusion

With multimodal fusion, identification or authentication is performed by information from several sources, which usually helps to improve recognition rates and anti-spoofing capabilities. Multimodal identification and/or authentication can also be performed by combining biometric and non-biometric data.

Methods for reliable, unobtrusive authentication (especially for privacy-safe, unobtrusive authentication) should be developed. Unobtrusive authentication should enable greater security because it is more user-friendly. People are not willing to use explicit authentication frequently, which reduces the overall security level, while unobtrusive authentication can be used frequently.

Methods for context-dependent user authentication, which would allow user control over the strength and method of authentication, should be developed, unlike the current annoying situation when users have to go through the same authentication procedure for viewing weather forecasts and for viewing personal calendar data.

[8] See, for example, Engberg, Stephan, "Empowerment and Context Security as the route to Growth and Security", and Pfitzmann, Andreas, "Anonymity, unobservability, pseudonymity and identity management requirements for an AmI world". Both papers were presented at the SWAMI Final Conference, Brussels, 21–22 March 2006.

5.1.5.5 User-configured applications settings

Recently, the meaning of the term "access control" has broadened to include checking which software is accessing personal data and how the personal data are processed.

Access control to software (data processing methods) is needed for enforcing legal privacy requirements and personal privacy preferences.

User-friendly interfaces are needed for providing awareness and configuring privacy policies. Maintaining privacy is not at the user's focus, so privacy information should not be a burden for a user. However, the user should easily be able to know and configure the following important settings:

- Purpose of the application (e.g., recording a meeting and storing the record for several years)
- How much autonomy the application has
- Information flow *from* the user
- Information flow *to* the user (e.g., when and how the application initiates interactions with the user).

Additionally, user-friendly methods are needed for fast and easy control over the environment, which would allow a person (e.g., a home owner but not a thief) to override previous settings, and especially those settings learned by AmI technologies.

Standard concise methods of initial warnings should be used to indicate whether privacy-violating technologies (such as those that record video and audio data, log personal identity data and physiological and health data) are used by ambient applications.

Licensing languages or ways to express legal requirements and user-defined privacy policies should be attached to personal data for the lifetime of their transmission, storage and processing. These would describe what can be done with the data in different contexts (e.g., in cases involving the merging of databases), and ensure that the data are really treated according to the attached licence. These methods should also facilitate privacy audits (checking that data processing has been carried out correctly and according to prescribed policies), including instances when the data are already deleted. These methods should be tamper-resistant, similar to watermarking.

5.1.6 Generic architecture-related solutions

High-level application design to provide an appropriate level of safeguards for the estimated level of threats can be achieved by data protection methods such as encryption and by avoiding usage of inexpensive RFID tags that do not have access control to their ID and by minimising the need for active data protection on the part of the user.

High-level application design should also consider what level of technology control is acceptable and should provide easy ways to override automatic actions. When communication capabilities move closer to the human body (e.g., embedded in

clothes, jewellery or watches), and battery life is longer, it will be much more difficult to avoid being captured by ubiquitous sensors. It is an open question how society will adapt to such increasing transparency, but it would be beneficial if the individual were able to make a graceful exit from AmI technologies at his or her discretion.

To summarise, the main points to consider in system design are:

- Data filtering on personal devices is preferred to data filtering in an untrustworthy environment. Services (e.g., location-based services) should be designed so that personal devices do not have to send queries; instead, services could simply broadcast all available information to devices within a certain range. Such an implementation can require more bandwidth and computing resources, but is safer because it is unknown how many devices are present in a given location. Thus, it is more difficult for terrorists to plan an attack in a location where people have gathered.
- Authorisation should be required for accessing not only personal data stored in the device, but also for accessing device ID and other characteristics.
- Good design should enable detection of problems with hardware (e.g., checking whether the replacement of certain components was made by an authorised person or not). Currently, mobile devices and smart dust nodes do not check anything if the battery is removed, and do not check whether hardware changes were made by an authorised person, which makes copying data from external memory and replacement of external memory or sensors relatively easy, which is certainly inappropriate in some applications, such as those involved in health monitoring.
- Personal data should be stored not only encrypted, but also split according to application requirements in such a way that different data parts are not accessible at the same time.
- An increase in the capabilities of personal devices is needed to allow some redundancy (consequently, higher reliability) in implementation and to allow powerful multitasking: simultaneous encryption of new data and detection of unusual patterns of device behaviour (e.g., delays due to virus activity). An increase in processing power should also allow more real-time processing of data and reduce the need to store data in raw form.
- Software should be tested by trusted third parties. Currently, there are many kinds of platforms for mobile devices, and business requires rapid software development, which inhibits thorough testing of security and the privacy-protecting capabilities of personal devices. Moreover, privacy protection requires extra resources and costs.
- Good design should provide the user with easy ways to override any automatic action, and to return to a stable initial state. For example, if a personalisation application has learned (by coincidence) that the user buys beer every week, and includes beer on every shopping list, it should be easy to return to a previous state in which system did not know that the user likes beer. Another way to solve this problem might be to wait until the system learns that the user does not like beer. However, this would take longer and be more annoying.

- Good design should avoid implementations with high control levels in applications such as recording audio and images as well as physiological data unless it is strictly necessary for security reasons.
- Means of disconnecting should be provided in such a way that it is not taken as a desire by the user to hide.

5.1.7 Artificial intelligence safeguards

To some extent, all software algorithms are examples of artificial intelligence (AI) methods. Machine-learning and data-mining are traditionally considered to belong to this field. However, safeguarding against Aml threats requires Al methods with very advanced reasoning capabilities. Currently, AI safeguards are not mature, but the results of current research may change that assessment.

Many privacy threats arise because the reasoning capabilities and intelligence of software have not been growing as fast as hardware capabilities (storage and transmission capabilities). Consequently, the development of AI safeguards should be supported as much as possible, especially because they are expected to help protect people from accidental, unintentional privacy violation, such as disturbing a person when he does not want to be, or from recording some private activity. For example, a memory aid application could automatically record some background scene revealing personal secrets or a health monitor could accidentally send data to "data hunters" if there are no advanced reasoning and anti-spyware algorithms running on the user's device. Advanced AI safeguards could also serve as access control and antivirus protection by catching unusual patterns of data copying or delays in program execution.

We recommend that AmI applications, especially if they have a high control level, should be intelligent enough to:

- Detect sensitive data in order to avoid recording or publishing such data
- Adapt to a person's ethics
- Adapt to common sense
- Adapt to different cultures and etiquettes for understanding privacy-protecting requirements
- Summarise records intelligently in real time
- Interpret intelligently user commands with natural interfaces
- Provide language translation tools capable of translating ambiguous expressions
- Detect unusual patterns of copying and processing of personal data
- Provide an automatic privacy audit, checking traces of data processing, data- or code-altering, etc.

These requirements are not easy to fulfil in full scale in the near future; however, we suggest that it is important to fulfil these requirements as far as possible and as soon as possible.

5.1.8 Recovery means

Data losses and identity theft will continue into the future. However, losses of personal data will be more noticeable in the future because of the growing dependence on AmI applications. Thus, methods must be developed to inform all concerned people and organisations about data losses and to advise and/or help them to replace compromised data quickly (e.g., if somebody's fingerprint data are compromised, a switch should be made to another authentication method in all places where the compromised fingerprint was used).

Another problem, which should be solved by technology means, is recovery from loss of or damage to a personal device. If a device is lost, personal data contained in it can be protected from strangers by diverse security measures, such as data encryption and strict access control. However, it is important that the user does not need to spend time customising and training a new device (so that denial of service does not happen). Instead, the new device should itself load user preferences, contacts, favourite music, etc, from some back-up service, like a home server. We suggest that ways be developed to synchronise data in personal devices with a back-up server in a way that is secure and requires minimal effort by the user.

5.1.9 Conclusions and recommendations

We suggest that the most important, but not yet mature technological safeguards are the following:

- Communication protocols that either do not require a unique device identifier at all or that require authorisation for accessing the device identifier
- Network configurations that can hide the links between senders and receivers of data
- Improving access control methods by multimodal fusion, context-aware authentication and unobtrusive biometric modalities (especially behavioural biometrics, because they pose a smaller risk of identity theft) and by aliveness detection in biometric sensors
- Enforcing legal requirements and personal privacy policies by representing them in machine-readable form and attaching these special expressions to personal data, so that they specify how data processing should be performed, allow a privacy audit and prevent any other way of processing
- Developing fast and intuitive means of detecting privacy threats, informing the user and configuring privacy policies
- Increasing hardware and software capabilities for real-time data processing in order to minimise the lifetime and amount of raw data in a system
- Developing user-friendly means to override any automatic settings in a fast and intuitive way

- Providing ways of disconnecting in such a way that nobody can be sure why a user is not connected
- Increasing security by making software updates easier (automatically or semi-automatically, and at a convenient time for the user), detection of unusual patterns, improved encryption
- Increasing software intelligence by developing methods to detect and to hide sensitive data; to understand the ethics and etiquette of different cultures; to speak different languages and to understand and translate human speech in many languages, including a capability to communicate with the blind and deaf
- Developing user-friendly means for recovery when security or privacy has been compromised.

The technological safeguards require actions by industry. We recommend that industry undertake such technological safeguards. Industry may resist doing so because it will increase development costs, but safer, more secure technology should be seen as a good investment in future market growth and protection against possible liabilities. It is obvious that consumers will be more inclined to use technology if they believe it is secure and will shield, not erode their privacy.

We recommend that industry undertake such safeguards voluntarily. It is better to do so than to be forced by bad publicity that might arise in the media or from action by policy-makers and regulators.

Security guru Bruce Schneier got it right when he said that "The problem is … bad design, poorly implemented features, inadequate testing and security vulnerabilities from software bugs. … The only way to fix this problem is for vendors to fix their software, and they won't do it until it's in their financial best interests to do so. … Liability law is a way to make it in those organizations' best interests."[9] If development costs go up, industry will, of course, pass on those costs to consumers, but since consumers already pay, in one way or another, the only difference is who they pay.

Admittedly, this is not a simple problem because hardware manufacturers, software vendors and network operators all face competition and raising the cost of development and lengthening the duration of the design phase could have competitive implications, but if all industry players face the same exacting liability standards, then the competitive implications may not be so severe as some might fear.

5.2 Socio-economic safeguards

Co-operation between producers and users of AmI technology in all phases from R&D to deployment is essential to address some of the threats and vulnerabilities posed by AmI. The integration of or at least striking a fair balance between the

[9] Schneier, Bruce, "Information security: How liable should vendors be?", *Computerworld*, 28 October 2004. http://www.schneier.com/essay-073.html

interests of the public and private sectors will ensure more equity, interoperability and efficiency. Governments, industry associations, civil rights groups and other civil society organisations can play an important role in balancing these interests for the benefit of all affected groups.

5.2.1 Standards

Standards form an important safeguard in many domains, not least of which are those relating to privacy and information security. Organisations should be expected to comply with standards, and standards-setting initiatives are generally worthy of support.

While there have been many definitions and analyses of the dimensions of privacy, few of them have become officially accepted at the international level, especially by the International Organization for Standardization. The ISO has at least achieved consensus on four components of privacy, i.e., anonymity, pseudonymity, unlinkability and unobservability.[10] (See section 5.1, p. 179, above for the definitions.)

Among the ISO standards relevant to privacy and, in particular, information security are ISO/IEC 15408 on evaluation criteria for IT security and ISO 17799, the Code of practice for information security management.

The ISO has also established a Privacy Technology Study Group (PTSG) under Joint Technical Committee 1 (JTC1) to examine the need for developing a privacy technology standard. This is an important initiative and merits support. Its work and progress should be tracked closely by the EC, Member States, industry and so on.

The ISO published its standard ISO 17799 in 2000, which was updated in July 2005. Since then, an increasing number of organisations worldwide formulate their security management systems according to this standard. It provides a set of recommendations for information security management, focusing on the protection of information as an asset. It adopts a broad perspective that covers most aspects of information systems security.[11]

Among its recommendations for organisational security, ISO 17999 states that "the use of personal or privately owned information processing facilities … for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented."[12] By implementing such controls,

[10] ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999. The standard is also known as the Common Criteria.

[11] Similar standards and guidelines have also been published by other EU Member States: The British standard BS7799 was the basis for the ISO standard. Another prominent example is the German IT Security Handbook (BSI, 1992).

[12] ISO/IEC 17799:2005(E), *Information Technology – Security techniques – Code of Practice for Information Security Management*, International Organization for Standardization, Geneva, 2005, p. 11.

organisations can, at the same time, achieve a measure of both organisational security and personal data protection.

ISO 17799 acknowledges the importance of legislative requirements, such as legislation on data protection and privacy of personal information and on intellectual property rights, for providing a "good starting point for implementing information security".[13]

ISO 17799 is an important standard, but it could be described more as a framework than a standard addressing specificities of appropriate technologies or how those technologies should function or be used. Also, ISO 17799 was constructed against the backdrop of today's technologies, rather than with AmI in mind. Hence, the adequacy of this standard in an AmI world needs to be considered. Nevertheless, organisations should state to what extent they are compliant with ISO 17799 and/or how they have implemented the standard.

5.2.2 Audits

Audit logs may not protect privacy since they are aimed at determining whether a security breach has occurred and, if so, who might have been responsible or, at least, what went wrong. Audit logs could have a deterrent value in protecting privacy and certainly they could be useful in prosecuting those who break into systems without authorisation.

In the highly networked environment of our AmI future, maintaining audit logs will be a much bigger task than now where discrete systems can be audited. Nevertheless, those designing AmI networks should ensure that the networks have features that enable effective audits.

5.2.3 Open standards

Apart from the positive effects of open innovations as such, we would support the development of protection software (against viruses, spam, spyware, etc.) under the open source development model. Though open source is no panacea for security problems, there is evidence that open source software can lead to robust and reliable products.

Promoting open systems and open standards at a European level could help to build a more trustworthy system, to mediate between public and private control over networked systems and, therefore, to contribute to security and privacy in AmI.[14]

---

[13] ISO/IEC 17799:2005, p. ix.

[14] Kravitz, D.W., K.-E. Yeoh and N. So, "Secure Open Systems for Protecting Privacy and Digital Services", in T. Sander (ed.), *Security and Privacy in Digital Rights Management*, ACM CCS-8 Workshop DRM 2001, Philadelphia, 5 November 2001, Revised Papers, Springer, Berlin, 2002, pp. 106–25; Gehring, R. A., "Software Development, Intellectual Property, and IT Security", *The Journal of Information, Law and Technology*, 1/2003. http://elj.warwick.ac.uk/jilt/03-1/gehring.html

5.2.4 Codes of practice

The OECD has been working on privacy and security issues for many years. It produced its first guidelines more than 25 years ago. Its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[15] were (are) intended to harmonise national privacy legislation. The guidelines were produced in the form of a Recommendation by the Council of the OECD and became applicable in September 1980. The guidelines are still relevant today and may be relevant in an AmI world too, although it has been argued that they may no longer be feasible in an AmI world.[16]

The OECD's more recent Guidelines for the Security of Information Systems and Networks are also an important reference in the context of developing privacy and security safeguards. These guidelines were adopted as a Recommendation of the OECD Council (in July 2002). In December 2005, the OECD published a report on "The Promotion of a Culture of Security for Information Systems and Networks", which it describes as a major information resource on governments' effective efforts to date to foster a shift in culture as called for in the aforementioned Guidelines for the Security of Information Systems and Networks.

In November 2003, the OECD published a 392-page volume entitled *Privacy Online: OECD Guidance on Policy and Practice*, which contains specific policy and practical guidance to assist governments, businesses and individuals in promoting privacy protection online at national and international levels.

In addition to these, the OECD has produced reports on other privacy-related issues including RFIDs, biometrics, spam and authentication.[17]

Sensible advice can also be found in a report published by the US National Academies Press in 2003, which said that to best protect privacy, identifiable information should be collected only when critical to the relationship or transaction that is being authenticated. The individual should consent to the collection, and the minimum amount of identifiable information should be collected and retained. The relevance, accuracy and timeliness of the identifier should be maintained and, when necessary, updated. Restrictions on secondary uses of the identifier are important in order to safeguard the privacy of the individual and to preserve the security of the authentication system. The individual should have clear rights to access information about how data are protected and used by the authentication system and the individual should have the right to challenge, correct and amend any information related to the identifier or its uses.[18]

---

[15] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[16] See Čas, Johann, "Privacy in Pervasive Computing Environments – A Contradiction in Terms?", *Technology and Society Magazine*, IEEE, Vol. 24, No. 1, Spring 2005, pp. 24–33.

[17] http://www.oecd.org/department/0,2688,en_2649_34255_1_1_1_1_1,00.html

[18] Kent, Stephen T., and Lynette I. Millett (eds.), *Who Goes There?*, Chapter 3.

Among privacy projects, PRIME has identified a set of privacy principles in the design of identity management architecture:

Principle 1: Design must start from maximum privacy.
Principle 2: Explicit privacy rules govern system usage.
Principle 3: Privacy rules must be enforced, not just stated.
Principle 4: Privacy enforcement must be trustworthy.
Principle 5: Users need easy and intuitive abstractions of privacy.
Principle 6: Privacy needs an integrated approach.
Principle 7: Privacy must be integrated with applications.[19]

5.2.5 Trust marks and trust seals

Trust marks and trust seals can also be useful safeguards because the creation of public credibility is a good way for organisations to alert consumers and other individuals to an organisation's practices and procedures through participation in a programme that has an easy-to-recognise symbol or seal.

