Chapter 3
Dark scenarios

In this chapter, we present four "dark scenarios" that highlight the key socio-economic, legal, technological and ethical risks to privacy, identity, trust, security and inclusiveness posed by new AmI technologies. We call them dark scenarios, because they show things that could go wrong in an AmI world, because they present visions of the future that we do *not* want to become reality. The scenarios expose threats and vulnerabilities as a way to inform policy-makers and planners about issues they need to take into account in developing new policies or updating existing legislation.

Before presenting the four scenarios and our analysis of each, we describe the process of how we created the scenarios as well as the elements in our methodology for analysing the scenarios.

3.1 Creating and analysing dark scenarios

The process we followed in constructing the four dark scenarios is depicted in Fig. 3.1.

As indicated in Fig. 3.1, we made an extensive review of existing AmI-related projects, studies and scenarios, with a view to understanding their implications in terms of the key issues. While most existing scenarios describe the brave new world of AmI, how great it will be living and working in an AmI-enabled future, we often found that the technological marvels had some negative aspects to which little attention had been given.

Following a workshop with other AmI experts to discuss the most important threats and vulnerabilities posed by AmI, we had our own internal workshop where we brainstormed until we agreed the rough outlines of four contrasting scenarios. We then developed these outlines into scenario stories or scripts. To ground our scenarios in reality – to ensure that they were not too far-fetched – we did a "technology check" (are the technologies referenced in the scenarios probable?) and a "reality check" (are there press reports of events similar to those mentioned in the scenarios?). Then, all of the partners reviewed all of the scenarios in order to eliminate doubtful points, unnecessary wordage, irrelevancies, etc., and to sharpen them

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

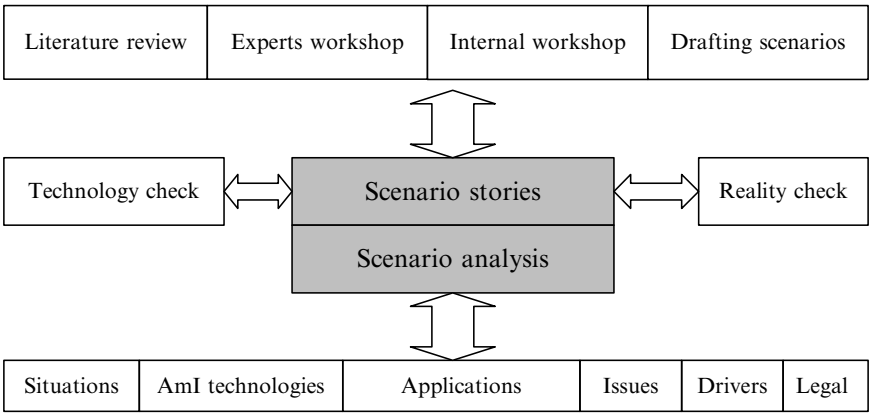

Fig. 3.1 The process of constructing the four dark scenarios

to illustrate the points we wanted to emphasise. Once the scenarios were "stable", we performed our analysis of them, including a legal analysis. We presented the scenarios and our analyses at a second workshop in order to benefit from the comments of other experts.

We devised a methodology, an analytical structure for both constructing and deconstructing scenarios, not only our own scenarios, but many other technology-oriented scenarios. Our analytical structure comprises the following elements or activities:

3.1.1 Framing the scenario

This first step summarises the scenario in question and explains its context – who are the main actors in the scenario, what happens to them or what do they do, how far into the future is the scenario set, where does it take place and in what domain (home, office, on the move, shopping, etc). It identifies the type of scenario (trend, normative and explorative) and key assumptions (e.g., intelligent technologies will be embedded everywhere in rich countries, but not in poor countries).

3.1.2 Identifying the technologies and/or devices

Next, we identify the most important AmI technologies and/or devices used and/or implied in the scenarios.

3.1.3 Identifying the applications

We consider the applications that emerge in each scenario and that are supported by the technologies mentioned in the previous step.

3.1.4 Drivers

At this step in the analysis, we identify the key drivers that impel the scenario or, more particularly, the development and use of the applications. Drivers are typically socio-economic, political or environmental forces (e.g., in our third scenario, the Data Mining Corporation seeks a global monopoly, economic disparities are inflaming poor countries, the world is becoming a hothouse) or personal motivations (e.g., greed).

3.1.5 Issues

Next, we identify and explicate the major issues raised in each scenario. The issues of concern, as mentioned above, are privacy, identity, trust, security and inclusiveness (or its opposite, the digital divide). A discussion of the issues considers the threats and vulnerabilities exposed by the scenario.

3.1.6 Legal synopsis

We present the legal and regulatory issues, especially in the context of today's legislation, and point out lacunae in today's legal framework and how those lacunae need to addressed to deal with issues that will be prevalent in an AmI future.

3.1.7 Conclusions

The final step is a reality check of the scenario itself (how likely is it? are the technologies plausible?) and a consideration of what should be done to address the issues it raises. One might conclude that a range of socio-economic, technological and legal safeguards are needed in order to minimise the risks posed by the threats and vulnerabilities highlighted by the scenario.

3.2 Scenario 1: The AmI family

3.2.1 The scenario script

Scene 1: At home and at work

The Sebastianis are a middle-class family who make intensive use of their smart AmI home. Both parents work full time but with flexible hours. The father (Paul)

mainly works from home for a private security company. His work concerns remote surveillance of company premises. His wife Maruja works for a real estate company in the city. They have two teenage children (Ricardo and Elena).

Paul has been called out for a meeting at the security company. Such meetings where security agents have face-to-face contacts are organised only occasionally. Although he likes working from home, Paul also enjoys actually meeting the colleagues with whom he collaborates on a daily basis.

He forgot to close the door of his highly protected study when he left the house. Usually, this is not a problem. The room knows when Paul leaves because embedded sensors in the room detect inactivity. Unfortunately, the door with its fingerprint reader did not close automatically because a carpet was displaced and folded accidentally. It prevented the door from closing.

Paul receives an alarm signal on his Personal Wrist Communicator (PWC). There is an intruder in the house. "How is that possible?" he asks himself. He knows that his son Ricardo is home. He had invited some friends to play a new virtual reality game (for which Ricardo has a licence) from the entertainment centre downstairs. Paul checks the home surveillance system remotely but only gets a still image from 30 minutes ago. There is no live image available from the front and back door cameras, nor is Paul able to play back who has passed in front of the doors today. Ricardo does not answer his calls. "What's happening? Where is he?"

Paul contacts the neighbourhood security service and asks them to check visually on his house and children. From the outside, nothing seems to be wrong except that all curtains and windows are closed. Moreover, it seems that all security systems are blocked and the security agents on the spot cannot get access to the security surveillance logs. Paul is informed of the situation and decides to call the police. In the past, AmI security systems alarmed the police automatically but because of too many false alarms, this procedure has been stopped.

Paul is just leaving the office to return home when his boss calls, "Come in, Paul. I'm glad you are still at the office. It seems we have a small problem. … I've just been contacted by the police who have asked for access to all the data we have on you. I understand this is just an informal request so we do not have to give them anything, but, as you know, as a security company, we cannot afford any suspicions of our staff."

Paul is astonished and does not understand what is happening. First the home problem, now this. "Surely, this must be some kind of mistake. I don't know why they'd want my data – although I have heard lately of cases where the police have been investigating innocent people based on inadequate profiling."[1]

"Yes, I know, Paul," she says. "And I trust you, but you must understand that under such circumstances, I can't go to the board of directors meeting tomorrow with a proposal for your promotion at a time when you are being investigated by the police. I'm sorry, but we'll just have to wait until this situation is clarified."

[1] Singel, Ryan, "Nun Terrorized by Terror Watch", *Wired News*, 26 September 2005. http://www.wired.com/news/privacy/0,1848,68973,00.html

"Okay, sure, I understand," Paul replies. He is disappointed to miss a promotion now, but he is confident that the opportunity will come around again. "I really don't know what the police could be after, but, of course, the best thing to do is to co-operate and let's clear up this misunderstanding." This is what he says, but what he thinks is "This is not my best day, but first I need to find out what's happening at home."

Paul receives multiple messages on his PWC the moment he leaves his boss's office.[2] *He had all incoming communications on hold from the moment he entered her office. This is a company default setting. There is one message that immediately attracts his attention. "If you want your house systems to work again, click on the following link …"*

"What? I'm being blackmailed! So that's why I couldn't get access to my home systems, nor could the local security agent. That's why I got the intruder message," he thinks, slightly reassured, since that probably means that his children at home are OK.

Ricardo is indeed enjoying himself with his friends in Paul's study. They were able to enter because the door was still open. At last, he has the opportunity to check whether the print-out he has of his father's iris can fool the iris scanner which it must do if Ricardo is to unlock his father's computer. It does because Paul still has an old-fashioned model without liveness testing![3] *With his father's profile and identity, Ricardo can circumvent the parental control system that governs use of the Internet by all terminals in the home. It's time for some fun. Ricardo places a bet on a sports gambling site, downloads some xxx-rated movies and games on his personal space on the family server and checks out his father's online favourites.*[4] *"Hmmm, I didn't know the old man likes erotic poetry. And I see he's just bought some pretty pricey lingerie. … Well, I hope it's for mum," Ricardo laughs. But he won't be laughing when his father finds out that Ricardo has spent 200 euros from his account.*

While one of his friends goes to the entertainment room to start a multiplayer virtual reality game, Ricardo goes to the kitchen to prepare some gin and tonics. The cupboard containing the alcohol can only be opened by a numerical code, but Ricardo figured that out long ago. The code is the date of his parents' wedding anniversary.[5]

---

[2] Alahuhta, P., M. Jurvansuu and H. Pentikäinen, "Roadmap for network technologies and service", *Tekes Technology Review* 162/2004, Tekes, Helsinki, 2004.

[3] Daugman, John, "Iris Recognition: Anti-spoofing Liveness Testing, Stable Biometric Keys, and Further Research Directions", BioSecure 1st Residential Workshop, Paris, August 2005; Maghiros, I., Y. Punie, S. Delaitre, et al., *Biometrics at the Frontiers: Assessing the Impact on Society*, Study commissioned by the LIBE Committee of the European Parliament, EC – DG Joint Research Centre, Institute for Prospective Technological Studies (IPTS), Seville, 2005.

[4] A recent study indicates that spyware risks are highest for broadband users and for those who visit pornographic sites or play games online: http://news.bbc.co.uk/1/hi/technology/4659145.stm

[5] Not everything in the smart house is accessed via biometric verification. But then, the human tendency to use easy-to-guess passwords and/or access codes continues to constitute a possible security weakness. For more on the security weakness of passwords, see Schneier, B., "Customers, Passwords, and Web Sites", in *IEEE Security and Privacy Magazine*, 2, No. 5, 2004.

Scene 2: Shopping while being at work

Across town, Paul's wife Maruja needs to find a funny (farewell to girlhood!) present for her best friend. Because she is busy at work, she decides to try her new Shopping Assistant Software (SAS), which, according to the hype, is supposed to have intelligent search capabilities and an advanced speech interface.[6] *But Maruja is not impressed. The SAS's suggestions seem too ordinary, so she instructs the SAS to keep searching "until you find something really funny".*[7] *On her way back to the office, Maruja notices that she has received a message from her daughter Elena on her Personal Wrist Communicator (PWC) for a special offer on the new "Real Magic Experience" (RME) she wants for her next birthday. Elena knows her mother would never buy her such an expensive game but with in view of a really good online offer, she might. The snag is that the offer is only valid for one hour. What Maruja does not know is that this new version of RME will allow Elena to play it at school without the teacher's noticing it.*

Neither Maruja nor Elena is aware that the web site with the attractive offer contains a powerful spyware program that looks for personal data and preferences, so that users can be targeted with personalised advertising. The spyware helps to reveal a person's attitude towards privacy and spam.[8] *Companies are paying a lot of money for personal and group profiles.*[9] *This phenomenon is known as "data laundering". Similar to money laundering, data laundering aims to make illegally obtained personal data look as if they were obtained legally, so that they can be used to target customers.*

Maruja receives the message from her daughter just before a business meeting starts. She looks at the message in a hurry and, attracted by the discount price, she buys the game. Turning her thoughts to the meeting, she is confident she will be able to convince her prospective client, a construction company, to invest in the land held by her company. If she's right, she expects a big annual bonus.