Trust marks and seals are a form of guarantee provided by an independent organisation that maintains a list of trustworthy companies that have been audited and certified for compliance with some industry-wide accepted or standardised best practice in collecting personal or sensitive data. Once these conditions are met, they are allowed to display a trust seal logo or label that customers can easily recognise.[20]

A trust mark must be supported by mechanisms necessary to maintain objectivity and build legitimacy with consumers. Trust seals and trust marks are, however, voluntary efforts that are not legally binding and an effective enforcement needs carefully designed procedures and the backing of an independent and powerful organisation that has the confidence of all affected parties.

Trust seals and trust marks are often promoted by industry, as opposed to consumer-interest groups. As a result, concerns exist that consumers' desires for stringent privacy protections may be compromised in the interest of industry's desire for the new currency of information. Moreover, empirical evidence indicates that even some eight years after the introduction of the first trust marks and trust seals in Internet commerce, citizens know little about them and none of the existing seals has reached a high degree of familiarity among customers.[21] Though

[19] For more details about each principle, see Sommer, Dieter, Architecture Version 0, PRIME Deliverable D14.2.a, 13 October 2004, pp. 35–36 and pp. 57–58. www.prime-project.eu.org

[20] Pennington, R., H.D. Wilcox and V. Grover, "The Role of System Trust in Business-to-Consumer Transactions", *Journal of Management Information System*, Vol. 20, No. 3, 2004, pp. 197–226; Subirana, B., and M. Bain, *Legal Programming: Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond*, Springer, New York, 2005.

[21] Moores, T., "Do Consumers Understand the Role of Privacy Seals in E-Commerce?" *Communications of the ACM*, Vol. 48, No. 3, 2005, pp. 86–91.

this does not necessarily mean that trust marks are not an adequate safeguard for improving security and privacy in the ambient intelligence world, it suggests that voluntary activities like self-regulation have – apart from being well designed – to be complemented by other legally enforceable measures.[22]

5.2.6 Reputation systems and trust-enhancing mechanisms

In addition to the general influence of cultural factors and socialisation, trust results from context-specific interaction experiences. As is well documented, computer-mediated interactions are different from conventional face-to-face exchanges due to anonymity, lack of social and cultural clues, "thin" information, and the uncertainty about the credibility and reliability of the provided information that commonly characterise mediated relationships.[23]

In an attempt to reduce some of the uncertainties associated with online commerce, many websites acting as intermediaries between transaction partners are operating so-called reputation systems. These institutionalised feedback mechanisms are usually based on the disclosure of past transactions rated by the respective partners involved.[24] Giving participants the opportunity to rank their counterparts creates an incentive for rule-abiding behaviour. Thus, reputation systems seek to imitate some of the real-life trust-building and social constraint mechanisms in the context of mediated interactions.

So far, reputation systems have not been developed for AmI services. And it seems clear that institutionalised feedback mechanisms will only be applicable to a subset of future AmI services and systems. Implementing reputation systems only makes sense in those cases in which users have real choices between different suppliers (for instance, with regard to AmI-assisted commercial transactions or information brokers). AmI infrastructures that normally cannot be avoided if one wants to take advantage of a service need to be safeguarded by other means, such as trust seals, ISO guidelines and regulatory action.

Despite quite encouraging experiences in numerous online arenas, reputation systems are far from perfect. Many reputation systems tend to shift the burden of quality control and assessment from professionals to the – not necessarily entirely

---

[22] Prins, J.E.J., and M.H.M. Schellekens, "Fighting Untrustworthy Internet Content: In Search of Regulatory Scenarios", *Information Polity*, Vol. 10, 2005, pp. 129–139.

[23] For an overview of the vast literature on the topic, see Burnett, R., and P.D. Marshall, *Web Theory: An Introduction*, Routledge, London 2002, pp. 45–80.

[24] Resnick, P., and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System", in Michael R. Baye (ed.), *The Economics of the Internet and E-Commerce*, Vol. 11 of Advances in Applied Microeconomics, JAI Press, Amsterdam, 2002, pp. 127–157; Vishwanath, A., "Manifestations of Interpersonal Trust in Online Interaction", *New Media and Society*, Vol. 6, No. 2, 2004, pp. 224 et seq.

informed – individual user. In consequence, particularly sensitive services should not exclusively be controlled by voluntary and market-style feedbacks from customers. Furthermore, reputation systems are vulnerable to manipulation. Pseudonyms can be changed, effectively erasing previous feedback. And the feedback itself need not necessarily be sincere, either due to co-ordinated accumulation of positive feedback, due to negotiations between parties prior to the actual feedback process, because of blackmailing or the fear of retaliation.[25] Last but not least, reputation systems can become the target of malicious attacks, just like any net-based system.

An alternative to peer-rating systems are credibility-rating systems based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains. Ratings would be based on systematic assessments along clearly defined quality standards. In effect, these variants of reputation- and credibility-enhancing systems are quite similar to trust marks and trust seals. The main difference is that professional rating systems enjoy a greater degree of independence from vested interests. And, other than in the case of peer-rating systems which operate literally for free, the independent professional organisations need to be equipped with adequate resources.

On balance, reputation systems can contribute to trust-building between strangers in mediated short-term relations or between users and suppliers, but they should not be viewed as a universal remedy for the ubiquitous problem of uncertainty and the lack of trust.

5.2.7 Service contracts

A possible safeguard is a contract between the service provider and the user that has provisions about privacy rights and the protection of personal data and notification of the user of any processing or transfer of such data to third parties. While this is a possible safeguard, there must be some serious doubt about the negotiating position of the user. It's quite possible the service provider would simply say here are the terms under which I'm willing to provide the service, take it or leave it. Also, from the service provider's point of view, it is unlikely that he would want to conclude separate contracts with every single user.

In a world of ambient intelligence, such a prospect becomes even more unlikely in view of the fact that the "user", the consumer-citizen will be moving through

[25] Resnick, P., R. Zeckhauser, E. Friedman and K. Kuwabara, "Reputation Systems: Facilitating Trust in Internet Interactions", *Communications of the ACM*, 43 (12), 2000, pp. 45–48. http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf.

different spaces where there is likely to be a multiplicity of different service providers. It may be that the consumer-citizen would have a digital assistant that would inform him of the terms, including the privacy implications, of using a particular service in a particular environment. If the consumer-citizen did not like the terms, he would not have to use the service.

Consumer associations and other civil society organisations (CSOs) could, however, play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. Consumer organisations could leverage their negotiating position through the use of the media or other means of communication with their members. CSOs could position themselves closer to the industry vanguard represented in platforms such as ARTEMIS by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop "best practices" in terms of provision of services to consumers.

5.2.8 Guidelines for ICT research

Government support for new technologies should be linked more closely to an assessment of technological consequences. On the basis of the far-reaching social effects that ambient intelligence is supposed to have and the high dynamics of the development, there is a clear deficit in this area.[26] Research and development (at least publicly supported R&D) must highlight future opportunities and possible risks to society and introduce them into public discourse. Every research project should commit itself to explore possible risks in terms of privacy, security and trust, develop a strategy to cover problematic issues and involve users in this process as early as possible.

A template for "design guidelines" that are specifically addressing issues of privacy has been developed by the "Ambient Agora" project[27] which has taken into account the fundamental rules by the OECD, notably its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23

[26] Langheinrich, M., "The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects", Paper presented at the Designing for Privacy Workshop, DC Tales Conference, Santorini, Greece, 2003.

[27] Lahlou, S., and F. Jegou, "European Disappearing Computer Privacy Design Guidelines V1", Ambient Agora Deliverable D15.4, Electricité de France, Clamart, 2003. http://www.ambient-agoras.org/downloads/D15[1].4_-_Privacy_Design_Guidelines.pdf. The guidelines were subsequently and slightly modified and can be found at http://www.rufae.org/privacy. See also Langheinrich, M., "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in G.D. Abowd, B. Brumitt and S.A. Shafer (eds.), *Proceedings of the Third International Conference on Ubiquitous Computing* (Ubicomp 2001), Springer-Verlag, Berlin, 2001, pp. 273–291.

September 1980, and the more recent *Guidelines for the Security of Information Systems and Networks*.[28]

5.2.9 Public procurement

If the state acts as a buyer of strategically important innovative products and services, it contributes to the creation of the critical demand that enables suppliers to reduce their business risk and realise spillover effects. Thus, public procurement programmes can be used to support the demand for and use of improved products and services in terms of security and privacy or identity protection.

In the procurement of ICT products, emphasis should therefore be given to critical issues such as security and trustworthiness. As in other advanced fields, it will be a major challenge to develop a sustainable procurement policy that can cope with ever-decreasing innovation cycles. The focus should not be on the characteristics of an individual product or component, but on the systems into which components are integrated.

Moreover, it is important to pay attention to the secondary and tertiary impacts resulting from deployment of large technical systems such as ambient intelligence. An evaluation of the indirect impacts is especially recommended for larger (infrastructure) investments and public services.

While public procurement of products and services that are compliant with the EU legal framework and other important guidelines for security, privacy and identity protection is no safeguard on its own, it can be an effective means for the establishment and deployment of standards and improved technological solutions.[29]

5.2.10 Accessibility and social inclusion

Accessibility is a key concept in helping to promote the social inclusion of all citizens in the information society embedded with AmI technologies. Accessibility is needed to ensure user control, acceptance, enforceability of policy in a user-friendly manner and the provision of citizens with equal rights and opportunities in a world of ambient intelligence.

---

[28] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development, Paris, 2001; *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Organisation for Economic Co-operation and Development, Paris, 2002.

[29] See for instance Edler, J. (ed.), "Politikbenchmarking Nachfrageorientierte Innovationspolitik", Progress report No. 99, Office for Technology Assessment at the German Parliament, Berlin, 2006; Molas-Gallart, J., "Government Policies and Complex Product Systems: The Case of Defence Standards and Procurement", *International Journal of Aerospace Management*, Vol. 1, No. 3, 2001, pp. 268–280.

Accessibility depends on four safeguards (or principles) relating to:

- Equal rights and opportunities
- Usability (vs complexity)
- Training
- Dependability.

5.2.10.1 Equal rights and opportunities

All citizens should have equal rights to benefit from the new opportunities that AmI technologies will offer. This principle promotes the removal of direct and indirect discrimination, fosters access to services and encourages targeted actions in favour of under-represented groups.

5.2.10.2 Usability (vs complexity of use)

This principle promotes system design according to a user-centric approach (i.e., the concept of "design for all"). The design-for-all concept enables all to use applications (speech technology for the blind, pictures for the deaf). It means designing in a way to make sure applications are user-friendly and can be used intuitively. In short, industry has to make an effort to simplify the usage of ICTs, rather than forcing prospective users to learn how to use otherwise complex ICTs.

Better usability will then support easy learning (i.e., learning by observation), user control and efficiency, thus increasing satisfaction and, consequently, user acceptance.

This principle aims to overcome user dependency and more particularly user isolation and stress due to the complexity of new technology, which leads to loss of control.

5.2.10.3 Training

Education programmes on how to use new technologies will increase user awareness about the different possibilities and choices offered by AmI technologies and devices. Training and education help to overcome user dependency and social disruptions. User awareness is important to reduce the voluntary exclusion caused by a misunderstanding on how the technology works.

5.2.10.4 Dependability

This safeguard is essential in order to prevent almost all facets of dependency, system dependency as well as user dependency.

5.2.11 Raising public awareness

Consumers need to be educated about the privacy ramifications arising from virtually any transaction in which they are engaged. An education campaign should be targeted at different segments of the population. School-age children should be included in any such campaign.

Any networked device, particularly those used by consumer-citizens, should come with a privacy warning much like the warnings on tobacco products.

When the UK Department of Trade and Industry (DTI) released its 2004 information security review, the UK e-commerce minister emphasised that everyone has a role to play in protecting information: "Risks are not well managed. We need to dispel the illusion the information security issues are somebody else's problem. It's time to roll up our sleeves."[30]

The OECD shares this point of view. It has said that "all participants in the new information society … need … a greater awareness and understanding of security issues and the need to develop a 'culture of security'."[31] The OECD uses the word "participants", which equates to "stakeholders", and virtually everyone is a participant or stakeholder – governments, businesses, other organisations and individual users. OECD guidelines are aimed at promoting a culture of security, raising awareness and fostering greater confidence (i.e., trust) among all participants.

There are various ways of raising awareness, and one of those ways would be to have some contest or competition for the best security or privacy-enhancing product or service of the year. The US government's Department of Homeland Security is sponsoring such competitions,[32] and Europe could usefully draw on their experience to hold similar competitions in Europe.

5.2.12 Education

In the same way as the principle that "not everything that you read in the newspapers is true" has long been part of general education, in the ICT age, awareness should generally be raised by organisations that are trustworthy and as close to the citizen as possible (i.e., on the local or regional level. Questions of privacy, identity

[30] Leyden, John, "Hackers cost UK.biz billions", *The Register*, 28 April 2004. http://www.theregister.co.uk/2004/04/28/dti_security_survey/

[31] *OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security*, OECD, Paris, 2002, p. 7.

[32] Lemos, Robert, "Cybersecurity contests go national", *The Register*, 5 June 2006. http://www.theregister.co.uk/2006/06/05/security_contests/. This article originally appeared at *Security Focus*. http://www.securityfocus.com/news/11394

and security are, or should be, an integral part of the professional education of computer scientists.

We agree with and support the Commission's "invitation" to Member States to "stimulate the development of network and information security programmes as part of higher education curricula".[33]

5.2.13 Media attention, bad publicity and public opinion

Perhaps one of the best safeguards is public opinion, stoked by stories in the press and the consequent bad publicity given to perceived invasions of privacy by industry and government.

New technologies often raise policy issues, and this is certainly true of ambient intelligence. AmI offers great benefits, but the risk of not adequately addressing public concerns could mean delays in implementing the technologies, a lack of public support for taxpayer-funded research and vociferous protests by privacy protection advocates.

5.2.14 Cultural safeguards

Cultural artefacts, such as films and novels, may serve as safeguards against the threats and vulnerabilities posed by advanced technologies, including ambient intelligence. Science fiction in particular often presents a dystopian view of the future where technology is used to manipulate or control people, thus, in so doing, such artefacts raise our awareness and serve as warnings against the abuse of technology. A *New York Times* film critic put it this way: "It has long been axiomatic that speculative science-fiction visions of the future must reflect the anxieties of the present: fears of technology gone awry, of repressive political authority and of the erosion of individuality and human freedom."[34]

An example of a cultural artefact is Steven Spielberg's 2002 film, *Minority Report*, which depicts a future embedded with ambient intelligence, which serves

[33] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Brussels, COM(2006) 251, Brussels, 31 May 2006, p. 9 (section 3.3.1). http://ec.europa.eu/information_society/doc/com2006251.pdf

[34] Scott, A.O., "A Future More Nasty, Because It's So Near", Film review of "Code 46", *The New York Times*, 6 August 2004.

to convey messages or warnings from the director to his audience.[35] *Minority Report* is by no means unique as a cultural artefact warning about how future technologies are like a double-edged knife that cuts both ways.

5.2.15 Conclusion and recommendation

To implement socio-economic safeguards will require action by many different players. Unfortunately, the very pervasiveness of AmI means that no single action by itself will be sufficient as a safeguard. A wide variety of socio-economic safeguards, probably even wider than those we have highlighted in the preceding sections, will be necessary.

As implementation of AmI has already begun (with RFIDs, surveillance systems, biometrics, etc.), it is clearly not too soon to begin implementation of safeguards. We recommend, therefore, that all stakeholders, including the public, contribute to this effort.

5.3 Legal and regulatory safeguards

5.3.1 Introduction

The fast emergence of information and communication technologies and the growth of online communication, e-commerce and electronic services that go beyond the territorial borders of the Member States have led the European Union to adopt numerous legal instruments such as directives, regulations and conventions on e-commerce, consumer protection, electronic signature, cyber crime, liability, data protection, privacy and electronic communication … and many others. Even the European Charter of Fundamental Rights will play an important role in relation to the networked information society.

Our analysis of the dark scenarios shows that we may encounter serious legal problems when applying the existing legal framework to address the intricacies of an AmI environment.

Our proposed legal safeguards should be considered as general policy options, aimed at stimulating discussion between stakeholders and, especially, policy-makers.

---

[35] Wright, David, "Alternative futures: Aml scenarios and *Minority Report*", *Futures*, Vol. 40:5, June 2008.

5.3.2 General recommendations

5.3.2.1 Law and architecture go together (Recommendation 1)

Law is only one of the available sets of tools for regulating behaviour, next to social norms, market rules, "code"[36] – the architecture of the technology (e.g., of cyberspace, wireless and wired networks, security design, encryption levels, rights management systems, mobile telephony systems, user interfaces, biometric features, handheld devices and accessibility criteria) and many other tools.

The regulator of ambient intelligence can, for instance, achieve certain aims directly by imposing laws, but also indirectly by, for example, influencing the rules of the market. Regulatory effect can also be achieved by influencing the architecture of a certain environment. The architecture of AmI might well make certain legal rules difficult to enforce (for example, the enforcement of data protection obligations on the Internet or the enforcement of copyright in peer-to-peer networks), and might cause new problems, particularly related to the new environment (spam, dataveillance[37]). On the other hand, the "code" has the potential to regulate by enabling or disabling certain behaviour, while law regulates via the threat of sanction. In other words, software and hardware constituting the "code", and architecture of the digital world, causing particular problems, can be at the same time the instrument to solve them. Regulating through code may have some specific advantages: Law traditionally regulates ex post, by imposing a sanction on those who did not comply with its rules (e.g., in the form of civil damages or criminal prosecution). Architecture regulates by putting conditions on one's behaviour, allowing or disallowing something, not allowing the possibility to disobey. It regulates ex ante.

Ambient intelligence is particularly built on software code. This code influences how ambient intelligence works, e.g., how the data are processed, but this code itself can be influenced and accompanied by regulation.[38] Thus, the architecture can be a tool of law. This finding is more than elementary. It shows that there is a choice: should the law change because of the "code"? Or should the law change "code" and thus ensure that certain values are protected?

---

[36] Lessig, Lawrence, "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, Vol. 113, 1999, pp. 501–546. See also Brownsword, Roger, "Code, control, and choice. Why East is East and West is West", *Legal Studies*, Vol. 25, No. 1, March 2005, pp. 1–21.

[37] "Dataveillance means the systematic monitoring of people's actions or communications through the application of information technology." See M. Hansen and H. Krasemann (eds.), *Privacy and Identity Management for Europe – PRIME White Paper – Deliverable 15.1.d.*, 18 July 2005, p. 11 (35 p.), with a reference to Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, 31(5), May 1988, pp. 498–512, and re-published in C. Dunlop and R. Kling (eds.), *Controversies in Computing*, Academic Press, 1991, available at http://www.anu.edu/people/Roger.Clarke/DV/CACM88.html

[38] Contrary to the long-lasting paradigm, as Lessig writes. See Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, and "The Law of the Horse: What Cyberlaw Might Teach", pp. 501–546.

The development of technology represents an enormous challenge for privacy, enabling increasing surveillance and invisible collection of data. A technology that threatens privacy may be balanced by the use of a privacy-enhancing technology: the "code", as Lessig claims,[39] can be the privacy saviour. Other technologies aim to limit the amount of data actually collected to the necessary minimum. However, most of the current technologies simply ignore the privacy implications and collect personal data when there is no such need. A shift of the paradigm to privacy-by-design is necessary to effectively protect privacy. Indeed, technology can facilitate privacy-friendly verification of individuals via, for example, anonymous and pseudonymous credentials. Leenes and Koops recognise the potential of these privacy-enhancing technologies (PETs) to enforce data protection law and privacy rules.[40] But they also point at problems regarding the use of such technologies, which are often troublesome in installation and use for most consumers. Moreover, industry is not really interested in implementing privacy-enhancing technology. They see no (economic) reason to do it.

The analysis of Leenes and Koops shows that neither useful technology, nor law is sufficient in itself. Equally important is raising stakeholder awareness, social norms and market rules. All regulatory means should be used and have to be used to respond to problems of the new environment to tackle it effectively. *For the full effectiveness of any regulation, one should always look for the optimal mixture of all accessible means*.[41]

5.3.2.2 Precaution or caution through opacity? (Recommendation 2)

As the impact and effects of the large-scale introduction of AmI in societies spawn a lot of uncertainties, the careful demarche implied by the precautionary principle, with its information, consultation and participation constraints, might be appropriate. The application of this principle might inspire us in devising legal policy options when, as regards AmI, fundamental choices between opacity tools and transparency tools must be made.[42] **Opacity tools** proscribe the interference by powerful actors into the individual's autonomy, while **transparency tools** accept such interfering practices, though under certain conditions which guarantee the control, transparency and accountability of the interfering activity and actors.

---

[39] Lessig, L., *Code and Other Laws of Cyberspace*, op. cit.

[40] Leenes, R., and B.J. Koops, " 'Code': Privacy's Death or Saviour?", *International Review of Law, Computers & Technology*, Vol. 19, No. 3, 2005.

[41] Lessig, L., "The Law of the Horse: What Cyberlaw Might Teach", op. cit., pp. 501–546.

[42] De Hert, Paul, and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Erik Claes, Anthony Duff and Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp/Oxford, Intersentia, 2006, pp. 61–104.

In our opinion, most of the challenges arising in the new AmI environment should be addressed by transparency tools (such as data protection and security measures). Transparency should be the default position, although some prohibitions referring to political balances, ethical reasons or core legal concepts should be considered too.

Legal scholars do not discuss law in general terms. Their way of thinking always involves an application of the law in concrete or exemplified situations. The legislator will compare concrete examples and situations with the law and will not try to formulate general positions or policies. Thus, the proposed legal framework will not deal with the AmI problems in a general way, but focus on concrete issues, and apply opacity and transparency solutions accordingly.

5.3.2.3 Central lawmaking for AmI is not recommended (Recommendation 3)

Another particularity of legal regulation in cyberspace is the absence of a central legislator. Though our legal analysis is based mostly on European law, we emphasise that not everything is regulated at a European level. Regulation of (electronic) identity cards, for instance, concerns a crucial element in the construction of an AmI environment, but is within the powers of the individual Member States.

Both at European and national level, some decision-making competences have been delegated to independent advisory organs (children's rights commissioners, data protection authorities). Hence, there exist many, what we can call, "little legislators" that adjust in some way the often executive power origin of legislation: The Article 29 Data Protection Working Party, national children's rights commissioners and international standardisation bodies can and do, for example, draft codes of conduct that constitute often (but not always) the basis for new legislation.

We do not suggest the centralisation of the law-making process. On the contrary, we recommend respect for the diversity and plurality of lawmakers. The solutions produced by the different actors should be taken into consideration and be actively involved in policy discussions. Development of case law should also be closely observed. Consulting concerned citizens and those who represent citizens (including legislators) at the stage of development would increase the legitimacy of new technologies.

5.3.3 Preserving the core of privacy and other human rights

5.3.3.1 Recommendations regarding privacy

Privacy aims to ensure no interference in private and individual matters. It offers an instrument to safeguard the opacity of the individual and puts limits

to the interference by powerful actors into the individual's autonomy. Normative in nature, regulatory opacity tools should be distinct from regulatory transparency tools, of which the goal is to control the exercise of power rather than to restrict power.[43]

We observe today that the reasonable expectation of privacy is eroding due to emerging new technologies and possibilities for surveillance: it develops into an expectation of being monitored. Should this, however, lead to diminishing the right to privacy? Ambient intelligence may seriously threaten this value, but the need for privacy (e.g., the right to be let alone) will probably remain, be it in another form adapted to new infrastructures (e.g., the right to be left offline).

The right to privacy in a networked environment could be enforced by any means of protecting the individual against any form of dataveillance. Such means are in line with the data minimisation principle of data protection law, which is a complementary tool to privacy. However, in ambient intelligence where collecting and processing personal data is almost a prerequisite, new tools of opacity such as the right to be left offline (in time, e.g., during certain minutes at work, or in space, e.g., in public bathrooms) could be recognised.

Several instruments of opacity can be identified. We list several examples, and there may be others. Additional opacity recommendations are made in subsequent sections, for example, with regard to biometrics. We observe that there is not necessarily an internal coherence between the examples listed below. The list should be understood as a wish list or a list with suggestions to be consulted freely.

[43] Opacity designates a zone of non-interference which should not be confused with a zone of invisibility: privacy, for instance, does not imply secrecy; it implies the possibility of being oneself openly without interference. Another word might have been "impermeability" which is too strong and does not contrast so nicely with "transparency" as "opacity" does. See Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS (Future of Identity in the Information Society), Deliverable D7.4, September 2005. http://www.fidis.net. See also De Hert, P., and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerp/Oxford, Intersentia, 2005, pp. 61–104; De Hert, P. and S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence" in *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies – Joint Research Centre, Seville, July 2003, pp. 111–162 (ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf); and Gutwirth, S., "De polyfonie van de democratische rechtsstaat" [The polyphony of the democratic constitutional state] in M. Elchardus (ed.), *Wantrouwen en onbehagen* [Distrust and uneasiness], Balans 14, VUB Press, Brussels, 1998, pp. 137–193.

5.3.3.2 Recommendation regarding digital territories

The concept of a digital territory represents a vision that introduces the notions of space and borders in future digitised everyday life. It could be visualised as a bubble, the boundaries and transparency of which depend on the will of its owner. The notion of a digital territory aims for a "better clarification of all kinds of interactions in the future information society. Without digital boundaries, the fundamental notion of privacy or the feeling of *being at home* will not take place in the future information society."[44] The concept of digital territories encompasses the notion of a virtual residence, which can be seen as a virtual representation of the smart home.

The concept of digital territories could provide the individual with a possibility to access – and stay in – a private digital territory of his own at (any) chosen time and place. This private, digital space could be considered as an extension of the private home. Today, already, people store their personal pictures on distant servers, read their private correspondences online, provide content providers with their viewing and consuming behaviour for the purpose of digital rights management, communicate with friends and relatives through instant messengers and Internet telephony services. The "prognosis is that the physical home will evolve to 'node' in the network society, implying that it will become intimately interconnected to the virtual world."[45]

The law guarantees neither the establishment nor the protection of an online private space in the same way as the private space in the physical world is protected. Currently, adequate protection is lacking.[46] For example, the new data retention law requires that telecommunication service providers keep communication data at the disposal of law enforcement agencies. The retention of communication data relates to mobile and fixed phone data, Internet access, e-mail and e-telephony. Data to be retained includes the place, time, duration and destination of communications. What are the conditions for accessing such data? Is the individual informed when such data are accessed? Does he have the right to be present when such data are examined? Does the inviolability of the home extend to the data that are stored on a distant server? Another example of inadequate protection concerns the increasing access to home activities from a distance, for example, as a result of the communication data generated by domestic

---

[44] Beslay, L., and H. Hakala, "Digital Territory: Bubbles", in P. T. Kidd (ed.), *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society*, Cheshire Henbury, Macclesfield, UK, 2007, p. 1.
http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf

[45] De Hert, P., and S. Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence", p. 159.

[46] Idem. See also Beslay, L., and Y. Punie, "The Virtual Residence: Identity, Privacy and Security", *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a Prospective Overview*, p. 67.

applications that are connected to the Internet. In both examples, there is no physical entrance in the private place.[47]

To ensure that these virtual private territories become a private domain for the individual, a regulatory framework could be established to prevent unwanted and unnoticed interventions similar to that which currently applies to the inviolability of the home.

A set of rules needs to be envisaged to guarantee such protection, amongst them, the procedural safeguards similar to those currently applicable to the protection of our homes against state intervention (e.g., requiring a search warrant). Technical solutions aimed at defending private digital territories against intrusion should be encouraged and, if possible, legally enforced.[48] *The individual should be empowered with the means to freely decide what kinds of information he or she is willing to disclose, and that aspect should be included in the digital territory concept. Similarly, vulnerable home networks should be granted privacy protection. Such protection could be extended to the digital movement of the person, that is, just as the privacy protection afforded the home has been or can be extended to the individual's car, so the protection could be extended to home networks, which might contact external networks.*[49]

5.3.3.3 Recommendation regarding spy-free territories for workers and children

Privacy at the workplace has already been extensively discussed.[50] Most of the legal challenges, we believe, that may arise can be answered with legal transparency rules. More drastic, prohibitive measures may be necessary in certain situations involving too far-reaching or unnecessary surveillance, which a society considers as infringing upon the dignity of the employee. *One of the ways to grant the individual a possibility to escape such disproportional surveillance at the workplace is obliging organisations to create physical spaces at work without surveillance technology, e.g., in social areas where the individual can take a short break and in bathrooms. The idea of cyber territories, accessible to the individual when he is in*

[47] See Koops, B.J., and M.M. Prinsen, "Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit" ["Glass house, transparent body. A future view on home law and body integrity"], *Nederland Juristenblad*, 12 March 2005, pp. 624–630.

[48] De Hert, P., and S. Gutwirth, "Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence", p. 159.

[49] Beslay, L., and Y. Punie, "The Virtual Residence: Identity, Privacy and Security", p. 67.

[50] See Chapter 3, section 3.2.8.1. See also Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (5401/01/EN/Final – WP 55), adopted on 29 May 2002. http://ec.europa.eu/justice_home/fsj/privacy/

the workplace, would grant him the possibility of being alone in his private digital or cyber activities.[51]

In addition, transparency rules are needed to regulate other, less intrusive problems. We recall here the specific role of law-making institutions in the area of labour law. Companies must discuss their surveillance system and its usage in collective negotiations with labour organisations and organisations representing employees before its implementation in a company or a sector, taking into account the specific needs and risks involved (e.g., workers in a bank vs. workers in public administration). *All employees should always be clearly and a priori informed about the employee surveillance policy of the employer (when and where surveillance is taking place, what is the finality, what information is collected, how long it will be stored, what are the (procedural) rights of the employees when personal data are to be used as evidence, etc.)*.[52]

Specific cyber territories for children have to be devised along the same lines. The United Nations Convention on the Rights of the Child (1990) contains a specific privacy right for children, and sets up monitoring instruments such as National Children's Rights Commissioners. Opinions of such advisory bodies should be carefully taken into account in policy discussion. National Children's Rights Commissioners could take up problems relating to the permanent digital monitoring of children.

5.3.3.4 Recommendation regarding restrictions on use of illegally obtained evidence

As concluded in the legal analysis of the dark scenarios above, courts are willing to protect one's privacy but, at the same time, they tend to admit evidence obtained through a violation of privacy or data protection.[53] There is a lack of clarity and uniformity regarding the consequence of privacy violations.

The European Court of Human Rights is unwilling to recognise a right to have evidence obtained through privacy violations rejected.[54] This line of reasoning is

---

[51] A similar recommendation has been proposed by the Article 29 Data Protection Working Party in *Working Document on the Processing of Personal Data by means of Video Surveillance* (11750/02/EN–WP67), adopted on 25 November 2002. http://ec.europa.eu/justice_home/fsj/privacy/

[52] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace*, op. cit.

[53] See Chapter 3, section 3.2.8.1.

[54] In the case of *Khan* v. *United Kingdom*, judgment of 12 May 2000, the European Court of Human Rights rejected the exclusionary rule. In that case, the evidence was secured by the police in a manner incompatible with the requirements of Article 8 of the European Convention on Human Rights (ECHR). The court accepted that the admission of evidence obtained in breach of the privacy right is not necessarily a breach of the required fairness under Article 6 of ECHR (the right to a fair trial), since the process taken as a whole was fair in the sense of Article 6. The evidence against the accused was admitted and led to his conviction. The Khan doctrine (followed in cases such as *Doerga* v. *The Netherlands* and *P.G. and J.H.* v. *The United*

followed by at least some national courts.[55] The fact that there is no general acceptance of an exclusionary rule creates legal uncertainty. Its general acceptance is, however, necessary to protect the opacity of the individual in a more effective way.

The departure from such position by the courts (namely "no inclusion of evidence obtained through privacy and/or data protection law infringements") could be considered and legislative prohibition of the admissibility (or general acceptance of the exclusionary rule) of such obtained evidence envisaged.[56]

5.3.3.5 Recommendations regarding implants

In ambient intelligence, the use of implants can no longer be considered as a kind of futuristic or extraordinary exception. Whereas it is clear that people may not be forced to use such implants, people may easily become willing to equip themselves with such implants on a (quasi) voluntary basis, be it, for example, to enhance their bodily functions or to obtain a feeling of security through always-on connections to anticipate possible emergencies. Such a trend requires a careful assessment of the opacity and transparency principles at a national, European and international level.

Currently, in Europe, the issue of medical implants has already been addressed.[57] In AmI, however, implants might be used for non-medical purposes. One of our dark scenarios suggests that organisations could force people to have an implant so they could be located anywhere at any time.

Now, the law provides for strict safety rules for medical implants. The highest standards of safety should be observed in AmI. The European Group on Ethics in Science and New Technologies also recommends applying the precautionary principle as a legal and ethical principle when it considers the use of implantable technologies. It also reminds us that the principles of data minimisation, purpose specification, proportionality and relevance are in particular applicable to implants. It means, inter alia, that implants should only be used when the aim

---

Kingdom) is discussed in De Hert, P., "De soevereiniteit van de mensenrechten: aantasting door de uitlevering en het bewijsrecht" [Sovereignty of human rights: threats created by the law of extradition and by the law of evidence], Panopticon, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, Vol. 25, No. 3, 2004, pp. 229–238 and in De Hert, P., and F.P. Ölcer, "Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging" [The notion of privacy made innocent. Implications for criminal procedure], *Strafblad. Het nieuwe tijdschrift voor strafrecht*, Vol. 2, No. 2, 2004, pp. 115–134. See also De Hert, P., *Biometrics: legal issues and implications*, Background paper for the Institute of Prospective Technological Studies, DG JRC, European Commission, Seville, January 2005, p. 33.

[55] Cour de Cassation (Belgium) 2 March 2005. http://www.juridat.be

[56] Although such a finding seems to contradict current case law (such as the *Khan* judgment), which has refused to apply the principle that evidence obtained in violation of privacy be rejected.