While giving her presentation, Maruja receives, much to her surprise, because she thought she had banned incoming messages, a "Most Funny Wedding Present" advertisement. She accidentally activates the message and displays it on the big screen. It shows an ad for a sex-related product. Flustered and embarrassed,

---

[6] Garate, A., I. Lucas, N. Herrasti and A. Lopez, "Ambient Intelligence Technologies for Home Automation and Entertainment", in EUSAI 2004, Workshop "Ambient Intelligence Technologies for Well-Being at Home", 2004.

[7] Dey, A., and J. Mankoff, "Designing Mediation for Context-Aware Applications", *ACM Transactions on Computer-Human Interaction*, Special issue on Sensing-Based Interactions 12(80), Issue 1, March 2005, pp. 53–80.

[8] Krebs, Brian, "Hacked Home PCs Fueling Rapid Growth in Online Fraud", *Washington Post*, 19 September 2005. http://www.washingtonpost.com/wp – dyn/content/article/2005/09/19/AR2005091900026.html

[9] Vijayan, Jaikumar, "ID Theft Continues to Increase. More than 13 million Americans have been victimized, new study reveals", *Computerworld*, 30 July 2003. http://www.pcworld.com/news/article/0,aid,111832,00.asp; Zetter, Kim, "TSA Data Dump Leads to Lawsuit", *Wired News*, 14 July 2005. http://www.wired.com/news/privacy/0,1848,68560,00.html

Maruja apologises and continues with her presentation, but she never really gets back on track after that.

An audio track of the meeting is recorded and converted to a document, as is normal practice in Maruja's company (thanks to AmI, nobody needs to write and distribute "meeting minutes" anymore!). Next day, Maruja's boss, surprised by the partners' decision to postpone financing of a joint project, checks the meeting report and gets the impression that Maruja did not prepare her presentation well enough. She will probably not get the annual bonus she was counting on. The reason for Maruja's embarrassment was not recorded to the "meeting minutes" since it was a video message, not an audio advertisement.

Scene 3: In the park

After the terrible business meeting experience she has had, Maruja leaves the office for a lunch break. She decides to buy a takeaway sandwich and walks towards the park. She is receiving almost continuously messages on the flexible screen on her sleeve.[10] *She likes the blouse she borrowed from her friend to test the on-screen possibilities of this smart piece of clothing. The screen shows there is a tai-chi gathering on the east side of the park. She might want to join because of her interest in relaxation exercises and in Eastern philosophies.*

"Not today," she thinks, "and I am certainly not having lunch in the Chinese restaurant around the corner, despite its interesting price. I do not like Chinese food. My avatar should know that and I already have a sandwich. … Damn, I should have indicated that I already had lunch. You have to think of everything here." The avatar could not know that she already has a sandwich, because she paid cash for it.

Another ad appears: "Special offers from the bookshop next door." Maruja gets annoyed by the location-based spam[11] *and decides to switch off almost completely, only allowing incoming emergency messages.*

Later, she finds out that her boss has phoned twice. She also misses a proximity message that a good friend was sitting in a nearby pub. She feels deprived and angry because it is so difficult to get the thresholds of her avatar right. It seems there will always be grey zones where intelligent agents are not able to take the most intelligent filtering decisions. "I should have been more open to the physical environment," she thinks, because then she would probably have noticed that she had passed one of her friend's favourite bars.

Maruja thinks about her friend Claire who is always fast in adopting new electronic gadgets such as this blouse. Maruja likes it. It seems really practical.

Claire, however, at that moment, is having a rather bad experience. She is working at home when burglars break into her apartment. The burglars are surprised to

---

[10] Espiner, T., "Philips unfurls prototype flexible display", ZDNet UK, 2 September 2005. http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

[11] Paciga, M., and H. Lutfiya, "Herecast: An open infrastructure for location – based services using WiFi, Wireless and Mobile Computing, Networking and Communications", WiMob'2005, IEEE International Conference, 2005, pp. 21–28.

find Claire at home. In the ensuing confrontation, Claire is punched in the face. The burglars get away with only her PWC, her wallet and some jewels that were lying on the table but the experience of getting robbed will haunt Claire for a much longer time. Moreover, she will now have to train her new PWC from scratch because she did not want to store her profile online, and because the burglars have destroyed her home computer which Claire had used to back up her PWC.

The burglary and mugging occurred because of an unlucky coincidence of circumstances, i.e., Maruja was wearing Claire's blouse when she went to the park where the criminal gang happened to be operating. As she was passing by, the gang "read" the RFID tag embedded in the blouse. As a result, the gang found out that the blouse had been sold at a certain shop. The gang hacked the client database to discover Claire's profile (a well-off woman living alone in the richer part of the city).[12] On the assumption that Claire was wearing the blouse, the criminals decided to break into the flat and to steal whatever luxury goods they could find.

After passing by the gang, Maruja is stopped by a young foreign woman. "Excuse me," she asks. "I want to go to the town hall in the central market square. Can you tell me which exit from the park to take?"

"Sure, let's look it up." Maruja clicks on the city map that locates their position and in the blink of an eye, they find that is the right exit on the upper-east side. "Thank you," the young woman replies and walks on.

Maruja wonders why this woman does not have her own location device. She would feel completely lost without hers.

The location device is not perfect, as Maruja knows from her experience last week when some thugs forced her to hand over her "smart" purse which did not require any authentication in order to make small payments. Maruja had forgotten to authorise an update of the location-based software and found herself walking in an area of the city frequented by drug addicts and criminals. Because there are so many surveillance cameras everywhere these days, criminal gangs and other bad sorts now move quickly from one area to another, taking advantage of the fact that the security information system only gets updated once a month and that only subscribers receive these updates.

3.2.2 Analysis

3.2.3 The context

Scenario 1 presents three different environments to depict AmI-related privacy and security weaknesses: at home, at work and in an open public space. There are differences between these environments but the distinction between them is blurring. Already today,

[12] Knospe, H., and H. Pohl, "RFID Security", *Information Security Technical Report* 9, No. 4, 2004, pp. 30–41.

ICTs enable work to be brought home and contact with the home at work. This trend will continue with AmI, although it can lead to some problems as shown in the scenario.

Scene 1: At home and at work

Although many people could be teleworking in the future, the scenario shows that face-to-face contacts are still important. Ricardo is able to make use of his father's absence to enter the study before the smart room door closes. Paul's employer has imposed certain security measures to enable Paul to work at home. One of these is the fingerprint scan needed to open the study door. Another is the biometric protection via iris recognition but Ricardo is able to spoof that with a picture of Paul's iris because iris scanners are inexpensive. Ricardo is able to use his father's identity to bypass the parental control system and to shop online. Another security weakness is the easy-to-guess passwords or codes. The scenario also shows that different security systems are used for different purposes.

Later, at work, Paul receives alarming information that something is wrong at home, but he does not know what. This obviously creates a feeling of loss of control. He soon finds out that he is being digitally blackmailed (a new crime, or rather an existing crime in new clothes). Then, Paul meets his boss following an informal police check caused by inadequate profiling. The search for all digital information on Paul highlights a disproportionate reaction to a suspicion based on an inaccurate profile.

Scene 2: Shopping at work

Scene two tells the story of Maruja's preparing for a business meeting while communicating with her daughter and with Shopping Assistant Software (SAS). It provides examples of AmI vulnerabilities within a commercial context. In the first instance, the SAS does not find a suitable gift. In the second instance, it misinterprets the notion of funny in relation to a farewell present for a girlhood friend and gives sex-related suggestions. These suggestions would normally only be visible on Maruja's PWC, but she accidentally projects them on the big screen during her business meeting. Not only is this embarrassing but also it leads to Maruja's losing a client and, consequently, an end-of-year bonus. The complexity of the technology in relation to the value the user gets from using it is in question here.

More vulnerabilities pop up when Maruja accepts a special offer, suggested by her daughter, to buy a computer game. Because they didn't have the time to check out the web site properly, Maruja is afflicted by powerful spyware that captures her personal data without her knowing about it. That was exactly the purpose of the special offer on the computer game. It is a manifestation of a new crime called data laundering.

Another issue is related to control as shown in the situation where children seek to circumvent parental and teacher control over playing computer games at school and the work situation where staff are "controlled" during business meetings to the extent that what is said is automatically recorded. The latter instance, however, can result in a decision taken on the basis of incomplete information, i.e., information that is not recorded.

Scene 3: At the park

Scene three starts with Maruja's going to a park for her lunch break to disconnect from her disastrous business meeting. Unfortunately, she gets spammed continuously with

location-based advertising as a result of a misinterpretation of her personal profile. The avatar makes mistakes (Chinese food), is not informed (sandwich lunch) or gets influenced (low price restaurant). It shows that people can be irritated and annoyed by certain AmI applications. Maruja decides to switch off temporarily but later she regrets having missed a call from her boss and not being aware of the nearby presence of a friend.

Her friend Claire goes through a much worse situation because she is robbed while working in her apartment. The high-tech criminals did not expect her to be at home. By reading the RFID tags on Claire's blouse and by hacking[13] the client database of the shop that sold the blouse, they were able to determine the location of her apartment. The criminals did not know that Maruja, not Claire, was wearing the blouse. Claire not only suffers physically and financially from the crime, but also needs to invest time in retraining her PWC again because she did not have her profile stored online. Although it was saved locally on her PC, the burglars wrecked her machine.

In the park, Maruja encounters a foreign visitor asking for the whereabouts of the central market. Maruja is surprised by the request because she (Maruja) would never go abroad without her location device. Maruja does not realise that this woman did not have a choice because of a lack of a roaming agreement between their respective service providers. Another issue is raised in the last situation in which Maruja reflects on theft of her electronic purse in a dangerous neighbourhood. While AmI technologies allow the update of neighbourhood crime rates and guide users out of such places, they still depend on the business models supporting such applications. Maruja did not know because she forgot to authorise the update of her location software.[14]

3.2.4 AmI technologies and devices

The scenario makes reference to several AmI or AmI-related technologies:

- Sensors and actuators
  - Embedded in the environment and in objects, such as the sensors in Paul's study used to monitor physical presence and actuators that close the door after a while for security reasons
  - RFID tags attached to clothing (readable from a distance) with backward traceability to the shop which sold it
- Indoor and outdoor positioning devices
- Biometrics including a fingerprint reader to open the door of the study and an iris scanner to authenticate online identity (which Ricardo manages to spoof because the model did not yet contain liveness testing)

[13] Krebs, Brian, "Teen Pleads Guilty to Hacking Paris Hilton's Phone", *Washington Post*, 13 September 2005. http://www.washingtonpost.com/wp–dyn/content/article/2005/09/13/AR2005091301423.html

[14] See recent experiments with so-called Map Mash-Ups, combining geographical visualisation tools such as Google Maps with other data such as local crime statistics: Wade Roush, Killer Maps, www.technologyreview.com, October 2005.

- Interfaces
  - Smart clothing, e.g., the blouse that has an integrated flexible screen
  - Speech and voice recognition
- Intelligent algorithms
  - For data mining (e.g., used by police)
  - Speech recognition
  - Web search algorithms
- A Personal Wrist Communicator which is a multi-functional (phone, watch, camera, colour display) personal intelligent device
- Wireless, wireline and broadband communications networks

3.2.5 AmI applications

The AmI technologies referenced in the scenario are used in various applications:

- Security – restricted and authenticated access to Paul's study via a fingerprint reader and to his online profile via an iris scanner; automatic closing of a door when the absence of a person is detected
- Remote surveillance of the home and other premises
- Digital rights management (DRM), e.g., a licence fee associated with an IP number to prevent illegal copies
- Audio tracking of meetings and automated transcription into text
- Shopping Assistant Software (SAS) with intelligent search capabilities for e-commerce
- Powerful spyware programmes to detect personal profiles
- Personalised advertising
- Seamless migration of content on different platforms/screens, from a PWC to big screens but only when explicitly authorised (and this went wrong in the case of Maruja as a result of a hasty decision)
- New crimes such as digital blackmail, determining the presence or absence of people by reading RFID tags incorporated in clothing and other objects, crime information networks (e.g., Google Earth combined with local crime statistics)
- Temporary online offers for quick decision-makers
- Location-based services
  - Automated priority settings on incoming messages (e.g., Paul in his boss's office; Maruja during her business meeting)
  - Advertising.