[57] Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active medical devices, *Official Journal* L 323, 26 November 1997, p. 39.

cannot be achieved by less body-intrusive means. Informed consent is necessary to legitimise the use of implants. We agree with those findings.

The European Group on Ethics in Science and New Technologies goes further, stating that non-medical (profit-related) applications of implants constitute a potential threat to human dignity. Applications of implantable surveillance technologies are only permitted when there is an urgent and justified necessity in a democratic society, and must be specified in legislation.[58] We agree that such applications should be diligently scrutinised.

We propose that the appropriate authorities (e.g., the Data Protection Officer) control and authorise applications of implants after the assessment of the particular circumstances in each case. When an implant enables tracking of people, people should have the possibility to disconnect the implant at any given moment and they should have the possibility to be informed when a (distant) communication (e.g., through RFID) is taking place.

We agree with the European Group on Ethics in Science and New Technologies that irreversible ICT implants should not be used, except for medical purposes. Further research on the long-term impact of ICT implants is also recommended.[59]

5.3.3.6 Recommendations regarding anonymity, pseudonymity, credentials and trusted third parties

Another safeguard to guarantee the opacity of the individual is the possibility to act under anonymity (or at least under pseudonymity or "revocable anonymity").

The Article 29 Working Party has considered anonymity as an important safeguard for the right to privacy. We repeat here its recommendations:

(a) The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy online as they currently enjoy offline.
(b) Anonymity is not appropriate in all circumstances.
(c) Legal restrictions which may be imposed by governments on the right to remain anonymous, or on the technical means of doing so (e.g., availability of encryption products) should always be proportionate and limited to what is necessary to protect a specific public interest in a democratic society.
(d) The sending of e-mail, the passive browsing of World Wide Web sites, and the purchase of most goods and services over the Internet should all be possible anonymously.

[58] European Group on Ethics in Science and New Technologies, "Ethical Aspects of ICT Implants in the Human Body", Opinion to the Commission, 16 March 2005. http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

[59] Ibid.

(e) Some controls over individuals contributing content to online public fora are needed, but a requirement for individuals to identify themselves is in many cases disproportionate and impractical. Other solutions are to be preferred.
(f) Anonymous means to access the Internet (e.g., public Internet kiosks, prepaid access cards) and anonymous means of payment are two essential elements for true online anonymity.[60]

According to the Common Criteria for Information Technology Security Evaluation Document (ISO 15408),[61] anonymity is only one of the requirements for the protection of privacy, next to pseudonymity, unlinkability, unobservability, user control/information management and security protection. All these criteria should be considered as safeguards for privacy.

The e-signature Directive promotes the use of pseudonyms and, at the same time, aims to provide security for transactions. *The probative value of digital signatures is regulated differently under the national laws of Member States*.[62] *More clarity as to the legal value of electronic signatures would be desirable, so that its admissibility as evidence in legal proceedings is fully recognised*.[63] *The status of pseudonymity under the law needs further clarification. A pseudonym prevents disclosure of the real identity of a user, while still enabling him to be held responsible to the other party if necessary. It may provide a privacy tool, and remedy against profiling. Using different pseudonyms also prevents the merging of profiles from different domains. However, the legal status of pseudonyms is unclear, i.e., whether they should be regarded as anonymous data or as personal data falling under the data protection regime. Clarification of the issue is desirable*.[64]

---

[60] Article 29 Data Protection Working Party, *Recommendation 3/97: Anonymity on the Internet* (WP 6), adopted on 3 December 1997. http://ec.europa.eu/justice_home/fsj/privacy/

[61] ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security*, First edition, International Organization for Standardization, Geneva, 1999.

[62] The German example was described in Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and Biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, p. 29. http://www.fidis.net

[63] Currently, the Directive on electronic signatures states that only advanced electronic signatures (those based on a qualified certificate and created by a secure signature-creation device) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data and are admissible as evidence in legal proceedings. Member States must ensure that an electronic signature (advanced or not) is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: (a) in electronic form, (b) not based upon a qualified certificate, (c) not based upon a qualified certificate issued by an accredited certification service-provider, or (d) not created by a secure signature-creation device.

[64] Olsen T., T. Mahler et al., "Privacy – Identity Management, Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *LEGAL Issues for the Advancement of Information Society Technologies*, LEGAL IST Deliverable D11, 2005. See the LEGAL IST web site http://193.72.209.176/default.asp?P = 369&obj = P1076

In ambient intelligence, the concept of *unlinkability* can become as important as the concept of anonymity or pseudonymity. Unlinkability "ensures that a user may make multiple uses of resources or services without others being able to link these uses together. … Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."[65] When people act pseudonymously or anonymously, their behaviour in different times and places in the ambient intelligence network could still be linked and consequently be subject to control, profiling and automated decision-making: linking data relating to the same *non-identifiable* person may result in similar privacy threats as linking data that relate to an identified or identifiable person.

Thus, in addition to and in line with the right to remain anonymous goes the use of anonymous and pseudonymous credentials, accompanied with unlinkability in certain situations (e.g., e-commerce), reconciling thus the privacy requirements with the accountability requirements of, e.g., e-commerce. In fact, such mechanisms should always be foreseen when disclosing someone's identity or when linking the information is not necessary. Such necessity should not be easily assumed, and in every circumstance more privacy-friendly technological solutions should be sought.[66] *However, the use of anonymity should be well balanced. To avoid its misuse, digital anonymity could be further legally regulated, especially stating when it is not appropriate.*[67]

5.3.3.7 Recommendation regarding criminal liability rules

Provisions on criminal liability are necessary to prevent cybercrime. The criminal law is a basic means to fight hackers, attackers and others tending to abuse the possibilities of communication. Moreover, *effective* criminal provisions have a general deterrent effect, thus stopping people from undertaking criminal activities.

Cybercrime has cross-border dimensions and global implications. The restrictive interpretation of criminal laws ("nulla poena sine crimen") requires international consensus on the definition of the different crimes. This issue has been addressed

[65] ISO99 ISO IS 15408, 1999. http://www.commoncriteria.org/. See also Pfizmann, A., and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, Version v0.27, 20 February 2006. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Pfizmann and Hansen define unlinkability as follows: "*Unlinkability* of two or more items (e.g., subjects, messages, events, actions, …) means that within the system (comprising these and possibly other items), from the attacker's perspective, these items are no more and no less related than they are related concerning his a-priori knowledge."

[66] Leenes, Ronald, and Bert-Jan Koops, " 'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No. 3, 2005, p. 37.

[67] Compare Gasson, M., M. Meints and K. Warwick (eds.), "A study on PKI and biometrics", FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, pp. 35–36. http://www.fidis.net

by the Cybercrime Convention,[68] which provides a definition for several criminal offences related to cybercrime and for general principles concerning international co-operation. The Cybercrime Convention, however, allows for different standards of protection. The Convention obliges its signatories to criminalise certain offences under national law, but Member States are free to narrow the scope of the definitions. The most important weakness of this Convention is the slow progress in its ratification by signatory states.

Council Framework Decision 2005/222/JHA[69] also provides for criminal sanctions against cybercrimes. The Framework decision is limited, however, both in scope and territory, since it only defines a limited number of crimes and is only applicable to the Member States of the European Union.

It is highly recommended that governments ensure a proper ratification of the Cybercrime Convention. A "revision" mechanism would desirable so that signatories could negotiate and include in the Convention definitions of new, emerging cybercrimes. Specific provisions criminalising identity theft and (some forms of) unsolicited communication could be included within the scope of the Convention.

International co-operation in preventing, combating and prosecuting criminals is needed and may be facilitated by a wide range of technological means, but these new technological possibilities should not erode the privacy of innocent citizens who are deemed to be not guilty until proven otherwise. Cybercrime prosecution, and more importantly crime prevention, might be facilitated by a wide range of technological means, among them, those that provide for the security of computer systems and data against attacks.[70]

5.3.4 Specific recommendations regarding data protection

5.3.4.1 Introduction

Almost all human activity in AmI can be reduced to personal data processing: opening doors, sleeping, walking, eating, putting lights on, shopping, walking in a street, driving a car, purchasing, watching television and even breathing. In short, all physical actions become digital information that relates to an identified or identifiable individual.

Often, the ambient intelligence environment will need to adapt to individuals and will therefore use profiles applicable to particular individuals or to individuals

[68] Council of Europe, Cybercrime Convention of 23 November 2001.

[69] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal* L 069, 16 March 2005.

[70] Pfitzmann, A., and M. Kohntopp, "Striking a Balance between Cyber-Crime and Privacy", *IPTS Report* 57, EC-JRC, Seville, September 2001. http://www.jrc.es/home/report/english/articles/vol57/welcome.htm

within a group profile.[71] AmI will change not only the amount, but also the quality of data collected so that we can be increasingly supported in our daily life (a goal of ambient intelligence). AmI will collect data not only about what we are doing, when we do it and where we are, but also data on how we have experienced things.[72] One can assume that the accuracy of the profiles, on which the personalisation of services depends, will improve as the amount of data collected grows. But as others hold more of our data, so grow the privacy risks. Thus arises the fundamental question: Do we want to minimise personal data collection?

Instead of focusing on reducing the amount of data collected alone, should we admit that they are indispensable for the operation of AmI, and focus rather on empowering the user with a means to control such processing of personal data?

Data protection is a tool for empowering the individual in relation to the collection and processing of his or her personal data. The European Data Protection Directive imposes obligations on the data controller and supports the rights of the data subject with regard to the transparency and control over the collection and processing of data. It does not provide for prohibitive rules on data processing (except for the processing of sensitive data and the transfer of personal data to third countries that do not ensure an adequate level of protection). Instead, the EU data protection law focuses on a regulatory approach and on channelling, controlling and organising the processing of personal data. As the title of Directive 95/46/EC indicates, the Directive concerns both the protection of the individual with regard to the processing of personal data *and* the free movement of such data. The combination of these two goals in Directive 95/46/EC reflects the difficulties we encounter in the relations between ambient intelligence and data protection law.

There is no doubt that some checks and balances in using data should be put in place in the overall architecture of the AmI environment. Civil movements and organisations dealing with human rights, privacy or consumer rights, observing and reacting to the acts of states and undertakings might provide such guarantees. It is also important to provide incentives for all actors to adhere to legal rules. Education, media attention, development of good practices and codes of conducts are of crucial importance. Liability rules and rules aimed at enforcement of data protection obligations will become increasingly important.

---

[71] See Hildebrandt, M., and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society) Deliverable D7.2; Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS Deliverable D7.3. Chapter 7 of this deliverable deals with legal issues on profiling. See also Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling on democracy and the rule of law*, FIDIS Deliverable D7.4, September 2005. http://www.fidis.net

[72] Lahlou, Saadi, Marc Langheinrich and Carsten Rocker, "Privacy and trust issues with invisible computers", *Communications of the ACM*, Vol. 48, No. 3, March 2005, pp. 59–60.

5.3.4.2 The right to be informed

Data protection law provides for the right to information on data processing, access to or rectification of data, which constitute important guarantees of individual rights. However, its practical application in an AmI era could easily lead to an administrative nightmare, as information overload would make it unworkable. We should try to remedy such a situation in a way that does not diminish this right.

The individual's right to information is a prerequisite to protect his interests. Such a right corresponds to a decentralised system of identity (data) management, but it seems useful to tackle it separately to emphasise the importance of the individual's having access to information about the processing of his data. Because of the large amounts of data to be processed in an AmI world, the help of or support by intelligent agents to manage such information streams seems indispensable.

The obligation to inform the data subject about when and which data are collected, by whom and for what purpose gives the data subject the possibility to react to mistakes (and thus to exercise his right to rectification of data) or abuses, and enables him to enforce his right in case of damage. It would be desirable to provide the individual not only with information about what data relating to him are processed, but also what knowledge has been derived from the data.

Information about what knowledge has been derived from the data could help the individual in proving causality in case of damage. Further research on how to reconcile access to the knowledge in profiles (which might be construed as a trade secret in some circumstances) with intellectual property rights would be desirable.

5.3.4.3 Information notices

The right to be informed could be facilitated by providing information in a machine-readable language, enabling the data subject to manage the information flow through or with the help of (semi-) autonomous intelligent agents. Of course, this will be more difficult in situations of passive authentication, where no active involvement of the user takes place (e.g., through biometrics and RFIDs).

Thus, information on the identity of the data controller and the purposes of processing could exist both in human-readable and machine-readable language. The way such information is presented to the user is of crucial importance – i.e., it must be presented in an easily comprehensible, user-friendly way.

In that respect, the Article 29 Working Party has provided useful guidelines and proposed multilayer EU information notices[73] essentially consisting of three layers:

[73] Article 29 Data Protection Working Party, *Opinion on More Harmonised Information Provisions* (11987/04/EN – WP 100), adopted on 25 November 2004. http://ec.europa.eu/justice_home/fsj/privacy/. The Article 29 WP provides examples of such notices (appendixes to the opinion on More Harmonised Information Provisions). See also Meints, M., "AmI – The European Perspective on Data Protection Legislation and Privacy Policies", presentation at the SWAMI International Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006.

Layer 1 – The short notice contains core information required under Article 10 of the Data Protection Directive (identity of the controller, purpose of processing, or any additional information which, in the view of the particular circumstances of the case, must be provided to ensure fair processing). A clear indication must be given as to how the individual can access additional information.

Layer 2 – The condensed notice contains all relevant information required under the Data Protection Directive. This includes the name of the company, the purpose of the data processing, the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the possibility of transfer to third parties, the right to access, to rectify and oppose choices available to the individual. In addition, a point of contact must be given for questions and information on redress mechanisms either within the company itself or details of the nearest data protection agency.

Layer 3 – The full notice includes all national legal requirements and specificities. It could contain a full privacy statement with possible additional links to national contact information.

We recommend that industry and law enforcement agencies consider an approach for AmI environments similar to that recommended by the Article 29 Working Party. Electronic versions of such notices should be sufficient in most of circumstances.

5.3.4.4 Data laundering obligations

Our dark scenarios indicate a new kind of practice that has emerged in recent years in the sector of personal data trading: while some companies collect personal data in an illegal way (not informing the data subjects, transfer of data to third parties without prior consent, usage for different purposes, installing spyware, etc.), these personal data are shared, sold and otherwise transferred throughout a chain of existing and disappearing companies to the extent that the origin of the data and the original data collector cannot be traced back. This practice has been described as "data laundering", with analogy to money laundering: it refers to a set of activities aiming to cover the illegitimate origin of data. In our AmI future, we should assume the value of personal data and therefore the (illegal) trading in these data will only grow.

A means to prevent data laundering could be to oblige those who buy or otherwise acquire databases, profiles and vast amounts of personal data to check diligently the legal origin of the data. Without checking the origin and/or legality of the databases and profiles, one could consider the buyer equal to a receiver of stolen goods and thus held liable for illegal data processing. They could be obliged to notify the national data protection officers when personal data(bases) are acquired. Those involved or assisting in data laundering could be subject to criminal sanctions.

5.3.4.5 Restricted interoperability

AmI requires efficient, faultless exchanges of relevant data and information throughout the AmI network. The need for efficiency requires interoperable data formats and interoperable hardware and software for data processing. Dark scenario 2 (about the bus accident) has shown the need for interoperability in ambient intelligence, but it must be recognised that, at the same time, interoperable data and data processing technologies in all sectors and all applications could threaten trust, privacy, anonymity and security. Full interoperability and free flow of personal data are not always desirable, and should not be considered as unquestionable.

Interoperability can entail an unlimited availability of personal data for any purpose. Interoperability may infringe upon the finality and purpose specification principles and erode the rights and guarantees offered by privacy and data protection law. Moreover, the purposes for which the data are available are often too broadly described (What is "state security", "terrorism", "a serious crime"?). Data can become available afterwards for *any* purpose. Interoperability of data and data processing mechanisms facilitates possible *function creep* (use of data for purposes other than originally envisaged).

Interoperability could contribute to the criminal use of ambient intelligence, for example, by sending viruses to objects in the network (interoperability opens the door for fast transmission and reproduction of a virus) or abusing data (interoperable data formats make data practical for any usage). Interoperability is thus not only a technological issue.

Awareness – already today – of the possible negative sides of interoperability should bring about a serious assessment of both law and technology *before* the market comes up with tools for interoperability. Legal initiatives in France (e.g., requiring interoperability of the iTunes music platform) and sanctions imposed by the European Commission (imposing interoperability of the Microsoft work group server operating system) indicate clearly that the need for interoperability is desired on a political and societal level.

In the Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 2005,[74] interoperability is defined as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge". This is, however, a more technological definition: It "explicitly disconnects the technical and the legal/political dimensions from interoperability, assuming that the former are neutral and the latter can come into play later or elsewhere. … Indeed, technological developments are not inevitable or neutral, which is *mutatis*

[74] Commission of the European Communities, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005) 597 final, Brussels, 24 November 2005.

mutandis also the case for technical interoperability. The sociology of sciences has shown that any technological artefact has gone through many small and major decisions that have moulded it and given it its actual form. Hence, the development of information technology is the result of micro politics in action. Technologies are thus interwoven with organisation, cultural values, institutions, legal regulation, social imagination, decisions and controversies, and, of course, also the other way round. Any denial of this hybrid nature of technology and society blocks the road toward a serious political, democratic, collective and legal assessment of technology. This means that technologies cannot be considered as *faits accomplis* or extra-political matters of fact."[75]

This way of proceeding has also been criticised by the European Data Protection Supervisor, according to whom this leads to justifying the ends by the means.[76]

Taking into account the need for interoperability, restrictions in the use and implementation of interoperability are required based on the purpose specification and proportionality principles. To this extent, a distinction between the processing of data for public (enforcement) and private (support) purposes may be absolutely necessary. Access to the databases by state enforcement agencies may be granted only on a case-by-case basis. Hereby, interoperability should not only be seen as a technical issue (solved by technical means) but also as a political, legal and economic issue (solved by political, legal and economic means). In addition, interoperability of the ambient intelligence system with third country systems that do not offer an adequate level of protection is very questionable.[77]

To achieve certain purposes, for which access to data has been granted, access to the *medium* carrying the information (e.g., a chip) may be sufficient, for example, when verifying one's identity. There should always be clarity as to what authorities are being granted access. In the case of deployment of centralised databases, a list of authorities that have access to the data should be promulgated in an adequate,

---

[75] De Hert, P., and S. Gutwirth, "Interoperability of police databases: an accountable political choice", *International Review of Law Computers & Technology*, Vol. 20, Nos. 1 and 2, March–July 2006; De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection*', No. 1, 2006. www.vub.ac.be/LSTS/pub/Dehert/006.pdf

[76] European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final)*, Brussels, 28 February 2006. http://www.edps.eu.int/legislation/ Opinions_A/06-02-28_Opinion_availability_EN.pdf

[77] European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004)835 final)*, *Official Journal* C 181/27, 23 July 2005, pp. 13–29, sub 3.13. See also De Hert, P., "What are the risks and what guarantees need to be put in place in a view of interoperability of the databases?", *Standard Briefing Note 'JHA & Data Protection*', No. 1. www.vub.ac.be/LSTS/pub/Dehert/006.pdf

official, freely and easily accessible publication.[78] Such clarity and transparency would contribute to security and trust, and protect against abuses in the use of databases.

5.3.4.6 Proportionality and purpose limitation principle

The proportionality and purpose limitation principles are already binding under existing data protection laws. The collection and exchange of data (including interoperability) should be proportional to the goals for which the data have been collected. It will not be easy to elaborate the principles of proportionality and purpose limitation in ambient intelligence; previously collected data may serve for later developed applications or discovered purposes. Creation and utilisation of databases may offer additional benefits (which are thus additional purposes), e.g., in the case of profiling. Those other (derived) purposes should, as has been indicated in the opinion of the European Data Protection Supervisor, be treated as independent purposes for which all legal requirements must be fulfilled.[79]

Technical aspects of system operation can have a great impact on the way a system works, and how the proportionality principles and purpose limitation principles are implemented since they can determine, for example, if access to the central database is necessary, or whether access to the chip or part of the data is possible and sufficient.

5.3.4.7 Biometrics

Biometric technology can be a useful tool for authentication and verification, and may even be a privacy-enhancing technology. However, it can also constitute a threat to fundamental rights and freedoms. Thus, specific safeguards should be put in place. Biometric safeguards have already been subject of reflection by European data protection authorities: the Article 29 Working Party has stated that biometric data are in most cases personal data, so that data protection principles apply to processing of such data.[80]

---

[78] European Data Protection Supervisor, *Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, (COM (2004) 835 final)*, *Official Journal* C 181/27, 23 July 2005, pp. 13–29, sub 3.7.

[79] Ibid., sub 3.2.

[80] See Article 29 Data Protection Working Party, *Working document on biometrics* (12168/02/EN – WP 80), adopted on 1 August 2003. http://ec.europa.eu/justice_home/fsj/privacy/. See also Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005, available through http://www.fidis.net [deliverables]

On the principle of proportionality, the Article 29 Working Party points out that it is not necessary (for the sake of authentication or verification) to store biometric data in central databases, but in the medium (e.g., a card) remaining in the control of the user.[81]

The creation and use of centralised databases should always be carefully assessed before their deployment, including prior checking by data protection authorities. In any case, all appropriate security measures should be put in place.

Framing biometrics is more than just deciding between central or local storage. Even storage of biometric data on a smart card should be accompanied by other regulatory measures that take the form of rights for the card-holders (to know what data and functions are on the card; to exclude certain data or information from being written onto the card; to reveal at discretion all or some data from the card; to remove specific data or information from the card).[82]

Biometric data should not be used as unique identifiers, mainly because biometric data still do not have sufficient accuracy.[83] Of course, this might be remedied in the progress of science and technological development. There remains, however, a second objection: using biometrics as the primary key will offer the possibility of merging different databases, which can open the doors for abuses (function creep).

European advisory bodies have considered biometric data as a unique identifier. Generally speaking, since the raw data might contain more information than actually needed for certain finalities (including information not known at the moment of the collection, but revealed afterwards due to progress in science, e.g., health information related to biometric data), it should not be stored.[84] Other examples of opacity rules applied to biometrics might be prohibitions on possible use of

[81] See also De Hert, P., *Biometrics: legal issues and implications*, Background paper for the Institute of Prospective Technological Studies, EC – JRC, Seville, January 2005, p. 13. http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf

[82] Neuwrit, K., *Report on the protection of personal data with regard to the use of smart cards*, Report of Council of Europe (2001), accessible through http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents, quoted by De Hert, P., *Biometrics: legal issues and implications,* p. 26.

[83] Institute for Prospective Technological Studies (IPTS), *Biometrics at the frontiers: assessing the impact on Society*, Study commissioned by the LIBE committee of the European Parliament, EC – DG Joint Research Centre, Seville, February 2005. http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

[84] European Data Protection Supervisor (EDPS), *Comments on the Communication of the Commission on interoperability of European databases*, 10 March 2006. http://www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf

"strong" multimodal biometrics (unless for high security applications)[85] for everyday activities. Codes of conduct can be appropriate tools to further regulate the use of technology in particular sectors.[86]

5.3.4.8 RFIDs

AmI will depend on profiling as well as authentication and identification technologies. To enable ubiquitous communication between a person and his or her environment, both things and people will have to be traced and tracked. RFID seems to offer the technological means to implement such tracking. Like biometrics, RFID is an enabling technology for real-time monitoring and decision making. Like biometrics, RFIDs can advance the development of AmI and provide many advantages for users, companies and consumers.[87]

No legislative action seems needed to support this developing technology. Market mechanisms are handling this. There is, however, a risk to the privacy interests of the individual and for a violation of the data protection principles, as CASPIAN and other privacy groups have stated.[88]

RFID use should be in accordance with privacy and data protection regulations. The Article 29 Working Party has already given some guidelines on the application of the principles of EU data protection legislation to RFIDs.[89] It stresses that the data protection principles (purpose limitation principle, data quality principle, conservation

[85] Biometrics, and especially multimodal biometrics, may increase the security of an application, and thus privacy as well. In its technical safeguards, the SWAMI consortium proposes use of multimodal fusion of several less privacy-intrusive biometrics (e.g., fat, weight, height, gait, behavioural patterns) for everyday activities such as user-friendly authentication in mobile phones or authentication of car drivers. Such biometrics have low accuracy now, but such emerging technology will most likely become more accurate in due course and represent a lower threat to privacy than "strong" biometrics. For high-security applications, we recommend a combination of strong multimodal biometrics with continuous unobtrusive authentication by less strong biometrics, provided that all modalities of the strong biometrics have good anti-spoofing capabilities. Use of biometrics should always be accompanied by adequate PETs.

[86] Article 29 Data Protection Working Party, *Working document on biometrics*.

[87] A description of RFID technologies and of usages can be found in Hildebrandt, M., and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS (Future of Identity in the Information Society), Deliverable D7.2, June 2005. http://www.fidis.net

[88] See e.g. Günther, Oliver, and Sarah Spiekermann, "RFID and the Perception of Control: The Consumer's View", *Communications of the ACM*, Vol. 48, No. 9, 2005, pp. 73–76.

[89] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology* (10107/05/EN – WP 105), 19 January 2005. http://ec.europa.eu/justice_home/fsj/privacy/

principle, etc.) must always be complied with when the RFID technology leads to processing of personal data in the sense of the Data Protection Directive.[90]

As the Article 29 Working Party points out, the consumer should always be informed about the presence of both RFID tags and readers, as well as of the responsible controller, the purpose of the processing, whether data are stored and the means to access and rectify data. Here, techniques of (visual) indication of activation would be necessary. The data subject would have to give his consent for using and gathering information for any specific purpose. The data subject should also be informed about what type of data is gathered and whether the data will be used by the third parties.

In AmI, such rights may create a great burden, both on the data subject, on the responsible data controller and on all data processors. Though adequate, simplified notices about the data processors' policy would be welcome (e.g., using adequate pictograms or similar means). In our opinion, such information should always be provided to consumers when RFID technology is used, even if the tag does not contain personal data in itself.[91] The data subject should also be informed how to discard, disable or remove the tag. The right to disable the tag can relate to the consent principle of data protection, since the individual should always have the possibility to withdraw his consent.

Disabling the tag should at least be possible when the consent of the data subject is the sole legal basis for processing the data. Disabling the tag should not lead to any discrimination of the consumer (e.g., in terms of the guarantee conditions).

Technological and organisational measures (e.g., the design of RFID systems) are of crucial importance in ensuring that the data protection obligations are respected (privacy by design, e.g., by technologically blocking unauthorised access to the data). Thus, availability and compliance with privacy standards are of particular importance.[92]

---

[90] The concept of "personal data" in the context of RFID technology is contested. WP 29 states: In assessing whether the collection of personal data through a specific application of RFID is covered by the Data Protection Directive, we must determine: (a) the extent to which the data processed relates to an individual, and (b) whether such data concerns an individual who is identifiable or identified. Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. In assessing whether information concerns an identifiable person, one must apply Recital 26 of the Data Protection Directive which establishes that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." And further: "Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity, are if not identified, identifiable, also triggers the application of the data protection Directive." Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, 10107/05/EN WP 105, 19 January 2005, point 4.1.

[91] Still, such information on a tag can be a unique identifier enabling the profiling activities. See Kardasiadou, Z., and Z. Talidou, *Report on Legal Issues of RFID Technology*, LEGAL IST (Legal Issues for the Advancement of Information Society Technologies) Deliverable D15, 2006, p. 16.

[92] Some standards have already been adopted in the RFID domain. The International Organization for Standardization has developed sector-specific standards, as well as more generic standards. EPCglobal Ltd. (www.epcglobal.org), an industry-driven organisation, has also developed some standards on connecting servers containing information relating to items identified by EPC (Electronic Product Code) numbers.

Data protection concerns should be reflected in initiatives leading to standardisation of technical specifications. Privacy assessment of each particular RFID application could be a legally binding obligation.[93]

Further research on the RFID technology and its privacy implications is recommended.[94] This research should also aim at determining whether any legislative action is needed to address the specific privacy concerns of RFID technology. Further development of codes of conducts and good practices is also recommended.[95]

5.3.4.9 Data protection and profiling: a natural pair

Profiling is as old as life, because it is a kind of knowledge that unconsciously or consciously supports the behaviour of living beings, humans not excluded. It might well be that the insight that humans often "intuitively know" something before they "understand" it can be explained by the role profiling spontaneously plays in our minds.

Thus, there is no reason to prohibit automated profiling and data mining concerning individuals with opacity rules. Profiling activities should in principle be ruled by transparency tools. In other words, the processing of personal data – collection, registration and processing in the strict sense – is not prohibited but submitted to a number of conditions guaranteeing the visibility, controllability and accountability of the data controller and the participation of the data subjects.

Data protection rules apply to profiling techniques (at least in principle).[96] The collection and processing of traces surrounding the individual must be considered as processing of personal data in the sense of existing data protection legislation.

---

[93] Borking, J., "RFID Security, Data Protection & Privacy, Health and Safety Issues", presentation made during European Commission Consultation on RFID, Brussels, 17 May 2006.

[94] Such research is now carried out in the framework of the FIDIS programme. See FIDIS Deliverable 7 on AmI, profiling and RFID.

[95] An example of such (emerging) initiatives is the EPCglobal Ltd. guidelines regarding privacy in RFID technology, http://www.epcglobal.org/public_policy/public_policy_guidelines.html, and the CDT (Centre for democracy and technology) Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology, Interim Draft, 1 May 2006. http://www.cdt.org/privacy/20060501rfid-best-practices.php. Though these are good examples of the involvement of stakeholders in the discussion, the results are not fully satisfactory. As a compromise between the different actors, the guidelines do not go far enough in protecting the interests of consumers. The ambiguous wording of some guidelines (e.g., whether practicable) may give flexibility to industry to interpret the scope of their obligations.

[96] We add "at least in principle" because we are well aware of the huge practical difficulties of effectively enforcing and implementing data protection, more particularly in the field of profiling. See Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, August 2005. http://www.fidis.net. See also Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", to be published in M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European citizen*, Springer, Dordrecht, 2008 (forthcoming). See also the discussion on RFID above.

Both individual and group profiling are dependent on such collection and on the processing of data generated by the activities of individuals. And that is precisely why, in legal terms, no profiling is thinkable outside data protection.

There is an ongoing debate in contemporary legal literature about the applicability of data protection to processing practices with data that are considered anonymous, i.e., they do not allow the identification of a specific individual.[97] Some contend that data protection rules do not allow processing practices that bring together data on certain individuals without trying to identify the said individual (in terms of physical location or name). Some contend that data protection rules do not apply to profiling practices that process data relating to non-identifiable persons (in the sense of the Data Protection Directive). We hold that it is possible to interpret the European data protection rules in a broad manner covering *all* profiling practices,[98] but the courts have not spoken on this yet.

Data protection should apply to all profiling practices. When there is confusion in the application and interpretation of the legal instruments, they should be adapted so that they do apply to all profiling practices. Profiling practices and the consequent personalisation of the ambient intelligence environment lead to an accumulation of power in the hands of those who control the profiles and should therefore be made transparent.

The principles of data protection are an appropriate starting point to cope with profiling in a democratic constitutional state as they do impose good practices. Nevertheless, while the default position of data protection is transparency ("Yes, you can process, but …"), it does not exclude opacity rules ("No, you cannot process, unless …"). In relation to profiling, two examples of such rules are relevant. On the one hand, of course, there is the explicit prohibition against taking decisions affecting individuals solely on the basis of the automated application of a profile without human intervention (see Article 15 of the Data Protection Directive).[99] This seems obvious because in such a situation, probabilistic knowledge is applied to a real

---

[97] We recall that *personal data* in the EU Data Protection Directive refers to "any information relating to an identified or identifiable natural person" (Article 1).

[98] De Hert, P., "European Data Protection and E-Commerce: Trust Enhancing?", in J.E.J. Prins, P.M.A. Ribbers, H.C.A. Van Tilborg, A.F.L. Veth and J.G.L. Van Der Wees (eds.), *Trust in Electronic Commerce,* Kluwer Law International, The Hague, 2002, pp. 190–199. See also Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector."

[99] Article 15 on automated individual decisions states: "1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests."

person. On the other hand, there is the (quintessential) purpose specification principle, which provides that the processing of personal data must meet specified, explicit and legitimate purposes. As a result, the competence to process is limited to well-defined goals, which implies that the processing of the same data for other incompatible aims is prohibited. This, of course, substantially restricts the possibility to link different processing and databases for profiling or data mining objectives. The purpose specification principle is definitely at odds with the logic of interoperability and availability of personal data: the latter would imply that all databases can be used jointly for profiling purposes.[100] In other words, the fact that the legal regime applicable to profiling and data mining is data protection does not give a *carte blanche* to mine and compare personal data that were not meant to be connected.[101]

The European Data Protection Supervisor indicated in his Annual Report 2005 a number of processing operations that are likely to encompass specific risks to the rights and freedoms of data subjects, even if the processing does not occur upon sensitive data. This list relates to processing operations (a) of data relating to health and to suspected offences, offences, criminal convictions or security measures, (b) intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct, (c) allowing linkages, not provided for pursuant to national or Community legislation, between data processed for different purposes, and (d) for the purpose of excluding individuals from a right, benefit or contract.[102]

5.3.5 Specific recommendations regarding security

Software can be the tool for regulating one's behaviour by simply allowing or not allowing certain acts. Thus, technology constituting the "software code" can affect the architecture of the Internet (and thus potentially of AmI) and can provide effective means for enforcing the privacy of the individual. For example, cryptology might give many benefits: it could be used for pseudonymisation (e.g., encrypting IP addresses) and ensuring confidentiality of communication or commerce.[103]

Privacy-enhancing technologies can have an important role to play, but they need an adequate legal framework.

---

[100] De Hert, P., "What are the risks and what guarantees need to be put in place in view of interoperability of police databases?", Standard Briefing Note 'JHA & Data Protection', No. 1, produced in January 2006 on behalf of the European Parliament. http://www.vub.ac.be/LSTS/

[101] Gutwirth, S., and P. De Hert, "Regulating profiling in a democratic constitutional state", to be published in M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European citizen*, Springer, Dordrecht, 2008 (forthcoming).