3.2.6 Drivers

Drivers for the AmI technologies and/or dark situations elaborated in the scenario are the following:

- *Telework* (working from home) – Although telework's importance and prevalence have been predicted for some decades, AmI might give a boost to it, not only because of the availability of high-bandwidth infrastructures, but also of its user-friendliness, media richness and proximity to face-to-face interactions (although these are still needed, as mentioned in the scenario).
- *Convenience* – The AmI home addresses human weaknesses (via sensors and actuators) such as forgetting to close a door or window or to put out the lights or to turn off the cooker, etc.
- *Parental control* – The adoption of AmI technologies may be stimulated by those who seek greater parental control of children and, in particular, their access to services, drinks, entertainment, etc. On the other hand, clever children such as Ricardo may try to circumvent control mechanisms in order to engage in ID theft within the family.
- *Crime* – Criminals may see AmI as offering opportunities for new forms of old crimes such as blackmail (on a small scale involving many people for small amounts of money) by intervening into personal and home networks; data laundering (personal profiles for which people are willing to pay money); robbery (of, e.g., electronic purses or by means of the remote detection of the presence/absence of wealthy individuals); exploiting weaknesses in AmI crime information networks such as a well-known weakness in the security of personal and home networks when rebooting.
- *Security* – Individuals, groups and societies will see AmI-based services such as remote surveillance as enhancing protection of physical premises as well as protecting their online identities.
- *Personalisation* – AmI will be driven by, inter alia, companies who see opportunities for better market penetration through the provision of personalised services such as suggestions for shopping (e.g., Shopping Assistant Software); for eating (e.g., restaurants) and for matching personal profiles with location-based information. Personalisation is also likely to be an important driver for individuals as well, who will enjoy the benefits of services specifically tailored to their interests, needs and desires.

3.2.7 Issues

The scenario raises several issues by showing what can go wrong with AmI in everyday life. Many of them have to do with human factors such as failing to take adequate measures and feelings of loss of control.

3.2.7.1 Human factors and security

Human factors such as excitement can cause people to forget things (closing the door to the study), but AmI can help address the consequences (closing the door, locking access to online services). As studies show repeatedly, however, human errors constitute major security weaknesses. AmI will certainly help to overcome

this problem, but it would be naïve to assume that human failings could be factored out completely. Since not everything in the smart home will be accessed via biometric verification only, people will continue to use easy-to-guess or accessible passwords and/or access codes.

Remote surveillance of the smart home is not enough to secure it. Security requires on-the-spot checks and back-up systems if something goes wrong. False "automatic" alarms could be an issue in the future to the extent that they become counterproductive and ignored.

The scenario depicts other vulnerabilities: Maruja accepts a special offer, suggested by her daughter, to buy a computer game on a web site that they did not check out properly because of lack of time.

3.2.7.2 Loss of control

Dark feelings can range from irksome to burdensome and entail annoyance and embarrassment. Although AmI is supposed to be seamless and only visible when we want it to be, it can be assumed that it also occupies our minds since settings have sometimes to be confirmed or changed. AmI cannot know everything. It has to be fed information, which places a burden on people. Also, when AmI does not function as it should, people will get annoyed, possibly leading to their temporarily rejecting it (switching off). Annoyance can be foreseen when AmI does things that are not expected or wanted, even if authorised (willingly or unwillingly). All this contributes to a feeling of loss of control.

Scene 1 shows a loss of control when Paul receives an alarm from his home system but without details on what is happening. He depends on his AmI system, but it does not behave as expected. More examples are raised in scene 2. Maruja gets an unexpected message on the same screen as her business presentation. The sex-related message came from an AmI service (Shopping Assistant Software), which had misinterpreted her desire for a "funny" gift. She is annoyed and embarrassed. In scene 3, Maruja is irritated because her avatar was not able to take into account her preferences.

Loss of control is also depicted when children seek to circumvent parental and teacher prohibitions over playing computer games at school. At work, employees are subjects controlled by automatic recording of what is said in meetings which in turn can lead to decisions taken on the basis of incomplete information, i.e., information that is not recorded.

3.2.7.3. Disproportionate reaction to suspicions

The scenario shows a weakness in profiling which leads to a disproportionate reaction to (unjustified) suspicions. Paul's boss informs him that he is being checked out by the police who have found that he seems to match one of their profiles of criminals. AmI systems generate lots of publicly available data on individuals, so

the police can check out people before seeking a search warrant. But profiling systems also generate false positives, and Paul's case is one such. Unfortunately for Paul, being subject to police scrutiny has negative consequences. He is under a cloud at work and misses out on a promotion.

3.2.7.4 Insider ID theft

Ricardo is able to use his father's identity to bypass parental controls and to shop and gamble online. The scenario shows that ID theft is possible without criminal intentions, that people who know each other can also breach privacy (the "little brother" phenomenon) and that once an ID is misappropriated, it is easy to spend money because payments are automated, at least up to a limit.

3.2.7.5 Exclusion

Not all AmI services will be available to everyone, of course. In scene 3, the foreign woman in the park does not have access to personalised location-based services because of a lack of an agreement between service providers.

3.2.8 Legal synopsis

3.2.8.1 Working from home

The first scene of this scenario highlights the important issue of privacy protection. Privacy is not only a social expectation, but it is also expressed in legal terms. Within the western legal system, privacy is primarily an issue of international and constitutional law, protected by explicit provisions, both in international human rights treaties and in the distinct national constitutions. The first provision to mention is Article 12 of the 1948 **Universal Declaration of Human Rights**,[15] although, strictly speaking, it has no legally binding force. Article 17 of the 1966 **International Covenant on Civil and Political Rights (ICCPR)** also seeks to protect privacy.[16] And finally, Article 8 of the

[15] Article 12 of the Universal Declaration of Human Rights (United Nations, 1948): "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[16] Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966): "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

European Convention on Human Rights (ECHR)[17] confers respect for private life. Both the ICCPR and the ECHR are binding treaties. Article 17 of the ICCPR and Article 8 of the ECHR[18] directly affect national legal systems. Both can be invoked and applied by national judges. The **Charter of Fundamental Rights of the European Union** also protects privacy (Article 7) and personal data (Article 8) of individuals.[19]

The protection of the private home together with the protection of privacy is guaranteed at the European level by Article 8 of the ECHR.[20] There is no explicit mention of a right to have data protected in the ECHR, but the case law of the European Court of Human Rights (the Strasbourg Court) leaves no mistake about this right being incorporated in the more general right to protection of privacy. Issues regarding violations of the home are also seen as privacy issues and vice versa. These rights are not absolute. Exceptions are possible (Article 8(2)), however, they have to fulfil several criteria: the restriction must be foreseen by law (the formal criterion); it must be necessary in a democratic society (the necessity criterion); it can only be used to achieve one of the specific and limited goals set out in Article 8 of the ECHR, including public security and the safeguarding of rights and freedoms of others (the legitimacy criterion). The Strasbourg Court has ruled that any action must be useful, indispensable and proportionate to achieve the set goal (the proportionality criterion). The last standard implies that the established goal could not be reached through measures that would have had a lesser impact on the guaranteed freedom of the individual concerned.

Article 8 of the ECHR has weaknesses. For instance, it does not apply to the private sector in a straightforward manner: you cannot take firms to Strasbourg; instead, you have to sue the Member State(s) responsible for human rights violations of private actors. The protection of personal data by privacy rights is not complete: the right to a private life, as interpreted by the Court, does not necessarily include all personal data; and the right of access to personal data is not covered by this Article, nor is the right to correct erroneous personal data.[21] These limitations explain why it was

---

[17] Council of Europe – European Convention on Human Rights of 4 November 1950.

[18] The ICCPR is overshadowed by the ECHR because the latter is older, has a strong supranational judicial control mechanism and the Strasbourg Court has issued an impressive list of judgments on privacy.

[19] Charter of Fundamental Rights of the European Union, *Official Journal* C 341, 18 December 2002. Article 7 says, "Everyone has the right to respect for his or her private and family life, home and communications"; Article 8 says, "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority."

[20] Article 8 of the European Convention on Human Rights states: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[21] Maghiros, I. (ed.), *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), IPTS Technical Report, Institute for Prospective Technological Studies, Seville, 2003. ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

necessary to create an independent set of data protection regulations at the level of the Council of Europe and the European Union. Unlike the ECHR privacy protection, the European Data Protection Directive[22] applies to the processing of personal data in both the private and public sectors (with limited exceptions).

The coexistence of privacy and data protection regulations can be understood as follows. According to Article 8 of the ECHR and its interpretation by the Court of Strasbourg, privacy is a legal concept to ensure non-interference in individual matters by the state and other powerful actors. It works as a shield to protect the opacity (anonymity) of the individual. Opacity is linked to the recognition of human rights, individual autonomy and self-determination. Normative in nature, opacity tools can be distinguished from transparency, which aims not against the power, but at channelling or controlling the power of the state and others. Transparency tools provide for a system of checks and balances and procedural safeguards. Interference into one's autonomy is then allowed, but under control.[23] This is the standpoint of the data protection laws, which also aim at protecting privacy. In sum, data protection is not prohibitive. The data protection regulations created a legal framework whereby the processing of personal data is in principle allowed and legal[24] (and therefore mainly belongs to tools of transparency) subject to safeguards protecting individuals, promoting accountability by government and private data holders, and providing data subjects with an opportunity to contest inaccurate or abusive record-holding practices. The rationale behind data protection in the public sector is the knowledge that authorities can easily infringe privacy and that in all administrative systems is an urge to collect, store and use data, an urge which must be curtailed by legal regulation. A similar rationale explains the European option to regulate data processing in the private sector.

The basic principles of data protection are spelled out by various international institutions, such as the Organization for Economic Cooperation and Development (**OECD Guidelines**[25]), the Council of Europe (**Treaty 108**[26]), the

[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *Official Journal* L 281, 23 November 1995. This Directive has been supplemented by data protection provisions in other, more specific directives.

[23] For more on opacity and transparency, see 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 Maghiros, I. (ed.) *Security and Privacy for the Citizen in the Post-September 11 Digital Age*, op. cit.

[24] An outright processing ban effectively applies only to special categories of sensitive personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

[25] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

[26] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *European Treaty Series – No. 108*, Strasbourg, 28 January 1981.

UN Guidelines[27] and the European Union (the Data Protection Directive). The European Union has also included the right to data protection in the European Charter of Fundamental Rights (see supra).

Within the European Union, the main source of regulation in the field is the **Data Protection Directive**,[28] together with legislation implementing it nationally. The Directive applies to the processing of data relating to an identified or identifiable natural person or "personal data".[29] Anonymous data do not fall under the scope of the Directive.[30] The Directive grants every person the right not to be subject to a decision that produces legal effects concerning him or significantly affects him and that is based solely on automated processing of data.[31]

The Directive applies to both the private and public sectors. It does not apply to processing of personal data by a natural person for purely personal and domestic purposes, and to data concerning legal persons. It also does not apply to processing carried out for purposes of public security, defence and national security or in the course of State activities in areas of criminal law and other activities that do not come within the scope of Community law.[32]

The Data Protection Directive and national data protection laws in general provide for a number of requirements in order to legally process personal information.[33] Those are twofold: on the one hand, there exists a series of rights for individuals[34] such as the right to receive certain information whenever data are collected, the right

[27] The United Nations Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990, are a more recent international instrument. We do not discuss these UN guidelines, because they are overshadowed by the other regulations in Europe.

[28] Directive 95/46/EC.

[29] It is not always clear what should be understood as "personal data" or when data are anonymous. See Chapter 5, section 5.3.4, subsection on "Data protection and profiling: a natural pair".

[30] However, the problem of anonymous data can be relative in some circumstances: the notion of "identifiable" in the European Directive is, unlike other international data protection texts, very extensive. Data that at first glance do not look like personal data can very often lead to an individual. Even if a processor wants data to be anonymous, they may not. The definition of "identifiable" is so broad that data can be considered personal as long as the controller himself is still able to identify the persons behind the data. Staying out of reach of European data protection is only possible through maximum anonymity.