[102] European Data Protection Supervisor (EDPS), *Annual Report 2005*, pp. 22–23. http://www.edps.eu.int/publications/annual_report_en.htm

[103] Leenes, Ronald, and Bert-Jan Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers &Technology*, Vol. 19, No. 3, 2005, pp. 331–332.

The Directive on the legal protection of software[104] obliges Member States to provide appropriate remedies against a person committing any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical devices which may have been applied to protect a computer program. This mechanism aims to protect programmes enforcing the intellectual property rights against circumvention.

Similar legal protection against circumvention of privacy-enhancing technologies could be legally foreseen.

Technology might go beyond what the law permits (e.g., DRM prevents intellectual property infringements but at the same time might limit the rights of the lawful user). Negative side effects of such technologies should be eliminated. More generally, when introducing new technology on the market, manufacturers together with relevant stakeholders should undertake a privacy impact assessment. *Development of a participatory impact assessment procedure would allow stakeholders to quickly identify and react to any negative features of technology* (see also section 5.3.10).

5.3.5.1 Empowering the individual

The European Data Protection Directive imposes obligations on the data controller and gives rights to the data subject. It aims to give the individual control over the collection and processing of his data. Many provisions in the Data Protection Directive have several weaknesses in an AmI environment. Principles of proportionality and fairness are relative and may lead to different assessments in similar situations; obtaining consent might not be feasible in the constant need for the collection and exchange of data; obtaining consent can be simply imposed by the stronger party. Individuals might not be able to exercise the right to consent, right to information, access or rectification of data due to the overflow of information. Thus, those rules might simply become unworkable in an AmI environment. And even if workable (e.g., thanks to the help of the digital assistants), are they enough? Should we not try to look for an approach granting the individual even more control?

5.3.5.2 Decentralised identity (data) management

Several European projects are involved in research on identity management. They focus on a decentralised approach, where a user controls how much and what kind of information he or she wants to disclose. Identity management systems, while operating on a need-to-know basis, offer the user the possibility of acting under pseudonyms, under unlinkability or anonymously, if possible and desirable.

[104] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17 May 1991, pp. 0042–0046.

Among the other examples of such systems,[105] there are projects that base their logic on the assumption that the individual has property over his data, and then could use licensing schemes when a transfer of data occurs. Granting him property over the data[106] is seen as giving him control over the information and its usage in a "distribution chain". However, it is doubtful if granting him property over the data will really empower the individual and give him a higher level of protection and control over his data. The property model also assumes that the data are disseminated under a contract. Thus, the question might arise whether the Data Protection Directive should serve as a minimum standard and thus limit the freedom of contracts.[107] But as our dark scenarios show, there exist many cases in which the individual will not be able to *freely* enter into a contract. Another question arises since *our* data are not always collected and used for commercial purposes. In most situations, the processing of personal data is a necessary condition for entering into a contractual relation (whereas the Data Protection Directive states in Article 7 that data processing without the individual's consent to use of his personal data is legitimate when such processing is necessary for the performance of a contract). The most obvious example is the collection of data by police, social insurance and other public institutions. The individual will not always be free to give or not give his data away. The property model will not address these issues. It will also not stop the availability of the data via public means.[108]

A weakness of the property model is that it might lead to treating data only as economic assets, subject to the rules of the market. But the model's aim is different: the aim is to protect personal data, without making their processing and transfer impossible. Regarding data as property also does not address the issue of the profile knowledge derived from personal data. This knowledge is still the property of the owner or the licenser of the profile. The data-as-property option also ignores the new and increasingly invisible means of data collection, such as RFIDs, cameras or online data collection methods.

Discussing the issue of whether personal data should become the individual's property does not solve the core problem. On the one hand, treating data as property may lead to a too high level of protection of personal information, which would conflict with the

[105] An overview of the existing identity management systems has been given by Bauer, M., M. Meints and M. Hansen (eds.), *Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS (Future of Identity in the Information Society) Deliverable D3.1, September 2005, and Hildebrandt, M., and J. Backhouse (eds.), *Descriptive analysis and inventory of profiling practices*, FIDIS Deliverable D7.2, June 2005, and Müller, G., and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net

[106] See Lessig, L., *Code and other law of cyberspace*, Basic Books, New York, 1999, and Leenes, Ronald, and Bert-Jan Koops, "'Code': Privacy's Death or Saviour?", *International Review of Law, Computers & Technology*, Vol. 19, No. 3, 2005, p. 329. See also Samuelson, P., "Privacy As Intellectual Property?", *Stanford Law Review*, Vol. 52, 2000.

[107] However, currently this is not the case. The weaker party in the contract is now protected by the general principles of law. Prins, J.E.J., "The Propertization of Personal Data and Identities", *Electronic Journal of Comparative Law*, Vol. 8.3, October 2004. http://www.ejcl.org/

[108] Ibid.

extensive processing needs of AmI. On the other hand, it would, by default, turn personal data into a freely negotiable asset, no longer ruled by data protection, but left to market mechanisms and consent of the data subjects (more often than not to the detriment of the latter). Finally, the data-as-property option loses its relevance in the light of a focus upon anonymisation and pseudonymisation of data processed in AmI applications.

The PRIME consortium proposes identity management systems controlled by data subjects.[109] It aims to enable individuals to negotiate with service providers the disclosure of personal data according to the conditions defined. Such agreement would constitute a contract.[110] An intelligent agent could undertake the management on the user side. This solution is based on the data minimisation principle and on the current state of legislation. It proposes the enforcement of (some) current data protection and privacy laws. It seems to be designed more for the needs of the world today than for a future AmI world. The user could still be forced to disclose more information than he or she wishes, because he or she is the weaker party in the negotiation; he or she needs the service.

The FIDIS consortium has also proposed a decentralised identity management, the vision of which seems to go a bit further than the PRIME proposal. It foresees that the user profiles are stored on the user's device, and preferences relevant for a particular service are (temporarily) communicated to the service provider for the purpose of a single service. The communication of the profile does not have to imply disclosure of one's identity. If there is information extracted from the behaviour of the user, it is transferred by the ambient intelligent device back to the user, thus updating his profile.[111] Thus, some level of exchange of knowledge is foreseen in this model, which can be very important for the data subject's right to information.

A legal framework for such sharing of knowledge from an AmI-generated profile needs to be developed, as well as legal protection of the technical solution enabling such information management. Such schemes rely on automated protocols for the policy negotiations. The automated schemes imply that the consent of the data subject is also organised by automatic means. We need a legal framework to deal with the situation wherein the explicit consent of the data subject for each collection of data is replaced by a "consent" given by an intelligent agent.

In such automated models, one could envisage privacy policies following the data. Such "sticky" policies, attached to personal data, would provide for clear information and indicate to data processors and controllers which privacy policy applies to the data concerned.[112] Sticky policies could facilitate the auditing and

---

[109] Hansen, M., and H. Krasemann (eds.), *Privacy and Identity Management for Europe*, PRIME White Paper, Deliverable D 15.1.d, 18 July 2005. http://www.prime-project.eu.org/

[110] Ibid., p. 7.

[111] Schreurs, W., M. Hildebrandt, M. Gasson and K. Warwick (eds.), *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, FIDIS (Future of Identity in the Information Society) Deliverable D7.3, August 2005, p. 32. http://www.fidis.net

[112] Meints, M., "AmI – The European Perspective on Data Protection Legislation and Privacy Policies", Presentation at the SWAMI Final Conference on Safeguards in a World of Ambient Intelligence, 21 March 2006.

self-auditing of the lawfulness of the data processing by data controllers.[113] *In any event, research in this direction is desirable*.

Since AmI is also a mobile environment, there is a need to develop identity management systems addressing the special requirements of mobile networks. The FIDIS consortium has prepared a technical survey of mobile identity management. It has identified some special challenges and threats to privacy in the case of mobile networks and made certain recommendations:

- Location information and device characteristics both should be protected.
- Ease of use of the mobile identity management tools and simplified languages and interfaces for non-experts should be enhanced.
- A verifiable link between the user and his digital identity has to be ensured. Accordingly, privacy should also be protected in peer-to-peer relationships.[114]

5.3.6 Specific recommendations regarding consumer protection law

The importance of consumer protection will grow in ambient intelligence, because of the likelihood that consumers will become more dependent on online products and services, and because product and service providers will strengthen their bargaining position through an increasing information asymmetry. Without the constraints of law, ambient intelligence service providers could easily dictate the conditions of participation in new environments. Consumer protection should find the proper balance in AmI.

Consumer protection law defines the obligations of the producers and the rights of consumer and consists of a set of rules limiting the freedom to contract, for the benefit of the consumer. Consumer protection law plays a role of its own, but can support the protection of privacy and data protection rights.[115]

The basis for the European framework for consumer protection rules can be found in Article 153 of the EC Treaty: "In order to promote the interests of consumers and to ensure a high level of consumer protection, the Community shall contribute to protecting the health, safety and economic interests of consumers, as well as

[113] For example, such an approach was adopted by the PAW project (Privacy in an Ambient World), which has developed the language enabling the distribution of data in a decentralised architecture, with the usage policies attached to the data that would provide information on what kind of usage has been licensed to the particular actor (licensee). Enforcement relies on auditing. http://www.cs.ru.nl/paw/results.html

[114] Müller, G., and S. Wohlgemuth (eds.), *Study on Mobile Identity Management*, FIDIS Deliverable D3.3, May 2005. http://www.fidis.net

[115] Although our focus here is on services, in an AmI environment, it can be difficult to distinguish between a product and a service. It is often difficult to draw the line between the two, and different legal regimes apply. Product liability issues are discussed below under section 5.3.8.4.

to promoting their right to information, education and to organise themselves in order to safeguard their interests."

Consumer protection at European level is provided by (amongst others) Directive 93/13 on unfair terms in consumer contracts,[116] Directive 97/7 on consumer protection in respect of distance contracts[117] and the Directive on liability for defective products (discussed below). Directive 93/13 and Directive 97/7 were both already discussed (in Chapter 3, sections 3.2.8.6 and 3.3.8.3). In many respects, their rules are not fitted to AmI and they need to be re-adapted. This especially relates to extending the scope of protection of those directives, thereby making sure that all services and electronic means of communications and trading are covered (including those services on the World Wide Web not currently covered by the Distance Contract Directive).[118]

5.3.6.1 Contracts could be concluded by intelligent agents

Due to the increasing complexity of online services, and due to the possibility of information overflow, it seems necessary to find legal ways to assess and recognise contracts made through the intervention of intelligent agents. Is the legal system flexible enough to endorse this? Moreover, the same should apply to the privacy policies and to the consent of individuals for the collection of data (because, in identity management systems, intelligent agents will decide what data are to be disclosed to whom).

Here is a challenge: how to technologically implement negotiability of contracts and the framework of binding law in electronic, machine-readable form?

5.3.6.2 Unfair privacy policies

Suppliers should not be allowed to set up privacy conditions which are manifestly not in compliance with the generally applicable privacy rules and which disadvantage the customer.

Data protection legislation and consumer protection law could constitute the minimum (or default) privacy protection level. Similar rules as those currently applicable under the consumer protection of Directive 93/13 on unfair terms in consumer contracts could apply. Mandatory rules of consumer protection require, *inter alia,* that contracts be drafted in plain, intelligible language, that the consumer

---

[116] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *Official Journal* L 095, 21 April 1993, pp. 29–34.

[117] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *Official Journal* L 144, 04 June 1997, pp. 0019–0027.

[118] Henderson, K., and A. Poulter, "The Distance Selling Directive: Points for Further Revision", *International Review for Law Computers & Technology*, Vol. 16, No. 3, 2002, pp. 289–300.

be given an opportunity to examine all terms, that – in cases of doubt – the interpretation most favourable to the consumer prevail.

Suppliers should not be allowed to unfairly limit their liability for security problems in the service they provide to the consumer.

In this respect, more attention could be given to a judgment of the Court of First Instance of Nanterre (France) in 2004 in which the online subscriber contract of AOL France was declared illegal in that it contained not less than 31 abusive clauses in its standard contractual terms (many of which infringed consumer protection law).[119]

5.3.6.3 Information to the consumer

The Directive on unfair terms in consumer contracts and the Directive on consumer protection in respect of distance contracts provide a broad right to information for the consumer. *It should be sufficient to dispense such information in electronic form*,[120] in view of the large amount of information directed towards consumers that would have to be managed by intelligent agents.

An increasing number of service providers will be involved in AmI services and it cannot be feasible to provide the required information about all of them. The solution may be to provide such information only about the service provider whom the consumer directly pays and who is responsible towards the consumer. Joint liability would apply (for liability issues, see below).

5.3.6.4 Right to withdrawal

The right to withdrawal, foreseen by the Directive 97/7 on consumer protection with respect to distance contracts, may not apply (unless otherwise agreed) to contracts in which (a) the provision of services has begun with the consumer's agreement before the end of the seven-working-day period and (b) goods have been made to the consumer's specifications or clearly personalised or which, by their nature, cannot be returned or are liable to deteriorate or expire rapidly.

In an AmI world, services will be provided instantly and will be increasingly personalised. This implies that the right of withdrawal will become inapplicable in many cases. New solutions should be developed to address this problem.

---

[119] Tribunal de grande instance de Nanterre, 2 June 2004 (*UFC Que Choisir* v. *AOL Bertelsmann Online France*). http://www.legalis.net/jurisprudence-decision.php3?id_article = 1211. For an English analysis, see Naylor, David, and Cyril Ritter, "B2C in Europe and Avoiding Contractual Liability: Why Businesses with European Operations Should Review their Customer Contracts Now", 15 September 2004. http://www.droit-technologie.org

[120] Currently, insofar as it is not received on a permanent medium, consumers must also receive written notice in good time of the information necessary for proper performance of the contract.

5.3.6.5 Temporary accounts

In AmI, payments will often occur automatically, at the moment of ordering or even offering the service.

Temporary accounts, administered by trusted third parties, could temporarily store money paid by a consumer to a product or service provider. This can support consumer protection and enforcement, in particular with respect to fraud and for effectively exercising the right of withdrawal. This would be welcome for services that are offered to consumers in the European Union by service providers located in third countries, as enforcement of consumer protection rights is likely to be less effective in such situations.

5.3.6.6 Group litigation and consumer claims

The possibility of group consumer litigation[121] can increase the level of law enforcement and, especially, enforcement of consumer protection law. Often an individual claim does not represent an important economic value, thus, individuals are discouraged from making efforts to enforce their rights.

Launching collective claims or similar actions would increase the effective power against service providers. A similar solution is now available at European level in the case of injunctions.

Bodies or organisations with a legitimate interest in ensuring that the collective interests of consumers are protected *can* institute proceedings before courts or competent administrative authorities and seek termination of any behaviour adversely affecting consumer protection and defined by law as illegal.[122] However, as far as actions for damages are concerned, issues such as the form and availability of group litigation are regulated by the national laws of the Member States as part of procedural law. The possibility to bring such a claim is restricted to a small number of states.[123]

---

[121] Group litigation is a broad term which captures collective claims (single claims brought on behalf of a group of identified or identifiable individuals), representative actions (single claims brought on behalf of a group of identified individuals by, e.g., a consumer interest association), class action (one party or group of parties may sue as representatives of a larger class of unidentified individuals), among others. These definitions as well as the procedural shape of such claims vary in different Member States. Waelbroeck D., D. Slater and G. Even-Shoshan G [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, p. 44. http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html. The SWAMI consortium abstains from designating one of these forms as adequate, which points to the controversial character of class actions on European grounds and thus proposes to focus on other possible forms. Instead, we recommend that the appropriate authority study the issue further.

[122] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 On injunctions for the protection of consumers' interests, *Official Journal* L 166, 11 June 1998, pp. 51–55.

[123] Belgian law provides that in certain circumstances associations can bring collective damage action or action for several individual damages. Waelbroeck D., D. Slater and G. Even-Shoshan [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44–47. http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.html

5.3.7 Specific recommendations regarding electronic commerce

5.3.7.1 The scope of the Directive on electronic commerce

The Directive on electronic commerce[124] aims to provide a common framework for information society services in the EU Member States. An important feature of the Directive is that it also applies to legal persons. Similar to the consumer protection legislation, the Directive contains an obligation to provide certain information to customers. In view of the increasing number of service providers, it may not be feasible to provide information about all of them. *Providing information about the service provider whom the customer pays directly and who is responsible towards him could be a solution to the problem of the proliferating number of service providers (joint liability may also apply here). The Directive should also be updated to include the possibility of concluding contracts by electronic means (including reference to intelligent agents) and to facilitate the usage of pseudonyms, trusted third parties and credentials in electronic commerce.*

5.3.7.2 Unsolicited communication (spam)

Unsolicited commercial communication is an undesirable phenomenon in cyberspace. It constitutes a large portion of traffic on the Internet, using its resources (bandwidth and storage capacity) and forcing Internet providers and users to adopt organisational measures to fight it (by filtering and blocking spam). Spam can also constitute a security threat.[125] The dark scenarios show that spam may become an even more serious problem than it is today.[126] An increase in the volume of spam can be expected because of the emergence of new means of electronic communication. Zero-cost models for e-mail services encourage these practices, and similar problems may be expected when mobile services pick up a zero-cost or flat-fee model.