[31] The Data Protection Directive, Article 15. See also sections 3.2.8.4 and 3.5.8.1 as well as Chapter 5, section 5.3.4, subsection on "Data protection and profiling: a natural pair".

[32] The Data Protection Directive, Article 3. There is now a debate about whether to extend data protection to third pillar issues: See Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM (2005) 475 final of 4 October 2005. http://eur – lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0475en01.pdf

[33] For an overview, see Gutwirth, S., *Privacy and the information age*, Rowman & Littlefield, Lanham/Boulder/New York/Oxford, 2002, pp. 83–112.

[34] See the discussion on the right to be informed in sections 3.2.8.4, 3.2.8.7 and 3.4.8.4; the right to consult the data, the right to have data corrected and the obligation on data controllers to collect and keep relevant, correct and up-to-date data in sections 3.2.8.2, 3.3.8.3 and 3.5.8.2 and the right to object to certain types of data processing in section 3.5.8.1.

of access to the data and, if necessary, the right to have the data corrected and the right to object to certain types of data processing. Also, data protection law generally demands good data management practices by the data controllers and imposes a series of obligations[35]: the obligation to use personal data for specified, explicit and legitimate purposes (finality or purpose specification principle), the obligation to guarantee the confidentiality and security of the data against accidental or unauthorised access or manipulation and, in some cases, the obligation to notify a specific independent supervisory body before carrying out certain types of data processing. These laws provide specific safeguards or special procedures to be applied in the case of transfers of data abroad. Any processing of personal data must be lawful and fair to the individuals (fairness principle). All data must be adequate, relevant and not excessive in relation to a purpose for which they are collected and/or further processed (proportionality principle). There is also a prohibition on processing sensitive data. To be legitimate, personal data may only be processed if the data subject has unambiguously given his consent. It may be processed without his consent under limited conditions provided by law.[36]

The challenge for data protection law in relation to AmI mainly concerns the reconciliation of the principles of data protection law with the concept of AmI. This challenge emerges because AmI and its supporting technologies need personal data and profiles to work. In order to provide people with information (enhanced goods and services), AmI needs to process personal information.[37] The decreasing cost of these technologies as well as the increasing emergence of customers willing to pay for these services are already noticeable trends.

The **Privacy & Electronic Communications Directive**[38] contains specific legal, regulatory and technical provisions for electronic communications. It applies only to

[35] See the discussion on the finality and purpose specification principle in sections 3.2.8.2 and 3.2.8.7, the confidentiality and security obligation in sections 3.2.8.3 and 3.3.8.3, the obligation to notify the supervisory body and the fairness principle in sections 3.2.8.2 and 3.5.8.2, the proportionality principle in sections 3.2.8.2 and 3.3.8.4, the prohibition on processing sensitive data in sections 3.3.8.4 and 3.5.8.1, and the specific safeguard to be applied in the case of transfer of data abroad in section 3.4.8.1.

[36] When the processing is necessary for (1) the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or (2) compliance with a legal obligation to which the controller is subject, or (3) protecting the vital interests of the data subject, or (4) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or (5) the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject (Data Protection Directive, Article 7). The issue of consent is further discussed in sections 3.3.8.4 and 3.4.8.2.

[37] However, this means that not only should concepts, scenarios, practices and techniques of AmI be tested on their compliance with data protection law, but also data protection law itself can and should be put into question if necessary, e.g., where some data protection rights cannot be reconciled on a reasonable ground with good practices and techniques of AmI that are preferable and desired by the user.

[38] 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 (Directive on privacy and electronic communications), *Official Journal* L 201, 31 July 2002, pp. 37–47.

public communication services, whereas the Data Protection Directive applies to both public and non-public services. The Privacy & Electronic Communications Directive not only protects fundamental rights and freedoms of natural persons, but also the legitimate interests of legal persons, whereas the Data Protection Directive only offers protection to natural persons. Neither of the directives applies to activities concerning public security, defence, state security and the activities of the state in areas of criminal law. The Privacy & Electronic Communications Directive stipulates that Member States may, for reasons of national security, defence, public security and the prevention, investigation and prosecution of criminal offences, enact legislation providing for the retention of traffic and location data pertaining to all forms of electronic communications by telecommunications operators.[39] It imposes security and confidentiality obligations on service providers[40] and foresees specific rules for traffic[41] and location[42] data and provides for limits in processing such information.

[39] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal* L 105, 13 April 2006. This retention possibility has been firmly criticised by EPIC (www.epic.org) and Privacy International (www.privacyinternational.org): "Although this data retention provision is supposed to constitute an exception to the general regime of data protection established by the Directive, the ability of governments to compel Internet service providers and telecommunications companies to store all data about all of their subscribers can hardly be construed as an exception to be narrowly interpreted. The practical result is that all users of new communications technologies are now considered worthy of scrutiny and surveillance in a generalized and preventive fashion for periods of time that States' legislatures or governments have the discretion to determine." See Andrews, S., *Privacy and human rights 2002*, produced by the Electronic Privacy Information Center (EPIC), Washington, DC, and Privacy International, London, 2002, p. 44. http://privacyinternational.org/survey/phr 2002. These privacy invasive retention schemes were devised in the aftermath of 11 September 2001. Critics also come from Internet service providers who are confronted with the storage and security costs, and from other human rights organisations like Statewatch (www.statewatch.org) and EDRI (http://www.edri.org). See also Article 29 Working Party, *Opinion 4/2005 on the Proposal for a Directive on the retention of Data processed in connection with the Provision of Public Electronic Communications Services and Amending Directive 2002/58/EC* (http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm). The Data Retention Directive is also discussed under section 3.2.8.4.

[40] See also sections 3.2.8.3 and 3.3.8.3.

[41] " '[T]raffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof" (Article 2). The level of protection of traffic data depends on the purpose of the processing: (1) transmission of communication, (2) billing or (3) marketing electronic communication as well as providing of value-added services, e.g., tourist information, route guidance, traffic information and weather forecasts, and generally may be processed by the service provider to the extent and for the duration necessary for that purpose. In any of these cases, processing of traffic data must be restricted to what is necessary for the purposes of such activities and must be restricted to persons acting under the authority of the network or service provider. In any of these cases, if data are processed for a longer time than for the transmission, the user or subscriber must be informed of the duration of such processing (Article 6 of the Privacy & Electronic Communications Directive).

[42] " 'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic

AmI will cause a blurring of the boundaries between spaces and activities. The first scenario gives an example of a father, working for a security company mostly from his private home. New communication technology facilitates teleworking and makes it possible to deal with private business from an office. Boundaries between what is private and what is professional will become less distinctive and more permeable than today. What are the consequences of such ambiguous situations from a privacy point of view? How can a distinction still be made between private and professional, private and public? Such situations result in doubts about the extent to which privacy is legally protected in professional contexts, especially when employees work outside the office.

The European Court of Human Rights has clarified that the protection of private life does not exclude the professional life, and that it is not limited to the life within the home or family. In *Niemitz* v. *Germany* (23 November 1992), the Court stated that there is no reason why the notion of "private life" should be taken to exclude activities of a professional or business nature. Moreover, the Court added that this view is supported by the fact that "it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not." In *Halford* v. *United Kingdom* (27 May 1997), the Court introduced the criterion of "reasonable expectations of privacy". Accordingly, Miss Halford, a senior officer whose telephone calls were intercepted without warning, was granted privacy protection in her office space, although not absolutely. The protection of privacy at work remains one of the grey areas in European human rights law. The case of Halford, a senior officer with privileges, is in itself not a typical case. More case law is needed to clarify the reasonable expectation of privacy in the workplace. It should also be borne in mind that surveillance of the individual after a suspicion has been raised raises fewer concerns than the general surveillance at workplace, in a public building or at home. It is unclear how and if the reasonable expectation of privacy would apply in AmI situations as described in Scenario 1. While being always online, would we be able to talk with any expectation of privacy at all?

An additional problem is the lack of clarity regarding the consequences of privacy violations. The European Court of Human Rights is unwilling to reject evidence obtained through privacy violations. In cases such as *Khan* (2000) and *P.H. & P.G. against the United Kingdom* (2001), the Strasbourg court decided that a violation of Article 8 of the ECHR had taken place, but it nevertheless accepted the evidence found in violation of Article 8 of the ECHR in a criminal process.

---

communications service" (Article 2). Location data may only be processed (a) when they are made anonymous or (b) with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a *value-added service*. When consent has been obtained, the user shall be given the possibility to *withdraw his consent* for the processing of such data at any time and must continue to have the possibility, using a simple means and free of charge, of *temporarily refusing* the processing of such data for each connection to the network or for each transmission of a communication (Article 9 of the Privacy & Electronic Communications Directive).

Some national courts have followed this line of reasoning. In Belgium, there are examples of the erosion of privacy law in the workplace: The Belgian Data Protection Act (1992, revised in 1998) and the Collective Labour Agreement 68 of 16 June 1998 foresee that strict procedures of information and negotiation must be followed when cameras are installed in the workplace. Thus, employees must be informed when an employer installs cameras. The *Cour de Cassation*, the highest Belgian court, argued in a recent case that Articles 6 and 8 of the ECHR do not necessarily mean that the infringement of the information and negotiation procedure laid down in data protection law voids the evidence obtained with a hidden camera (in this case, a theft by an employee).[43]

Most probably AmI will challenge our understanding of the terms "home" and "communication" and require a reinterpretation of the term private life, since the distinction between private and professional life might become further blurred. It is unclear how and if the criterion of "reasonable expectations of privacy" will be applied further by the European courts. It is equally unclear how this criterion will apply in an AmI world. If the privacy case law does not offer sufficient and clear privacy protection of AmI environments, additional legal and constitutional protection may be warranted.

3.2.8.2 Digital rights management

The scenario gives an example of using online content and accessing online services by unauthorised individuals, who manage to spoof the technical access control. It also shows a new model of consuming the content legally by accessing it from a given location in accordance with the licence provisions (Ricardo's friends play an online game for which Ricardo has a licence). Licence provisions (stipulating how the content might be used, on which device, or how many times) will most probably be governed by digital rights management (DRM) systems.

In order to manage access rights, some digital rights management mechanisms would probably be used. If intrusive DRMs are chosen, systems might require identification and authentication of users having rights to the content, and might monitor how many times users access the work, how long they consume the content, what other content they like, etc. Such DRM systems allow content holders not only to process personal data (user behaviour), but also to construct (group) profiles, building statistics, consumer behaviour, etc. Here again, personal data are stored for a longer period and for purposes of which the user may not always be aware. This issue bears on the protection of privacy and personal data.

---

[43] See also De Hert, P., and M. Loncke, "Camera Surveillance and Workplace Privacy in Belgium", in Sjaak Nouwt, Berend R. de Vries and Corien Prins (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, The Netherlands, 2005, pp. 167–209. See also the judgment of the Belgian *Cour de Cassation* of 2 March 2005 at http://www.juridat.be.

Creating profiles via DRM systems may conflict with some principles expressed in Article 6 of the Data Protection Directive,[44] like, inter alia, fairness and lawfulness, purpose specification and finality, data accuracy and proportionality. For example, the proportionality criterion laid down in Article 6 obliges policy-makers to consider alternative, less infringing ways of reconciling intellectual property rights with privacy rights.

DRMs are protected against circumvention under the **Copyright Directive**,[45] even if they impede data protection provisions. Member States must grant protection against any person knowingly performing without authority acts such as: "(a) the removal or alteration of any electronic rights-management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority" (Article 7).

The Directive harmonised the legal protection against circumvention of effective technological measures (and against provision of devices and products or services aiming at circumvention), which effectively restrict acts not authorised by the holders of any copyright, rights related to copyright or the *sui generis* right in databases.[46] Notwithstanding this legal protection, Member States shall take appropriate measures to ensure "that the right holders make available to the beneficiaries of an exception or limitation provided for in national law the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned" (Article 6(4)).

---

[44] Article 6 says, "1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use; 2. It shall be for the controller to ensure that paragraph 1 is complied with."

[45] 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.

[46] Article 6 of the Directive states: "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective."

Another instrument providing for legal protection of the technological measures is the **Software Directive**.[47] The Directive 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 device which may have been applied to protect a computer program.[48] An important difference between this Directive and the Copyright Directive is that this Directive requires that the "sole" intended purposes is circumventing the technical device, while the Copyright Directive requires that it would be "primarily" designed for this purpose. The Software Directive only protects against the putting into circulation of devices that have no other function than circumventing protective measures, which is an important limitation. Another important difference is that the Software Directive only protects against the putting into circulation, possession of these devices and not against the act of circumventing as such. It would be advisable to have a uniform solution which includes the protection of privacy-enhancing technologies.

The Directive on the protection of services based on conditional access[49] should be also mentioned here. This Directive deals with the legal protection of all of those services whose remuneration relies on conditional access, such as television broadcasting, radio broadcasting and especially information society services. Many services in an AmI world will rely on conditional access and it is important to provide sufficient protection of those services. The Directive obliges the Member States to prohibit (a) the manufacture, import, distribution, sale, rental or possession for commercial purposes, (b) the installation, maintenance or replacement for commercial purposes, and (c) the use of commercial communications to promote devices, which enable or facilitate without authority the circumvention of any technological measures designed to protect the remuneration of a legally provided service. A similar legal protection could be provided for privacy-enhancing technologies.

DRM systems might also prevent users from anonymously "consuming" (reading, viewing, listening to) "information". The argument of freedom of expression will probably prove to be one of the more powerful in the future, next to privacy and data protection arguments, against such rights management systems, based on individual identification. General principles of data protection and freedom of expression and thought oppose digital rights management systems and applications that rely on unnecessary individual monitoring or that are used for purposes other than DRM, such as profiling, especially when these other uses are imposed in a

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

[48] Privacy-enhancing technology might be protected against their circumvention under this provision, since they are often software.

[49] Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, *Official Journal* L 320, 28 November 1998, pp. 54–57.

non-negotiable way. Possible solutions may be found in e-commerce and consumer protection law, by giving, for example, more legal (and technological) possibilities to consumers to negotiate use of their personal data.

3.2.8.3 ID theft and liability

As we saw in the scenario, it was not difficult for Ricardo to obtain access to his father's profile and preferences, as well as to access to his father's professional and confidential documents. Who is responsible for the fact that Ricardo could enter the office and obtain his father's profile? Was the system developed in a way sufficient to prevent manipulation of the kind described in the scenario? Was the father careful enough or did he put the confidential information in his office in jeopardy?

The Data Protection Directive imposes a number of obligations on the data controller, such as those on confidentiality and security of data. Appropriate technical and organisational measures must be taken, at the time of the design of the processing system and at the time of the processing itself to ensure an appropriate level of confidentiality and security, taking into account the state of the art and the costs of their implementation in relation to the risks represented by the processing and nature of the data to be protected (Articles 16 and 17). Analogous security obligations of the service providers are included in the Privacy & Electronic Communications Directive.[50] Compliance with such security obligations is not clearly regulated. When Paul works at home or at any place in the AmI environment and processes personal data of data subjects, for example, his employer's clients, strict compliance with the Data Protection Directive is needed. It is not clear, however, how far the obligations

[50] Article 4 says: "(1) Service providers should take appropriate technical and organisational measures to safeguard the security of their services, if necessary in conjunction with the network provider and having in regard the state of the art and the cost of their implementation." According to recital 20, they also have the obligation to take, at their own cost, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. See also in the same Article: "(2) In case of a particular risk of a breach of the security of the network, the service provider must inform the subscribers of such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved." This information must be free of charge. According to recital 20 of the Directive, the service provider must also inform the users and subscribers of Internet communication services of measures they can take to protect the security of their communications, for instance, by using specific software or encryption technologies.

Article 5 obliges Member States to guarantee the *confidentiality* of communication through national regulations prohibiting any unauthorised listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users (except when legally authorised to do so or when legally authorised for the purpose of providing evidence of a commercial transaction). In any case, the subscriber or user concerned is provided with clear and comprehensive information in accordance with the Data Protection Directive. The confidentiality of communications applies both to the contents of communications and to the data related to such communications.

of both the "data controller" and the "data processor" (acting under the responsibility of the data controller) go. Who is responsible for the security of the home network used for telework? Is the employer obliged to secure at his risk and at his cost the employee's home-work environment? Who – the employee or the employer – is responsible if personal data relating to customers are copied, altered or stolen through the employee's home network as a consequence of a lack of security? How can the security of the home system network be controlled by a third party? When is the employer liable when something goes wrong with personal data, and when the employee?

All controllers and processors must be aware of the security and confidentiality requirements. National laws should be harmonised to organise data protection and security measures in telework conditions and clear policies should be agreed.

Many Member States have no criminal sanctions for violation of the duty to foresee sufficient security safeguards. Especially when unique identifiers are being collected and processed, lack of protection could be considered as a criminal act. One can foresee specific measures on the use of biometric data and to prohibit badly protected or too risky use of biometrics.[51]

Ricardo was able to enter his father's office and profile relatively easily. Perhaps he was able to hack the profile and view the confidential information (both private and professional information) due to defects in the security system (hardware or software). The question is whether the provider of the security software can be held liable and to what extent this liability can be waived in general contractual terms and conditions. Today, software products' licence agreements clearly indicate that the software is purchased without liability for the loss of information. In this scenario, it is not clear if the defects, if any, are linked to the software or to the hardware. On the basis of actual regulation, this is important: Article 1 of the **Directive on liability for defective products**[52] provides that the producer of a product is liable for damage caused by a defect in his product. A product, however, is only defective when it does not provide the "safety which a person is entitled to expect taking all circumstances into account, including: (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put; (c) the time when the product was put into circulation. A product shall not be considered defective for the sole reason that a better product is subsequently put into circulation."[53] A product is defined as "all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable".[54] It is

[51] De Hert, P., "Biometrics: legal issues and implications", Background paper for EC JRC – Institute of Prospective Technological Studies, Seville, January 2005.

[52] 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, 7 August 1985.

[53] Article 6 of the Directive on liability for defective products.

[54] Article 2 of the Directive on liability for defective products.

unclear today whether this Directive applies to defective software and/or hardware, and whether the Directive could be invoked in the case of ICT products. Also, it is not clear if and to what extent economic damages fall under the concept of damage (injury) in the sense of the Directive.[55]

From a consumer perspective, there are reasons to argue in favour of a full application of the Directive to the issues mentioned in the preceding paragraph. The strict liability regime of the Directive on liability for defective products facilitates establishing the producer's liability, since no proof of fault is required: demonstrating that the product is defective is sufficient. Since the security system did not prevent the son from using his father's profile, we could consider the system to be defective. An important question is, of course, which producer caused the defect and how to find him. Article 3 of the Directive provides for the joint liability of producers and suppliers. It states clearly that, when the producer of a product cannot be identified (which might be a serious problem in an AmI world), the supplier is liable unless "he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product". On the basis of Article 5, two or more persons shall be liable jointly and severally when they are liable for the same damage. This implies that if several service providers are coresponsible for the defect, the victim can claim the total damages from one of them, probably his direct supplier.

In certain specific situations, defined in Article 7, the producer can limit his liability. A producer cannot invoke the fault of others to escape his liability when his product was defective.[56] He can reduce his liability when the victim was coresponsible,[57] as in this case where the father has been negligent. Article 12 does not allow provisions excluding or limiting liability arising from this Directive.

3.2.8.4 Inadequate profiling

Paul is astonished because the police request access to his personal data. He has heard that the police have been investigating innocent people because their suspicions were based on inadequate profiling. Paul does not understand why the cyber police suspect him of a certain crime. Probably the cyber police treat him as a suspect, because a small part of his profile fits with that of a perpetrator of a crime. The decision to ask for information from his employer on the basis of this small match is a decision based solely on the automated processing of data intended to

[55] See section 6.3.8.

[56] Article 8 (1) of Directive on liability for defective products states: "The liability of the producer shall not be reduced when the damage is caused both by a defect in the product and by the act or omission of a third party."

[57] Article 8 (2) of Directive on liability for defective products states: "The liability of the producer may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person or any person for whom the injured person is responsible."

evaluate certain personal aspects relating to him, such as his reliability and conduct. In order to be able to defend himself against these accusations, Paul will need to know which personal data the cyber police collected and processed. The data protection laws traditionally grant rights to the data subject, enabling him to safeguard his interests in the collection and processing of his personal data, including the right to access and correct, the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is solely based on such an automated processing of personal data. Such rights are explicitly granted by the Data Protection Directive.[58] However, the Directive does not apply to activities in areas of criminal law (nor, as mentioned above, public security, defence and state security. These services are governed by national data protection laws, which have not been harmonised by an instrument of the European Union. At the same time, threats to security as well as new policing and antiterrorism strategies are paving the way for the acceptance of police practices based on profiling. The principle of availability, for example, included in the European Union's Hague Programme[59] gives greater data protection flexibility to the police.

It is also clear that the longer electronic communications traffic data are retained, the greater are the possibilities for the police to collect and process personal data and to build and use profiling techniques. According to the Privacy & Electronic Communications Directive, electronic communication data must be deleted when they are no longer needed for the provision of the service or for the billing thereof. However, like the Data Protection Directive, the Privacy & Electronic Communications Directive does not apply to activities in areas of criminal law, nor to public security, defence or state security.

That does not mean there is a complete lack of protection and individual guarantees. National data protection rules may provide some safeguards (e.g., the Belgian national data protection law is applicable in such circumstances). National data protection rules have to be in line with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108. With regard to police, security and defence issues, however, the provisions of the 1981 Convention are very sober. The 1981 Convention contains no provision comparable to Article 15 of the Data Protection Directive providing the right not to be subject to a decision that produces legal effects concerning the data subject or significantly affects him and that is solely based on such an automated processing of personal data. This is only partly compensated for in Recommendation No. R (87)15

[58] Articles 6, 12 and 15 of the Data Protection Directive.

[59] In the Hague Programme of October 2005, the Commission proposed to substitute the principle that data can only be transmitted to another Member State on the conditions established by the state that holds the information with the "principle of availability". Under the latter principle, the authorities of any Member State would have the same right of access to information held by any other authority in the Union as applies to state authorities within the state where the data are held. According to the Hague Programme, the Commission made a proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490 final. http://europa.eu.int/eur – lex/lex/LexUriServ/site/en/com/2005/com2005_0490en01.pdf

regulating the use of personal data in the police sector (17 September 1987). The recommendation, a "soft law" instrument developed by experts in the context of the 1981 Council of Europe Convention, is not legally binding and was conceived in an era that was unaware of (or unwilling to accept) new forms of systematic and intelligence-led policing. If our police forces were to apply the recommendation today, they would have no choice except to collect data only when there are sufficient grounds to do so and to destroy such data as soon as possible. Clearly, this is not in line with current policing and antiterrorism policies and strategies.

In addition to national laws and international instruments, there are some initiatives at European level relevant to protection of personal data with regard to police, security and defence issues. The **Data Retention Directive**[60] provides for at least six months and a maximum of two years for data retention necessary for the purpose of investigation, detection and prosecution of serious crime. The data to be retained are the traffic and location data necessary to identify the subscriber or registered user. It applies to legal entities and natural persons both. However, it does not apply to the content of communication.[61] The Directive does not indicate what is regarded as a serious crime, except to say that it applies to serious crimes as defined in national laws. It also states that the necessity and proportionality principles must be defined in national laws in accordance with international rules.[62] The respect for the freedoms and fundamental rights of persons concerned are expressed in recitals to the Directive.[63] The Directive also sanctions the access to and transmission of the retained data, which is not permitted under national laws adopted pursuant to this Directive, and provides for the right to compensation in case of damages caused by any unlawful processing of data.[64]

Moreover, the European Commission has proposed a third-pillar data protection instrument.[65] There is a strong need for a coherent instrument for the protection of personal data under the fields now covered by Titles V and VI of the EU Treaty covering current police practices such as profiling. A framework favourable to profiling practices as described in the scenario is not unthinkable, although it should be balanced with adequate guarantees for the data subjects. Defining the rights of the data subject in the context of data processing in a criminal investigation is one of the aims of the draft Framework Decision on the protection of

[60] Directive 2006/24/EC.