As we become increasingly dependent on electronic communication – ambient intelligence presupposes that we are almost constantly online – we become more vulnerable to spam. In the example from the first dark scenario, spamming may cause irritation and make the individual reluctant to use ambient intelligence.

---

[124] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), *Official Journal* L 178, 17 July 2000, pp. 0001–0016.

[125] Sorkin, David E., "Technical and Legal Approaches to Unsolicited Electronic Mail", *University of San Francisco Law Review*, Vol. 35, 2001, p. 336 ff.

[126] See Chapter 3, Scenario 1, situation 2.

Fighting spam may well demand even more resources than it does today as new methods of spamming – such as highly personalised and location-based advertising – emerge.

Currently, many legal acts throughout the world penalise unsolicited communication, but without much success. The Privacy & Electronic Communication Directive[127] provides for an opt-in regime, applicable in the instance of commercial communication, thus inherently prohibiting unsolicited marketing.[128] Electronic communications are, however, defined as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information."[129] The communications need to have a commercial content in order to fall under the opt-in regulation of the Privacy & Electronic Communication Directive.[130]

Consequently, this Directive may not cover unsolicited, location-based advertisements with a commercial content that are broadcast to a group of people ("the public"). The impact of this exception cannot be addressed yet since location-based services are still in their infancy.

A broad interpretation of electronic communications is necessary (the Directive is technology-neutral). Considering any unsolicited electronic communication as spam, regardless of the content and regardless of the technological means, would offer protection that is adequate in ambient intelligence environments in which digital communications between people (and service providers) will exceed physical conversations and communications.[131]

---

[127] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Privacy & Electronic Communications Directive), *Official Journal* L 201, 31 July 2002, pp. 37–47.

[128] Andrews, S., *Privacy and human rights 2002*, produced by the Electronic Privacy Information Center (EPIC), Washington, DC, and *Privacy International*, London, 2002, p. 12. http://www.privacyinternational.org/survey/phr2002/

[129] Article 2 (d) of Directive 2002/58/EC.

[130] Recital 40 states, "Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient."

[131] Schreurs, W., M. Hildebrandt, E. Kindt and M. Vanfleteren, "*Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector", *op. cit*; Schreurs, W., "Spam en electronische reclame [Spam and electronic communication]", *Nieuw Juridisch Weekblad*, 2003-48, pp. 1174–1185.

5.3.8 Specific recommendation regarding liability law

5.3.8.1 General

Civil damages address a harm already done, and compensate for damages sustained. Effective civil liability rules might actually form one of the biggest incentives for all actors involved to adhere to the obligations envisaged by law. One could establish liability for breach of contract, or on the basis of general tort rules. To succeed in court, one has to prove the damage, the causal link and the fault. Liability can be established for any damages sustained, as far as the conditions of liability are proven and so long as liability is not excluded (as in the case of some situations in which intermediary service providers are involved[132]). However, in AmI, to establish such proof can be extremely difficult.

As we have seen in the dark scenarios, each action is very complex, with a multiplicity of actors involved, and intelligent agents acting for service providers often undertake the action or decision causing the damage. Who is then to blame? How easy will it be to establish causation in a case where the system itself generates the information and undertakes the actions? How will the individual deal with such problems? The individual who is able to obtain damages addressing his harm in an efficient and quick way will have the incentive to take an action against the infringer, thus raising the level of overall enforcement of the law. Such an effect would be desirable, especially since no state or any enforcement agency is actually capable of providing a sufficient level of control and/or enforcement of the legal rules.

The liability provisions of the Directive on electronic commerce can become problematic. The scope of the liability exceptions under the Directive is not clear. The Directive requires ISPs to take down the content if they obtain knowledge on the infringing character of the content (notice-and-take-down procedure). However, the lack of a "put-back" procedure (allowing content providers whose content has been wrongfully alleged as illegal, to re-publish it on the Internet) or the verification of take-down notices by third parties is said to possibly infringe freedom of speech.[133]

It is recommended that the liability rules be strengthened and that consideration be given to means that can facilitate their effectiveness.

---

[132] Articles 12 to 15 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), *Official Journal* L 178, 17 July 2000, pp. 1–16. The Directive provides for exceptions to the liability of intermediary service providers (ISPs) under certain conditions. In the case of hosting, for example, a service provider is not liable for the information stored at the request of a recipient of the service, on condition that (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. See also section 3.3.8.

[133] See Sutter, Gavin, "'Don't Shoot the Messenger?' The UK and Online Intermediary Liability", *International Review of Law Computers & Technology*, Vol. 17, No. 1, 2003, pp. 73–84; Julia-Barcelo, R., and K.J. Koelman, "Intermediary Liability in the E-commerce Directive: So far so Good, But It's not Enough", *Computer Law and Security Report*, Vol. 16, No. 4, 2000, pp. 231–239.

5.3.8.2 Liability for infringement of privacy law

In addition to the general considerations regarding liability presented in this section, we also draw attention to the specific problems of liability for infringement of privacy, including security infringements. Currently, the right to remedy in such circumstances is based on the general liability (tort) rules. The Data Protection Directive refers explicitly to liability issues stating that an immediate compensation mechanism shall be developed in case of liability for an automated decision based on inadequate profiles and refusal of access. However, it is not clear whether it could be understood as a departure from general rules and a strengthening of the liability regime. Determining the scope of liability for privacy breach and security infringements might also be problematic. In any case, the proof of the elements of a claim and meeting the general tort law preconditions (damage, causality and fault) can be very difficult.

Opacity instruments, as discussed above, aiming to prohibit the interference into one's privacy can help to provide some clarity as to the scope of the liability. In addition, guidelines and interpretations on liability would be generally welcome, as would standards for safety measures, to provide for greater clarity and thus greater legal certainty for both users and undertakings.

5.3.8.3 Joint and several liability

As already mentioned, it can be difficult for a user to identify the party actually responsible for damages, especially if he or she does not know which parties were actually involved in the service and/or software creation and delivery.

The user should be able to request compensation from the service provider with whom he or she had direct contact in the process of the service. Joint and several liability (with the right to redress) should be the default rule in the case of providers of AmI services, software, hardware or other products. The complexity of the actions and multiplicity of actors justify such a position.[134] Moreover, this recommendation should be supplemented by the consumer protection recommendation requiring the provision of consumer information by the service or product provider having the closest connection with the consumer, as well as the provision of information about individual privacy rights (see above) in a way that would enable the individual to detect a privacy infringement and have a better chance to prove it in court. There is a need to consider the liability regime with other provisions of law.

[134] The Directive on liability for defective products makes provision for joint and several liability. See also sections 3.2.8.3 and 5.3.8.4.

5.3.8.4 Strict liability

The Directive on liability for defective products[135] provides for a liability without fault (strict liability).[136] As a recital to the Directive states, strict liability shall be seen as "the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production." We should keep this reasoning in mind since it seems even more adequate when thinking about the liability issues in AmI.

Most of the "products" offered in the AmI environment will consist of software-based, highly personalised services. We should then think about adjusting the liability rules to such an environment. If it is difficult to distinguish between hardware and software from a technological perspective, why should we draw such a distinction from a legal perspective?[137] *An explicit provision providing for strict liability for software can be considered*.[138] Nevertheless, such a proposal is controversial as it is said to threaten industry. Since software is never defect-free, strict liability would expose software producers unfairly to claims against damages. Thus, the degree of required safety of the programmes is a policy decision.[139] Strict liability could also impede innovation, especially the innovation of experimental and life-saving applications.[140] Others argue that strict liability might increase software quality by making producers more diligent, especially, in properly testing their products.[141]

Despite these policy considerations, there are some legal questions about the applicability of strict liability to software. The first question is whether the software can be regarded as "goods" or "products" and whether they fall under the strict

[135] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *Official Journal* L 210, 07 August 1985, pp. 29–33.

[136] A strict product liability regime based on the Directive is the basis of the claims under the general tort regime. See Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, pp. 75–79. http://www.ejcl.org/64/art64-6.html

[137] Hilty, Lorenz, et al., *The Precautionary Principle in the Information Society, Effects of Pervasive Computing on Health and Environment*, Report of the Centre for Technology Assessment, February 2005, p. 269.

[138] In such a case, the intelligent software agent's failure and the PET's failure might be covered by the strict liability regime. Special derogation for PETs could be envisaged.

[139] Alheit, K., "The applicability of the EU Product Liability Directive to Software", *The Comparative and International Law Journal of South Africa*, Vol. 3, No. 2, 2001, p. 204.

[140] Singsangob, A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers, 2003, p. 113.

[141] Desai, M.S., J. Oghen and T.C. Richards, "Information Technology Litigation and Software Failure", *The Journal of Information, Law & Technology*, 2002 (2). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/desai/

liability regime.[142] In fact, the answer depends on national laws and how the Directive has been implemented. The Directive applies to products defined as movables,[143] which might suggest that it refers to tangible goods. Software not incorporated into a tangible medium (available online) will not satisfy such a definition. There are a growing number of devices (products) with embedded software (e.g., washing machines, microwaves, possibly RFIDs), which fall under the Directive's regime.[144] This trend will continue; the software will be increasingly crucial for the proper functioning of the products themselves, services and whole environments (smart car, smart home). Should the distinction between the two regimes remain?

Strict liability is limited to death or personal injury, or damage to property intended for private use.[145] The damage relating to the product itself, to the product used in the course of business and the economic loss will not be remedied under the Directive.[146] Currently, defective software is most likely to cause financial loss only, thus the injured party would not be able to rely on provisions of the Directive in seeking redress. However, even now in some life-saving applications, personal injury dangers can emerge. Such will also be the case in the AmI world (see, e.g., the first and second dark scenarios in which software failures cause accidents, property damage and personal injury) so the importance and applicability of the Directive on liability for defective products will grow. The increasing dependence on software applications in everyday life, the increasing danger of sustaining personal injury due to a software failure and, thus, the growing concerns of consumers justify strengthening the software liability regime.

However, the Directive allows for a state-of-the-art defence. Under this defence, a producer is not liable if the state of scientific and technical knowledge at the time the product was put into circulation was not such that the existence of the defect would be discovered. It has been argued that the availability of such a defence (Member States have the discretion whether to retain it in national laws[147]) will always be possible since, due to the complexity of "code", software will never be defect-free.[148]

These policy and legal arguments indicate the difficulty in broadening the scope of the Directive on liability for defective products to include software. Reversal of the burden of proof might be a more adequate alternative solution, one that policy-makers should investigate.

---

[142] Similar discussion takes place in the United States. It seems that, despite the fact that the issue is not clearly stated, there is a tendency to regard software as a good, especially if the parties to the contract intended to treat it as such (as opposed to an information service). See Singsangob A., *Computer Software and Information Licensing in Emerging Markets, The Need for a Viable Legal Framework*, Aspen Publishers, 2003, p. 113.

[143] Article 2 of the Directive.

[144] Reed, Ch., and A. Welterveden, "Liability", in Ch. Reed and J. Angel (eds.), *ComputerLaw*, London, 2000, p. 99.

[145] Article 9 of the Directive on liability for defective products.

[146] Giensen, I., and M.B.M. Loos, "Liability for Defective Products and Services: The Netherlands", *Netherlands Comparative Law Association*, 2002, p. 82. http://www.ejcl.org/64/art64-6.html

[147] Article 15 (1)(b) of the Directive on liability for defective products.

[148] Alheit, K., p. 204.

It is often difficult to distinguish software from hardware because both are necessary and interdependent to provide a certain functionality. Similarly, it may be difficult to draw the line between software and services. Transfer of information via electronic signals (e.g., downloaded software) could be regarded as a service.[149] Some courts might also be willing to distinguish between mass-market software and software produced as an individual product (on demand). AmI is a highly personalised environment where software-based services will surround the individual, thus the tendency to regard software as a service could increase.

Strict liability currently does not apply to services. Service liability is regulated by national laws.[150] Extending such provision to services may have far-reaching consequences, not only in the ICT field. The AmI environment will need the innovation and creativity of service providers; therefore, one should refrain from creating a framework discouraging them from taking risks. However, some procedural rules could help consumers without upsetting an equitable balance. The consumer, usually the weaker party in a conflict with the provider, often has difficulty proving damages. Reversing the burden of proof might facilitate such proof. Most national laws seem to provide a similar solution.[151]

Since national law regulates the issue of service liability, differences between national regulations might lead to differences in the level of protection. The lack of a coherent legal framework for service liability in Europe is regrettable. Learning from the differences and similarities between the different national legal regimes, as indicated in the Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services,[152] *is the first step in remedying such a situation.*

5.3.8.5 Reversing the burden of proof

Reversing the burden of proof is less invasive than the strict liability rules where the issue of fault is simply not taken into consideration. Such a solution has been adopted in the field of the non-discrimination and intellectual property laws, as well as in national tort regimes.[153] An exception to the general liability regime is also

---

[149] The OECD has treated software downloads as a service for the VAT and custom duties purposes. See Henderson, K., and A. Poulter, "The Distance Selling Directive: points for further revision", *International Review for Law Computers & Technology*, Vol. 16, No. 3, 2002, pp. 289–300.

[150] As a basis for liability, the contractual liability or the fault-based tort liability applies. See Giensen, I., and M.B.M. Loos, op. cit., as well as Magnus, U., and H.W. Micklitz, *Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services*: A study commissioned by the European Commission, Final Report, Part D: The Comparative Part, April 2004, p. 62. http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

[151] Magnus, U., and H.W. Micklitz, p. 8.

[152] Magnus, U., and H.W. Micklitz. http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportabc_en.pdf and http://europa.eu.int/comm/consumers/cons_safe/serv_safe/liability/reportd_en.pdf

[153] Magnus, U., and H.W. Micklitz.

provided in Directive 1999/93/EC on the community framework for electronic signatures.[154] In that Directive, the certification service provider is liable for damage caused by non-compliance with obligations imposed by the Directive[155] unless he proves he did not act negligently.[156]

Technology could potentially remedy the information asymmetry between users and AmI service suppliers or data processors. The latter could have an obligation to inform consumers what data are processed, how and when and what is the aim of such activities (thus actually fulfilling their obligations under the Data Protection Directive). This information could be stored and managed by an intelligent agent on behalf of the user, who is not able to deal with such information flow. However, the user would have the possibility to use such information to enforce his rights (e.g., to prove causation). Other technological solutions (e.g., watermarking) could also help the user prove his case in court.

5.3.8.6 Consumer claims and fixed damages

In many cases, the damage sustained by the individual will be difficult to assess in terms of the economic value or too small to actually provide an incentive to bring an action to court. However, acts causing such damage can have overall negative effects. Spam is a good example. *Fixed damages, similar to the ones used in the United States, or punitive damages could remedy such problems (some US state laws provide for fixed damages such as US$200 for each unsolicited communication without the victim needing to prove such damage). They would also provide clarity as to the sanctions or damages expected and could possibly have a deterrent effect*. The national laws of each Member State currently regulate availability of punitive damages; a few countries provide for punitive and exemplary damages in their tort systems.[157]

---

[154] On issues relating to digital signatures, see Gasson, M., M. Meints and K. Warwick (eds.), *A study on PKI and biometrics*, FIDIS (Future of Identity in the Information Society) Deliverable D3.2, July 2005. http://www.fidis.net. See also Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *Official Journal* L 013, 19 January 2000, pp. 0012–002. See also section 3.2.8.6.

[155] For example, the service provider is liable for the inaccuracy or incompleteness of the information contained in the certificate at the time the certificate was issued.

[156] The liability rules described above seem sufficient as a legal framework for qualified digital signatures. The general tort rules apply in relation to liability in all other cases (other than qualified signatures).

[157] There are not enough sources to state if they would apply in anti-spam cases. "Available sources" refers here to antitrust claims. Waelbroeck D., D. Slater and G. Even-Shoshan [Ashurst], *Study on the conditions of claims for damages in case of infringement of EC Competition rules*, commissioned by European Commission DG Competition, 2004, pp. 44–47. http://ec.europa.eu/comm/competition/antitrust/others/actions_for_damages/study.htm

Actions allowing consolidation of the small claims of individuals could be also examined (i.e., group consumer actions).

5.3.9 Specific recommendation regarding equality law

5.3.9.1 What is non-discrimination law?

Non-discrimination law can regulate and forbid the unlawful usage of processed data, for example, in making decisions or undertaking other actions on the basis of certain characteristics of the data subjects. This makes non-discrimination law of increasing importance for AmI. The *creation* of profiles does not fall under non-discrimination law[158] (potential use), but decisions based on profiling (including group profiling based on anonymous data) that affect the individual might provide the grounds for application of the non-discrimination rules. They apply in the case of identifiable individuals as well as to anonymous members of the group.[159]

Profiles or decisions based on certain criteria (health data, nationality, income, etc.) may lead to discrimination against individuals. It is difficult to determine when it is objectively justified to use such data and criteria, and when they are discriminatory (e.g., the processing of health-related data by insurance companies leading to decisions to raise premiums). Further legislative clarity would be desirable.

However, certain negative dimensions of profiling still escape the regime of non-discrimination law (e.g., manipulation of individuals' behaviour by targeted advertising). Here no remedies have been identified.