[61] Articles 1 and 6 of the Data Retention Directive.

[62] Article 4 of the Data Retention Directive.

[63] Recitals 9, 16, 17, 22 and 25 of the Data Retention Directive.

[64] Article 13 of the Data Retention Directive.

[65] Proposal for a Council Framework Decision on the protection of personal data in the framework of police and judicial cooperation in criminal matters, COM(2005) 475 final of 4 October 2005. http://eur – lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0475en01.pdf. The European Union was founded on three pillars. First pillar issues fall within the domain of the European Community. The second pillar concerns matters of common foreign and security policy. The third pillar concerns criminal matters within the domain of police and judicial co-operation.

personal data in the framework of police and judicial co-operation in criminal matters.[66] Such rights are defined in Chapter IV of the proposal. The proposal envisages a data subject's right to information,[67] when data are collected with his knowledge as well as when such data are not obtained from him or are collected without his being aware of such collection.[68] Necessarily, there are some restrictions on such disclosures.[69]

The proposal also foresees the right of access, rectification, erasure or blocking of data,[70] also subject to some restriction.[71] This provision, analogous to Article 12 of the Data Protection Directive, should allow Paul to know why he is suspected by the police and might allow him to prove he is not the person for whom the cyber police are searching. Moreover, the right to rectification, blocking and erasure of data would allow him to correct his profile as created by the cyber police. Article 22 of the proposal would require that any rectification, erasure or blocking be notified to third parties to whom the data have also been disclosed, such as Paul's employer or other state agencies. In addition, the proposal contains provisions relating to the principles of fairness and lawfulness, purpose specification, legitimacy and proportionality, and to data quality.[72]

The obligation to ensure the high quality of data is crucial in order to make sure profiles built on those data are correct and effective as a tool of modern investigation practices.

The above safeguards are essential to protect data subjects against victimisation and abusive commercial practices.

---

[66] See recital 14 of the proposal.

[67] Articles 19 and 20 of the proposal. Some information must be provided, including the identity of the controller, the purposes of the processing the recipients of the data.

[68] Some additional conditions are imposed. See Article 20 (1) of the proposal.

[69] Article 19 (2) and Article 20 (2) of the proposal.

[70] Article 21 (1) states: "(a) without constraint, at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, the legal basis of the processing and the recipients or categories of recipients to whom the data have been disclosed; communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; (b) as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Framework Decision, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort."

[71] Article 21 (2) – (4) of the proposal.

[72] Article 4 (1) (d) of the proposal states that personal data must be "accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they must provide that data are distinguished in accordance with their degree of accuracy and reliability, and in particular that data based on facts are distinguished from data based on opinions or personal assessments."

3.2.8.5 Monitoring behaviour

Paul and Maruja installed a system to monitor the digital movements of their children. It does not function, since the son has disabled the system, but should the parents be entitled to do so in an AmI world (even outside the private home)? Has Ricardo the right to protect his privacy, especially in his own home? Article 8 of the ECHR protects the private life of every natural person and thus that of Ricardo. Paul may have certain rights to control what his children are doing, but these rights are to be balanced.

The United Nations Convention on the Rights of the Child[73] contains a specific privacy right for children. Without denying parental rights, this UN Convention adds more weight to the privacy rights of children. The Convention also sets up monitoring instruments such as National Children Rights Commissioners. "New" problems such as the digital monitoring of children will thus also have to be taken up by National Children Rights Commissioners. It is unclear what the outcome of this balancing act will be. Permanent monitoring infringes on children's privacy rights, but it might be looked upon as a way of or price for granting more physical liberty to children.

3.2.8.6 ID theft and payments

Ricardo accessed his father's profile to download movies and make online payments. What is the status of a contract concluded by a minor (probably not capable of concluding contracts independently)? What is the status of contracts concluded by someone who has infringed another's private profile? Ricardo misleads the system, but we can ask how much effort the service supplier should make to ensure that he verifies who the real customer is.

There are two main legal texts relevant to electronic contracts.[74] The first is the **Distance Contract Directive**.[75] It applies to consumer contracts concluded under an organised distance sales or service-provision scheme run by a supplier by means of distance communication. The Directive obliges the supplier to provide to the consumer specific information related to a contract in good time prior to its conclusion. This obligation, created to protect the consumer, also refers to the protection of those unable to give their consent, such as minors. The supplier is obliged to identify himself and the main stipulations of the contract (characteristics of goods or services, price, including all taxes, delivery costs, arrangements for payment, the period for which the offer remains valid and so on). In order to obtain a certain AmI service, many service providers may be involved and it may not be feasible

[73] United Nation Convention on the Rights of the Child of 20 November 1989.

[74] On consumer protection, see section 3.3.8.3.

[75] 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, 4 June 1997.

for all of them to provide the required information. How to solve this problem? How can electronic contracts be concluded through intelligent agents? How can conditions, such as consent, provision of information prior to the contract, approval of the goods, etc., be fulfilled?

Article 6 of the Distance Contract Directive provides for a right of withdrawal within at least seven working days. Where the right of withdrawal has been exercised by the consumer, the supplier must reimburse the consumer free of charge. In principle, the father could use this right to cancel the contract. However, he cannot exercise this right where services (such as downloading X-rated movies) are provided before the withdrawal period concludes, or for the supply of goods made to the consumer's specifications or clearly personalised, or for the supply of audio or video recordings or computer software which were unsealed by the consumer or for certain other services such as online betting.[76] It is likely that the goods or services bought by Ricardo fall under one of these exceptions which will be true for many AmI services too. Thus, the right of withdrawal may not be very helpful in an AmI future.

Also, even if Paul were entitled to exercise his right of withdrawal, the refund of sums already paid might be difficult to achieve in practice, especially when goods or services are delivered from outside the European Union. The Distance Contract Directive will not offer much assistance in such cases. What could help is the creation of a trusted third party that receives the payments on behalf of the service provider, while keeping the amount of the payment automatically in a temporary account, until the right of withdrawal has expired.

The Directive also provides for specific information requirements and a written confirmation or confirmation in another "durable medium" that must be made available to the consumer. Among the requirements are information on the right to withdrawal, the supplier's geographical address, after-sales services and guarantees, and the conclusion for cancelling the contract, where it is of unspecified duration or exceeding one year.[77] Again a problem might arise when several suppliers are involved.

The **Directive on electronic commerce** protects consumers in the domain of e-commerce.[78] It applies to information society services defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[79] Insofar as they represent an

[76] Article 6(3) of the Distance Contract Directive. The Directive also mentions goods that, by reason of their nature, cannot be returned or are liable to deteriorate or expire rapidly.

[77] Article 5 of the Distance Contract Directive.

[78] 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.

[79] Article 2 (a) of the Directive on electronic commerce in relation to Article 1(2) of the Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down the procedure for the provision of information in the field of technical standards and regulations and on rules on information society services, *Official Journal* L 204, 21 July 1998, p. 37. The Directive was amended by the Directive 98/48/EC *(Official Journal* L 217, 5 August 1998, p. 18).

economic activity, they also extend to services which are not remunerated by those who receive them, such as online information or commercial communications or tools for search, access and retrieval of data. Information society services also include the transmission of information via communication networks, providing access to a communication network or hosting information provided by a recipient of the service.

Electronic mail or equivalent individual communications used by natural persons acting outside their business, trade or profession is not regarded as an information society service. The contractual relationship between employers and employees is excluded. Activities that, by their very nature, cannot be carried out at a distance and by electronic means, such as medical advice requiring the physical examination of a patient, also cannot be considered as information society services. In an AmI world, more services will be carried out at a distance and the definition of information society services might change dramatically.

The Directive on electronic commerce imposes important information obligations on the service provider,[80] especially if the contract is concluded by electronic means.[81] Those additional rules, however, do not apply to contracts concluded *exclusively* by exchange of electronic mail or equivalent individual communications. In any case, the contract terms and conditions must be made available to the recipient in a way that allows him to store and reproduce them.[82] Although such provisions might appear useful when contracting online, the Directive does not provide a direct solution in cases where contracts are concluded in abuse of personal profiles.

Ensuring the security of contracts was one of the objectives of the **Directive on electronic signatures**.[83] This Directive creates a legal framework for electronic signatures and for certain certification services. Electronic signatures might

[80] Article 5 of the Directive on electronic commerce obliges service providers to provide at least the following information: his name, geographic address, e-mail address, the trade register in which the service provider is entered and his registration number, VAT number, the particulars of the relevant supervisory authority. If the service provider is in a regulated profession, he must identify the relevant professional body with which he is registered, its professional title and make reference to applicable professional rules in the Member State of establishment and the means to access them.

[81] Article 10 (1) of the Directive on electronic commerce states that in such a case, the service provider must supply the following information in a clear, comprehensible and unambiguous way prior to the order being placed: (a) the steps to be followed to conclude the contract; (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible; (c) the technical means for identifying and correcting input errors prior to the placing of the order; and (d) the languages offered for the conclusion of the contract. Article 11 requires the service provider to acknowledge the receipt of the recipient's order without undue delay and by electronic means and has to provide effective and accessible technical means allowing the recipient to identify and correct input errors, prior to the placing of the order.

[82] Article 10 (2–4).

[83] 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.

enhance the security of electronic transactions in an AmI world.[84] To make electronic signatures reliable, they should be certified by professional organisations that can ensure they fulfil the necessary requirements. That is why the Directive tries to promote the establishment of certification service providers. To further enhance the trust in electronic signatures, the Directive enumerates the requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures. The Directive also deals with the legal effects of electronic signatures[85] and the liability of certification service providers.

3.2.8.7 Spyware, personal preferences and the illegal collection of data

When Maruja purchases the game for her daughter on the Web, a powerful spyware program is active, searching personal data and preferences.

The use of spyware clearly constitutes an infringement of the basic principles of data protection. Article 6 of the Data Protection Directive provides that personal data must be processed "fairly and lawfully", a provision linked to the principle of transparency in processing. Moreover, according to the purpose specification principle, personal data must be collected for previously specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The use of techniques such as spyware runs counter to the rights conferred on the individual by the data protection law. In principle, data subjects have to be truly and fully informed about all phases and contexts of the processing procedure.[86] Such transparent information is a *conditio sine qua non* for subsequent controls on data processing. It specifically applies to the gathering of personal data, which should

[84] They are also important in an AmI world, since they might allow the use of pseudonyms: Only the certification provider needs to know the identity of the signatory. The party who receives the document with an electronic signature can rely on the certification provider and in case of a legal conflict, the certification provider can exceptionally make the identity of the signatory public.

[85] The legal effects of electronic signatures depend on whether they are advanced electronic signatures according to the criteria laid down by Article 5 of the Directive.

[86] The right to be informed is granted by Articles 10 and 11 of the Data Protection Directive. In collecting data from the data subject, the controller must always provide the data subject with (1) the identity of the controller or his representative and (2) the purposes of the processing for which the data are intended. Some additional information should be provided if necessary to guarantee a fair processing, such as (1) the recipients or categories of recipients of the data, (2) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of a failure to reply [this refers to the question as the data collection technique] and (3) the existence of the right of access and the right to rectify the data concerning the data subject. When the data have not been obtained from the data subject himself but from a third party, the controller or his representative must at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, also provide the data subject with information as described above, including the indication of the categories of data concerned.

not be based on secret, hidden or sly methods. The secret, hidden gathering and processing of personal data or the hidden use of microphones, cameras, listening devices, detectors and programmes are in principle prohibited. No openness, no legitimacy. To be legitimate, according to Article 7 of the Data Protection Directive, personal data may only be processed if the data subject has unambiguously given his consent or if the processing is necessary in certain situations which are clearly not covered in the case of spyware.

The Cybercrime Convention[87] is an international instrument that obliges the contracting parties to create both substantive and procedural legislation related to certain offences. The use of spyware programs (installing and spying) is a criminal offence since it involves illegal access (Article 2) and illegal interception (Article 3) when there is, in the latter case, an interception, without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system.

Not only is the use of spyware a criminal offence, the Cybercrime Convention also incriminates the following misuses of devices: "when committed intentionally and without right (a) the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing an illegal access or interception or a data or system interference." Simple possession might constitute a criminal offence (Article 6).

The Convention also provides – under certain conditions – for corporate liability for the above-mentioned offences.

The Convention contains specific procedural rules about expedited preservation of stored computer data, production order, search and seizure of stored computer data, real-time collection of computer data and jurisdiction. General principles are set out concerning international co-operation, extradition, mutual assistance and spontaneous information. In an AmI world, countries will have to co-operate to deal effectively with criminal offences. However, some question such efficiency under the Cybercrime Convention and point out the unsatisfactory status of ratification and the problems with enforcement.

3.2.8.8 Data laundering

Companies are paying a lot of money for personal and group profiles, although their origin is not always very clear. As a matter of fact, the illegal origin (illegal collection) of personal data can be camouflaged via a large number of transactions and operations. This phenomenon is known as "data laundering". By definition, data laundering is a violation of data protection legislation, since it hides the fact that personal data were illegitimately processed. Persons and companies involved in or assisting data laundering should be subject to penal sanctions.

Especially companies are prone to participate in data laundering. A way to prevent data laundering could be an obligation on those who buy or otherwise

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

acquire databases, profiles or significant amounts of personal data to check diligently the legal origin of these data. Without checking the origin and/or the legality of the databases and profiles, one could consider the buyer equal to a receiver of stolen goods.

Another possibility is to apply the rules of money laundering in a similar way to data laundering, for example, by the obligation to notify the national data protection officer when, how and from whom personal data are acquired. Data laundering via large uncontrolled (commercial) traffic of individual profiles and personal data could become one of the "escape routes" in the struggle against data protection infringements. There are no clear provisions for this in criminal law, but there could be, making it a criminal offence to acquire obviously illegally collected personal data.

3.2.8.9 Location-based advertising and spam

Maruja receives lots of targeted advertisements. With new communication possibilities, location-based advertisements and spam grow to new levels. As she gets annoyed with advertisements, Maruja switches off almost completely, cutting herself off from potentially useful information.

Unsolicited electronic communications for the purposes of direct marketing is prohibited, although exceptions exist, for example, in an existing customer relationship. In principle, however, the Privacy & Electronic Communications Directive establishes an opt-in regime, implying the prior consent or wish of the subscriber (Article 13). Other obligations are that the identity of the sender may not be disguised or concealed and that each message must contain an electronic address so that the receiver can easily opt out.

The "unsolicited communications" chapter of the Privacy & Electronic Communications Directive may not apply in some situations. First of all, it will not protect the user against the advertisements for which he did opt in, even though his consent is being abused. In such a case, the user would need to exercise his opt-out right, as mentioned above (which still can lead to frustration and disappointment on the part of the user). Secondly, the article is about commercial communications (see recital 40), so that non-commercial communications fall outside the scope of Article 13. Moreover, the opt-in rule is applicable only to the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) and electronic mail for purpose of direct marketing.

But, in addition, in order to apply the opt-in rule, it must be a commercial "communication". A "communication" is defined in Article 2 (d) of the Privacy & Electronic Communications Directive as "any information exchanged or conveyed between a finite number of parties by means of publicly available electronic communications service. This does not include," continues the definition, "any information conveyed as part of 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."

One can argue that the opt-in obligation does not apply when the messages are sent to (displays or other embedded devices on clothing, like Maruja's blouse, or other devices that belong to) anonymous persons. In that case, the information cannot be related to an identifiable subscriber or user receiving the information. One can also argue that, if messages are broadcast to everybody who enters a certain area or walks in a certain park or street with his device on, this case falls outside the scope of the Directive as well: There is a constant broadcast in Elm Street and every person walking in Elm Street with his device on can be compared to a person switching his TV from channel X to channel Y.

United States case law has confirmed that pop-ups (small windows separately popping up when visiting a web site, often containing commercial information) do not infringe anti-spam law.[88]

Article 13 of the Privacy & Electronic Communications Directive also provides for an opt-out mechanism in some circumstances. When electronic contact details of consumers are obtained in the context of the sale of a product or a service, these electronic contact details may be used by the same entrepreneur for direct marketing of his own similar products or services, provided, however, that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use. The opt-out mechanism has several disadvantages. The data subject has to declare specifically that he does not want to receive these messages, which puts a burden on him. He might not know who sends the information[89] and he might have to opt out from a number of personalised message systems. When he opts out, he might also lose important information and services. This limits his freedom to opt out to a great extent. People are even considered suspicious when they decide not to use certain services. Some solution to the above-mentioned problems with location-based communication are foreseen by Article 9(2) of Privacy & Electronic Communications Directive which says that the user has to be able to temporarily refuse processing of location data using simple means and free of charge. That would allow the user to shield himself from location-based (commercial) communication, while still being able to receive other useful information. However, this provision does not protect users against broadcast advertisements, nor does it provide a solution for not losing other location-based information (e.g., "locate my friend" applications) when using the possibility afforded by Article 9(2) to protect oneself against commercial messages.

---

[88] Utah Court of Appeals, *Jesse Riddle* v. *Celebrity Cruises*, 30 December 2004. http://www.droit – technologie.org/1_2.asp?actu_id=1038)

[89] It should be mentioned, however, that the Directive on electronic commerce 2000/31/EC contains an information obligation in the case of commercial communication. The Directive states that, among other information requirements, natural or legal persons on whose behalf the commercial communication is made must be clearly identifiable (Article 6 (b)). As already mentioned, similar provisions facilitating opt-out are contained in Article 13 (4) of the Privacy & Electronic Communications Directive.

The **Directive on electronic commerce 2000/31/EC** also contains important provisions on commercial communications. Article 6 of the Directive obliges the provider of commercial communications, even when they are solicited, to ensure that commercial communications are clearly identifiable as such; to identify the person on whose behalf the commercial communications are made; to ensure that promotional offers and promotional competitions are clearly identifiable as such, and their conditions are easily accessible and presented clearly and unambiguously. Providing this information should allow users to understand the aim of the messages they receive and to distinguish useful from manipulated information. Article 7 of this Directive sets out additional conditions for unwanted commercial communications.

Service providers undertaking unsolicited commercial communications by e-mail should consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves. Consumers should be better protected against spam and unsolicited communications through enforcement. Opt-out registers seem to be insufficient and impractical.

Spam laws, spam filters and other mechanisms have not stopped spam, which already accounts for most of the traffic on the Internet today. Europeans confronted with spam have great difficulties in undertaking civil actions because they cannot find the spammer and, even if they were able to do so, they cannot prove the damage (which is indeed low, from an individual point of view) in a procedure which is too expensive.[90] In the United States, fixed civil remedies (e.g., US$10 per spam received) are built into laws of states such as Arizona, Arkansas, Connecticut, Illinois, Minnesota, New Mexico and North Carolina. Legal certainty should exist in the enforcement of spam law and in new methods and applications targeting people with commercial communications in an AmI world.

In the Distance Contracts Directive,[91] an opt-in rule (prior consent) is provided for use of faxes or automated calling systems, while an opt-out possibility for users must exist for all other means of communication through which distance contracts can be concluded.[92] The opt-in rule for unsolicited communication is important to ensure respect for the consumers' privacy. It should, however, not be limited to faxes and automated calling systems. Opt-out mechanisms for unsolicited communication are less effective.

3.2.8.10 An RFID-tagged blouse

Burglars "read" the blouse worn by Maruja. The blouse contains an RFID chip with information about the shop where it was bought. The thieves hack the shop's database

[90] But some actions have been successful. A small claims court in Colchester awarded £270 damages against Media Logistics UK for spamming after the complaint took on the company. See Lewis, Paul, "Court victory hailed as spam stopper", *The Guardian*, 28 December 2005. http//www.guardian.co.uk/uk_news/story/0,,1674316,0,0.html

[91] 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, 4 June 1997.

[92] Article 10 of Distance Contract Directive.

to find out where the buyer of the blouse lives. Because the blouse was borrowed from a friend, the burglars confront this friend when they break into the house.

The personal data contained and processed in the RFID-embedded blouse fall under the rules and conditions of data protection law which does not allow secret and unfair collection of personal data. The RFID tag that identifies the object links the purchase data that identify the subject, which is sufficient to regard information on the tag as "personal data".[93]

Moreover, when the burglars accessed the information in the blouse, they committed offences defined by the **Cybercrime Convention**, such as illegal access, possibly illegal interception. The Cybercrime Convention defines illegal access as "when committed intentionally, the access to the whole or any part of a computer system without right". Illegal interception is "when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data".

The **Council Framework Decision 2005/222/JHA** of 24 February 2005 on attacks against information systems[94] defines illegal access, data and system interference. Article 3 (illegal system interference) obliges Member States to "take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

It is important to have a common definition of these criminal activities, since they often have a cross-border dimension. The Convention gives participating countries the option to set extra conditions for described actions to be a criminal offence. This freedom limits harmonisation of Member States' laws.

The Council Framework Decision 2005/222/JHA obliges Member States to take measures to comply with the provisions of this Framework Decision by 16 March 2007. Thus, Member States are more bound by this instrument than by the Cybercrime Convention. 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 EU Member States.

It could also be argued that the RFID chip (hardware) and the embedded protection software were defective products, causing damage to Maruja, because they were easy to access while the user does not have any control over such access. This could bring the Directive on liability for defective products into play, as discussed above.

---

[93] However, it is not always clear what constitutes "personal data" in the context of RFIDs, and whether all RFIDs contain "personal data", which would trigger application of the Data Protection Directive. See also Chapter 5 on Safeguards and, in particular, section 5.3.4.

[94] 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.

3.2.9 Conclusions

This scenario depicts AmI vulnerabilities in the life of a typical family, in different environments – at home, at work and in a park. It indicates some of the potential benefits of AmI services but also shows dark aspects, including human failings in security measures, identity theft, loss of control, inadequate profiling, spyware and spamming, data laundering, illegal interception and so on. Additional legal measures will be needed to address some of these issues, but legal safeguards alone cannot fix all problems. Improved security measures will be necessary. Consumers will also need to adjust their behaviour, e.g., to be sceptical of special offers, to make sure their personal devices reflect their preferences, to be more conscious of what they can and should do to improve the security of the systems and services they use.

3.3 Scenario 2: A crash in AmI space

3.3.1 The scenario script

3.3.1.1 Introduction

Martin and Barbara Schmitt have lived for more than 10 years in an AmI-equipped alpine village specifically designed for senior citizens. For their age (Martin is 77, his wife is 75), both are healthy. Their daughter Heike lives in northern Germany. Heike sees her parents only once or twice a year, but maintains contact during the rest of the year by means of AmI.

In this scenario, the Schmitts are in a group of senior citizens touring Florence.

Scene 1: News from the police report: Senior citizen dies after bus accident

Florence – Twenty-four senior citizens were injured, one fatally, in a bus accident on a sightseeing trip on Friday afternoon.

According to Florence police reports, the bus was on a sightseeing trip with 46 senior tourists from Germany and Austria when for unknown reasons the traffic lights at a major intersection went to green for all directions. The bus driver avoided a collision with the oncoming traffic but knocked down some traffic signs, went off the street and finally crashed into a lamppost.

Fifteen of the passengers on the bus had minor injuries but nine were more seriously injured and had to be treated at the Careggi Hospital. Though the emergency service arrived quickly, the severe internal injuries of an 84-year-old woman from Austria remained undetected because she used an outdated health monitoring system. She died on the way to the hospital.

Heike Lengbacher-Schmitt is sitting in the subway on her way home when she suddenly receives two alarm messages on her personal wrist communicator (PWC). Her parents' health monitoring devices (HMD) issued the alarms, indicating that a critical situation had occurred.

Of course, Heike becomes concerned. She had picked up similar messages before from one of her parent's HMD, and in all of these instances things eventually turned out to be fine. But this was the first time she received alarms from both parents at once. Moreover, she knows that her parents are on a bus tour, making the situation even more worrisome.

Heike's attempts to call her parents are not successful. As she learned later that day, in an emergency situation, the HMDs by default block any incoming communications from people not directly involved in the rescue efforts in order not to disrupt the immediate rescue process. And during the examinations at the hospital, mobile communication devices are to be turned off.