The non-discrimination rules should be read in conjunction with the fairness principle of data protection law. The application of the two may have similar aims and effects; they might also be complementary: Can the limitations of non-discrimination law be justified if they are regarded as not fair, as in the example of insurance companies raising premiums after processing health data? They can address a range of actions undertaken in AmI, such as dynamic pricing or refusal to provide services (e.g., a refusal of service on the grounds that no information (profile) is available could be regarded as discriminatory).

Non-discrimination rules should be taken into consideration at the design stage of technology and service development.

---

[158] However, such issues might be addressed by the data protection legislation. In the opinion of Gutwirth and De Hert, principles of data protection are appropriate to cope with profiling. Hildebrandt, M., and S. Gutwirth (eds.), *Implications of profiling practices on democracy and rule of law*, FIDIS Deliverable D7.4, September 2005. http://www.fidis.net/fidis_del.html

[159] Custers, B., *The Power of Knowledge, Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen, 2004, pp. 164–165.

5.3.9.2 Universal service

The Universal Service Directive[160] provides for a minimum of telecommunication services for all at an affordable price as determined by each Member State. Prices for universal services may depart from those resulting from market conditions.[161] Such provisions aim at overcoming a digital divide and allowing all to enjoy a certain minimum of electronic services. The Directive is definitely a good start in shaping the Information Society and the AmI environment. The development of new technologies and services generates costs, both on individuals and society. Many high-added-value AmI services will be designed for people who will be able to pay for them. Thus, AmI could reinforce the inequalities between the poor and rich. Everyone should be able to enjoy the benefits of AmI, at least at a minimum level. *The Commission should consider whether new emerging AmI services should be provided to all. Some services (e.g., emergency services) could even be regarded as public and provided free of charge or as part of social security schemes.*

5.3.10 Specific recommendations regarding interoperability and IPR

5.3.10.1 General

As shown in Scenario 2, AmI might cause major problems for current intellectual property protection, because AmI requires interoperability of devices, software, data and information, for example, for crucial information systems such as health monitoring systems used by travelling seniors. There is also a growing need to create means of intellectual property protection that respect privacy and allow for anonymous content viewing. Intellectual property rights give exclusive rights over databases consisting of personal data and profiles, while the data subjects do not have a property right over their own information collected. We discuss these issues below.

5.3.10.2 Protection of databases and profiling

The Directive on the legal protection of databases[162] provides for a copyright protection of databases, if they constitute the author's own intellectual creation by

---

[160] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), *Official Journal* L 108, 24 April 2002, pp. 0051–0077.

[161] For more on the Directive, see section 3.3.8.2.

[162] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077, 27 March 1996, pp. 0020–0028.

virtue of his selection or arrangement of their content. The Directive also foresees a *sui generis* protection if there has been a qualitatively and/or quantitatively substantial investment in either the acquisition, verification or presentation of the content. *Sui generis* protection "prevents the extraction and/or the re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database".[163] This implies that the database maker can obtain a *sui generis* protection of a database even when its content consists of personal data. Although the user does not have a property right over his personal data, the maker of a database can obtain an exclusive right over this type of data. Hence, a profile built on the personal data of a data subject might constitute somebody else's intellectual property.

The right to information about what knowledge has been derived from one's data could, to some extent, provide a safeguard against profiling. We recommend that further research be undertaken on how to reconcile this with intellectual property rights.[164]

5.3.10.3 DRMs

The Copyright Directive[165] provides for the protection of digital rights management (DRMs) used to manage the licence rights of works that are accessed after identification or authentication of a user.[166] But DRMs can violate privacy, because they can be used for processing of personal data and constructing (group) profiles, which might conflict with data protection law.

Less invasive ways of reconciling intellectual property rights with privacy should be considered.

This not only relates to technologies but also to an estimation of the factual economic position of the customer. For example, the general terms and conditions for subscribing to an interactive television service – often a service offered by just a few players – should not impose on customers a condition that personal data relating to their viewing behaviour can be processed and used for direct marketing or for transfer to "affiliated" third parties.

As the Article 29 Working Party advises, greater attention should be devoted to the use of PETs within DRM systems.[167] In particular, it advises that tools be used to

[163] Article 7 (1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. http://europa.eu.int/ISPO/infosoc/legreg/docs/969ec.html

[164] See section 5.3.4 on the right to information.

[165] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal* L 167, 22 June 2001, pp. 0010–0019.

[166] See also section 5.3.5, Specific recommendation regarding security.

[167] Article 29 Data Protection Working Party, *Working document on data protection issues related to intellectual property rights* (WP/ 104), adopted on 18 January 2005. http://ec.europa.eu/justice_home/fsj/privacy

preserve the anonymity of users and it recommends the limited use of unique identifiers. Use of unique identifiers allows profiling and tagging of a document linked to an individual, enabling tracking for copyright abuses. Such tagging should not be used unless necessary for performance of the service or unless with the informed consent of individual. All relevant information required under data protection legislation should be provided to users, including categories of collected information, the purpose of collecting and information about the rights of the data subject.[168]

The Directive on the legal protection of software[169] obliges Member States to provide appropriate remedies against a person's committing any act of putting into circulation or the possession for commercial purposes of any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program. *The Software Directive only protects against the putting into circulation of such devices and not against the act of circumventing as such. It would be advisable to have a uniform solution in that respect. DRMs can also violate consumer rights, by preventing the lawful enjoyment of the purchased product. The anti-circumvention provisions should be then coupled with better enforcement of consumer protection provisions regarding information disclosure to the consumer.*[170] *The consumer should always be aware of any technological measures used to protect the content he wishes to purchase, and restrictions in use of such content as a consequence of technological protection (he should also be informed about technological consequences of DRMs for his devices, if any, e.g., about installing the software on his computer).*[171] *Product warnings and consumer notifications should always be in place and should aim to raise general consumer awareness about the DRMs.*

5.3.10.4 Decompilation right

As interoperability is a precondition for AmI, AmI would have to lead to limitations on exclusive intellectual property rights. One could argue that software packages should be developed so that they are interoperable with each other. That implies creating standards. ICT global standards are desirable for interoperability and

---

[168] Ibid.

[169] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122, 17 May 1991, pp. 0042–0046.

[170] See also OECD, *Report on Disclosure Issues Related to the Use of Copy Control and Digital Rights Management Technologies*, DSTI/CP(2005)15/FINAL, 2006. https://www.oecd.org/dataoecd/47/31/36546422.pdf. For comments on consumer needs re DRM, see also INDICARE Project, "Content Providers' Guide to Digital Rights Management: Any side effects in using DRM?". www.indicare.org

[171] Those restrictions might, inter alia, prevent the user from making backups or private copies, downloading music to portable devices, playing music on certain devices, or constitute the geographical restrictions such as regional coding of DVDs.

privacy protection. A broader scope of the decompilation right under software protection would be desirable.

The EC's battle with Microsoft was in part an attempt to strengthen the decompilation right with the support of competition law.

5.3.11 Specific recommendations regarding international co-operation

5.3.11.1 Jurisdiction in criminal matters

Currently, there is no international or European framework determining jurisdiction in criminal matters, thus, national rules are applicable. The main characteristics of the legal provisions in this matter have already been discussed in Chapter 3, section 3.3.8.1; however, it seems useful to refer here to some of our earlier conclusions. The analysis of the connecting factors for forum selection (where a case is to be heard) shows that it is almost always possible for a judge to declare himself competent to hear a case. Certain guidelines have already been developed, both in the context of the Cybercrime Convention[172] as well as the 2005 EU Framework Decision on attacks against information systems[173] on how to resolve the issue of concurrent competences. According to the Cybercrime Convention, "The Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[174]

The 2005 EU Framework Decision on attacks against information systems states, "Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall co-operate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralizing proceedings in a single Member State."[175]

Legal experts and academics should follow any future developments in application of those rules that might indicate whether more straightforward rules are needed. The discussion on the Green Paper on double jeopardy should also be closely followed.[176]

---

[172] Council of Europe, Cybercrime Convention of 23 November 2001.

[173] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal* L 069, 16 March 2005, pp. 67–71.

[174] Article 22 paragraph 5 of the Cybercrime Convention.

[175] Article 10 paragraph 5 of the 2005 EU Framework Decision on attacks against information systems raises the possibility of invoking any institutional mechanism to facilitate such co-operation, and factors that should be taken into account when considering an appropriate forum.

[176] European Commission, Green Paper on Conflicts of Jurisdiction and the Principle of *ne bis in idem* in Criminal Proceedings, COM(2005) 696, December 2005.http://ec.europa.eu/comm/off/green/index_en.htm

5.3.11.2 Private international law

Scenario 2 ("A crash in AmI space") turns on an accident involving German tourists in Italy, while travelling with a tourist company established in a third country.[177] It raises questions about how AmI might fit into a legal framework based on territorial concepts. Clear rules determining the law applicable between the parties are an important guarantee of legal certainty.

Private international law issues are dealt at the European level by the Rome Convention on the law applicable to contractual obligations[178] as well as the Rome II Regulation on the law applicable to non-contractual obligations,[179] the Brussels Regulation on jurisdiction and enforcement of judgments.[180]

5.3.11.3 Jurisdiction in civil matters

The Regulation on jurisdiction and enforcement of judgments in civil and commercial matters covers both contractual and non-contractual matters. It also contains specific provisions for jurisdiction over consumer contracts, which aim to protect the consumer in case of court disputes.[181] These provisions should be satisfactory and workable in an AmI environment.

However, provisions of this Regulation will not determine the forum if the defendant is domiciled outside the European Union.[182] Also, the provisions on the jurisdiction for consumer contracts apply only when both parties are domiciled in EU Member States. Although the Regulation provides for a forum if the dispute arises from an operation of a branch, agency or other establishment of the defendant in a Member State, a substantial number of businesses offering services to EU

[177] See also Chapter 3 section 3.3.1 (the scenario script) and section 3.3.8.1 on the legal analysis of private international law aspects of the scenario.

[178] Convention of Rome on the law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC), *Official Journal L* 266, 9 October 1980, pp. 0001–0019 (Consolidated version CF498Y0126(03)).

[179] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). *Official Journal* L 199, 31 July 2007, pp. 40–49.

[180] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *Official Journal L* 012, 16 January 2001, pp. 0001–0023.

[181] Consumer contracts are regulated by Articles 15–17 of the Brussels Regulation. The consumer may bring a case in the court of the company domicile or in his own domicile. On the other hand, consumers may be sued only in a court of their own domicile. Such rules aim to protect the consumer who is the weaker party in a contractual relationship.

[182] Article 4 of the Brussels Regulation states: 1. If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Articles 22 and 23, be determined by the law of that Member State; 2. Any person domiciled in a Member State may, whatever his nationality, avail himself of the rules of jurisdiction in force in that State, and in particular those specified in Annex I, in the same way as the nationals of that State.

consumers will still be outside the reach of this Regulation. *This emphasises again the need for a more global approach*[183] *beyond the territory of the Member States.*

Clarification and simplification of forum selection for non-consumers would also be desirable. The complexity of the business environment, service and product creation and delivery would justify such approach. It would be of special importance for SMEs.

5.3.11.4 Applicable law

Currently, the applicable law for contractual obligations is determined by the 1980 Rome Convention.[184] Efforts have been undertaken to modernise the Rome Convention and replace it with a Community instrument. Recently, the Commission has presented a proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations.[185]

The provisions of the Rome Convention refer to contractual issues only. Recently, the so-called Rome II Regulation[186] has been adopted, which provides for rules applicable to non-contractual obligations.

The Rome Convention on law applicable to contractual obligations relies heavily on the territorial criterion. It refers to the habitual residence, the central administration or place of business as the key factors determining the national law most relevant to the case.[187] But IT services can be supplied at a distance by electronic means. The AmI service supplier could have his habitual residence or central administration anywhere in the world and he could choose his place of residence (central administration) according to how beneficial is the national law of a given country. The habitual residence factor has been kept and strengthened in the Commission's proposal for a new regulation replacing the Rome Convention (Rome I proposal, Article 4).[188]

---

[183] Ofcom, the UK regulator for communications, has made a similar point: "The global reach and open nature of the internet gives rise to some well-known problems, which cannot be addressed by a translation of existing powers and structures." *Online protection: A survey of consumer, industry and regulatory mechanisms and systems*, 21 June 2006, p. 1. http://www.ofcom.org.uk/research/technology/onlineprotection/report.pdf

[184] Convention of Rome on the law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC), *Official Journal* L 266, 9 October 1980, pp. 0001–0019.

[185] The Commission has presented the proposal for a regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I), COM (2005) 650 final, 2005/0261 (COD).

[186] Regulation (EC) No 864/2007

[187] According to Article 4, "the contract shall be governed by the law of the country with which it is most closely connected." Article 4 further reads: "It shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporated, its central administration. However, if the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or, where under the terms of the contract the performance is to be effected through a place of business other than the principal place of business, the country in which that other place of business is situated."

[188] The new proposal does not use the presumption that the country of habitual residence is the most closely connected with the case, as it is under the Rome Convention. In the proposal, the relevant factor of the habitual residence of, inter alia, the seller or service provider is the fixed rule.

The new proposal for the Rome I Regulation amends the consumer protection provisions.[189] It still relies on the *habitual residence* of the consumer, but it brings the consumer choice of contract law in line with the equivalent provisions of the Brussels Regulation, and broadens the scope of the application of its provisions. The Commission proposal for the Regulation on the law applicable to contractual obligations is a good step forward.

The Rome II Regulation on law applicable to non-contractual obligations applies to the tort or delict, including claims arising out of strict liability. The basic rule under the Regulation is that a law applicable should be determined on the basis of where the direct damage occurred (*lex loci damni*). However, some "escape clauses" are foreseen and provide for a more adequate solution if more appropriate in the case at hand. This allows for flexibility in choosing the best solution. Special rules are also foreseen in the case of some specific torts or delicts.

Uniform rules on applicable law at the European level are an important factor for improving the predictability of litigation, and thus legal certainty. In that respect, the new Regulation should be welcomed. The Regulation will apply from January 2009.

Some other legislative acts also contain rules on applicable law. Most important are provisions in the Data Protection Directive. This Directive also chooses the territorial criterion to determine the national law applicable to the processing of data, which is the law of the place where the processing is carried out in the context of an establishment of the data controller. Such a criterion, however, might be problematic: more than one national law might be applicable.[190] Moreover, in times of globalisation of economic activity, it is easy for an undertaking to choose the place of establishment, which offers the most liberal regime, beyond the reach of European data protection law. In situations when a non-EU state is involved, the Directive points out a different relevant factor, the location of the equipment used,[191] thus enabling broader application of the EU Data Protection Directive.[192]

---

[189] As recital 10 of the proposal states, these amendments aim to take into account the developments in distance selling, thus including ICT developments.

[190] Article 4 (1) of the Directive stipulates: Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

[191] The Directive stipulates in article 4 (1) that the national law of a given Member State will apply when the controller is not established on Community territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

[192] The Article 29 Data Protection Working Party interprets the term "equipment" as referring to all kinds of tools or devices, including personal computers, which can be used for many kinds of processing operations. The definition could be extended to all devices with a capacity to collect data, including sensors, implants and maybe RFIDs. (Active RFID chips can also *collect* information. They are expensive compared to passive RFID chips but they are already part of the real world.) See Article 29 Data Protection Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites* (5035/01/EN/Final WP 56), 30 May 2002. http://ec.europa.eu/justice_home/ fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

As we see, in all these cases, the territorial criterion (establishment) prevails. *We should consider moving towards a more personal criterion, especially since personal data are linked with an identity and a state of the data subject (issues which are regulated by the national law of the person). Such a criterion could be more easily reconciled with the AmI world of high mobility and without physical borders*. The data subject will also be able to remain under the protection of his/her national law, and the data controller/service provider will not have the possibility of selecting a place of establishment granting him the most liberal treatment of law.[193]

5.3.11.5 Data transfer

Data transfer is another issue highlighting the need for international co-operation in the creation of a common playing field for AmI at the global level. What is the sense of protecting data in one country if they are transferred to a country not affording comparable (or any) safeguards? Also, the globalisation of economic and other activities brings the necessity of exchanging personal data between the countries. The Data Protection Directive provides a set of rules on data transfer to third countries.[194] Data can be transferred only to countries offering an adequate level of protection. The Commission can conclude agreements (e.g., the Safe Harbour Agreement) with third countries which could help ensure an adequate level of protection. The Commission can also issue a decision in that respect. However, the major problem is enforcement of such rules, especially in view of the fact that some "safeguards" rely on self-regulatory systems whereby companies merely promise not to violate their declared privacy policies (as is the case with the Safe Harbour Agreement*). Attention by the media and consumer organisations can help in the enforcement of agreed rules. The problem of weak enforcement also emphasises the need to strengthen international co-operation with the aim of developing new enforcement mechanisms. Providing assistance in good practices in countries with less experience than the European Union would also be useful*.

[193] Such a solution has the advantage of covering, with the protection of EU legislation, third country residents whose data are processed via equipment in the EU. A broad interpretation of the term "equipment" would help guarantee the relatively broad application of such a rule (see above). As a result, in most cases, application of the domicile/nationality rule or the place of the equipment used as the relevant factor would have the same result. However, we can envisage the processing of data not using such equipment, for example, when the data are already posted online. Then the EU law could not be applicable.

[194] See chapter 3, section 3.4.8.1.