Over the course of the next three hours, she leaves numerous messages at her parents' digital communication manager, urging her parents to return her calls as soon as possible.

In addition, Heike accesses her father's personal data storage. The system recognises her and, because she was granted comprehensive access rights beforehand, releases the travel information she requests such as her parents' itinerary, stopovers, etc. Eventually, she finds out that her parents are at the Careggi Hospital in Florence. After phoning the hospital, Heike is informed that her parents are receiving medical treatment.

After Martin Schmitt has been thoroughly examined, he is allowed to leave the emergency room and turn on his communication devices again.[95] *He immediately calls his daughter.*

Heike: Hello? Oh, it's you, dad. Thank goodness! Are you all right? How's mom? What happened?

Martin: Our bus had an accident, and your mom was slightly injured, nothing serious. She has a slight concussion and I have a few scratches. Nothing to worry about, believe me.

Heike: Can I talk to her?

Martin: Sorry, honey, but she's still being treated and the doctors said she should not be disturbed.

Heike: By the way, Aunt Anna called me just a few minutes ago. She was totally freaking out because she received the same alarm messages as me. Apparently she became so excited that her HMD even alarmed her doctor!

Martin: Oh no, I forgot to take Anna off the list of people to be automatically notified in an emergency. Please call her and try to calm her down. Listen, I want to go back to your mother. I'll call you later. Just wanted to let you know everything's okay.

As it is already past midnight when Martin finally leaves the hospital, he decides to send a video message to his daughter instead of calling her. In his hotel room, Martin sets up his mobile phone in front of him and starts recording his

[95] At the moment it is debated if wireless technology can be banned from hospital any longer or if "wireless tagging is 'inevitable'". Carr, S., "Wireless tagging in hospitals is 'inevitable': Prepare to be chipped …", silicon.com, 7 December 2004. http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

message. He also attaches a short clip showing Barbara in the hospital, saying a few words to reassure her daughter. Martin had ignored the ban on using mobile recording devices in the hospitals and filmed a short video-sequence of his wife anyway.

Dear Heike! As you can see, I'm absolutely fine. And your mother is recovering quickly. She will be released tomorrow morning. But let me tell you what happened from the beginning.

Scene 2: Travel preparation and check-in procedure for public transportation

Your Mom and I had completed travel preparations way ahead of time. So there was no need to get stressed out. And thanks to the travel-assistance procedure of the AmI environment in our home in Murnau, this time we even thought of recharging our PWCs and HMDs early enough to avoid losing "our identity" like on our last trip.

In Munich, I experienced an awkward situation after I located a former colleague of mine using the "friend-locator" function (LBS) of my PWC.[96] *I just wanted to say "Hi", but when I walked up to him, I was surprised to see that he had a good-looking, younger woman with him who obviously was not his wife. He blushed, mumbled a few words and disappeared in the crowd. It seems difficult to keep secrets these days …*

At Munich station, we met our old friends Brigitte and Peter as planned. The four of us proceeded to meet up with the travel group in the new bus terminal, just next to the station.

Alessandra, our Italian tour manager, introduced herself and welcomed us to the tour and we finally started to pass through the security gates in order to board the bus.

I guess I'll never feel comfortable with all these safety measures you have to endure when travelling: biometric ID verification,[97] *detectors for drugs and explosives, etc., especially if they reject you erroneously.*[98] *One of our fellow travellers, Michael from Baden-Baden, was denied access to the boarding area of the terminal, even though he had a valid ticket and had the receipt from his travel agent!*[99] *Apparently, some kind of data mismatch between his personal ID, the e-ticket and the information stored on the central server had caused the problem.*

The security personnel at the terminal were absolutely stubborn and unwilling to make an exception, despite several interventions by Alessandra and Peter, who is a good friend of Michael. The officials urged Alessandra to accept the situation

---

[96] Paciga, M., and H. Lutfiya, 2005.

[97] Bolle, R.M., J.H. Connell, S. Pankanti, N.K. Ratha and A.W. Senior, *Guide to Biometrics*, Springer, New York, 2004.

[98] Maghiros, I., Y. Punie, S. Delaitre et al., 2005.

[99] Schneier, Bruce, "Identification and Security", *Crypto-Gram Newsletter*, 15 February 2004. http://www.schneier.com/crypto–gram–back.html

and told her to leave without Michael. But they hadn't reckoned on the solidarity of the whole group – we made it unequivocally clear that we wouldn't leave behind a member of the group.

According to the law, Michael was obliged to receive a "possible risk status for an unlimited time" because he is causing more security risks than normal. He has to accept this "possible risk status", granted to him by the officer, which means that all his actions and movements are tracked and stored.

To make a long story short, it took another hour before Alessandra had worked out an agreement with one of the senior officials. The solution was that the tour manager and all passengers had to sign a statement discharging the bus terminal of any responsibility for possible damages that Michael might cause. Pretty ridiculous if you ask me, especially considering that once you leave the terminal, anybody can hop on the bus without any security checks at all!

Scene 3: Traffic supported by ambient intelligence

After a pleasant stopover in Bolzano, we continued our journey the next day. The ride through Upper Italy was uneventful. Some of us were watching on-demand videos or reading books on their portable screens.[100] *And Alessandra turned on the interactive tour guide of the bus that explains what we could have seen outside the bus if it had not been so foggy in the Po lowland. Instead, some videos of the scenery were projected onto the windowpanes.*

Later on, our bus driver managed to by-pass a major traffic jam on the highway near Modena. Well, actually he just had to follow the instructions he received on his on-board navigation system. We learned that the traffic monitoring system had detected a severe accident about 30 km ahead of us, and within seconds of the disruption of the traffic flow, a traffic warning was issued and an alternative route suggested.

Thanks to the intelligent filtering system, our driver was able to take the decision at the right moment without being distracted by too much information while driving.

Luckily, the bus company we were travelling with had subscribed to one of these expensive premium traffic information schemes. Many other people travelling in the same direction weren't as fortunate.

In Florence, traffic volume was pretty high, but considering the rush hour, we moved along quite smoothly. The electronic road signs told us that inbound traffic was given priority. In addition, our bus had permission to use the lane reserved for public transport. Paying tolls is always a pain, but these urban traffic management systems seem to pay off.

---

[100] Espiner, T., "Philips unfurls prototype flexible display", ZDNet UK, 2 September 2005. http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39216111,00.htm

Scene 4: Emergency situation

But then again, traffic management systems are far from secure: We learned later that the accident we were involved in was caused by a kid who had managed to hack into the Florence traffic management system.[101]

All of a sudden, cars coming from the right entered the junction at high speed. In order to avoid a collision, our bus driver pulled to the left and we ran into the central reserve, hitting all kinds of signs and objects. Finally, we crashed into a large lamppost and came to a brutal and sudden stop.

It took me a few moments to realise what had happened and to regain orientation. Your Mom was unconscious. So I checked her HMD immediately. The display indicated that an emergency call had already been issued. Thank goodness, all vital parameters such as blood pressure and pulse rate were okay.

I looked around and saw the mess we were in. You should see the camera images taken in the bus (as you know, the cameras in the bus record everything constantly), but they were not immediately available because the bus company gave commercial exclusivity to a television station. … So we have to wait until the police give us a copy, if we ever get one.

What I did not know was that some passengers were using HMDs that are not compatible with the Italian system. Thus, they were not able to download the health information of a couple of people on the bus and the semi-automatic rescue co-ordination centre assumed there were only 32 people on board and sent too few ambulances. This did not have severe repercussions since many of us were not seriously hurt.

The police, ambulances and fire brigade arrived rather quickly. The fire brigade, however, was not needed. It was called because the alarm signal stopped after three minutes due to a power shortage in the vehicle and the rescue centre interpreted this as an indication that the bus might have caught fire – the travel organisation will have to pay for this service, but who wants to grouse?

On their way, the paramedics had checked the medical records of the passengers and the HMD signals and set up a list of people with more serious injuries and those with private health insurance.[102] *Apparently, they were given priority treatment and transport to the hospital. Too bad we didn't opt for such insurance and had to wait for more than half an hour before being examined.*[103]

---

[101] In summer 2005, the US government outlawed the possession of "traffic signal-pre-emption transmitters" after hackers had used them to manipulate traffic lights. Poulsen, K., "Traffic Hackers Hit Red Light", *WiredNews*, 12 August 2005. http://www.wired.com/news/technology/0,1282,68507,00.html

[102] Michahelles, F., P. Matter, A. Schmidt, B. Schiele, "Applying Wearable Sensors to Avalanche Rescue: First Experiences with a Novel Avalanche Beacon" in *Computers & Graphics* 27, No. 6, 2003, pp. 839–847.

[103] Carr, Sylvia, "Wireless tagging in hospitals is 'inevitable'. Prepare to be chipped …", Silicon.com, 7 December 2004. http://hardware.silicon.com/storage/0,39024649,39126387,00.htm

My neighbour on the bus had two narrow escapes. He escaped from the bus crash without a scratch but he was almost given an injection just because he had picked up someone else's HMD and not his own.

But something really tragic occurred with Monika Klein, a nice 84-year-old lady from Salzburg. She was one of those whose health insurance refused to pay for an update of the HMD to the latest model; the paramedics had neither her patient record nor her current vital data. When one of the paramedics walked around and talked to those who were not on his automatically-produced list, she told him that she was not in pain, only exhausted. Because there weren't enough ambulances at the scene, they left her sitting on a bench next to the road. Since the introduction of HMDs, these guys depend too much on the technology. They are not even able to practise the simplest diagnosis. Otherwise they would have diagnosed that Mrs Klein had internal bleeding. I heard that when they finally decided to take her to the hospital, one of the last to go, she suddenly lost consciousness and passed away before the ambulance reached the hospital.

Scene 5: Ambient intelligence and medical care

After we arrived at the hospital, I had a fierce argument with the lady at the reception who complained that she was not able to get full access to my health and insurance record. The doctors, she said, were unable to help me if I wouldn't disclose my complete data to the hospital.

Heike, you probably remember that I had forbidden the health services to give away certain data because I had been spammed with so many drug adverts last year after that scandal over the illegal trading of personal health data. I saw no necessity to give the hospital complete access since I only had some scratches. However, I had to sign a statement that the hospital is not liable for any impairment resulting from their treatment.

I really wonder if the benefits of automated health care are really worth this mess. I promise to keep you posted. Say hi to George and hug the kids for us!

Bye for now!

3.3.2 Analysis

3.3.3 The context

The scenario presents three different environments that reveal possible weaknesses in public or semi-public infrastructures and the trade-off between economically efficient procedures as implemented in AmI services and the variety of individual needs.

Citizens must be able to trust and rely on unfailing operation of these infrastructures – especially for vital functions. Fair access and user-friendliness are needed to prevent an ambient intelligence divide. While equal and fair access is the basic requirement for public utilities, user-friendliness is a critical consideration regarding actual use of AmI services. In this respect, disabled and elderly people have special requirements that need to be factored in.

Scene 1: Framework situation: AmI-supported communication

This scene depicts communication links between a senior citizen and his daughter who lives far away.[104] Synchronous and asynchronous communication using text, phone or video from basically any location is assumed to be standard. For both the father and daughter, these communication possibilities are part of everyday life, including receiving all kinds of information automatically issued by personal agents such as HMDs. In an emergency situation, however, automatic alerts can actually cause more harm than good unless they inform the recipient adequately about the situation.

Scene 2: Travel preparation and check-in procedure for public transportation

This scene shows the senior citizens' preparations for their bus trip to northern Italy. The scenario assumes that the couple remain healthy and active up to an advanced age and are supported by AmI technology in their daily activities.[105] AmI-enabled services can remind users not to forget important things (like an HMD).

In the aftermath of 11 September and other terrorist attacks in recent years, boarding public transportation usually involves more or less extensive procedures of identification, control and surveillance. People have to get used to it. Flaws in technologies and/or applications periodically lead to nuisance and sometimes even to open insubordination when results are *obviously* faulty and authorities deny services. An open issue in this respect is the trade-off between public security and individualism.[106]

Scene 3: Traffic supported by ambient intelligence

This scene explores the delicate balance between market- and supply-driven approaches to many new mobile services enabled by the availability of personal information in fields that are considered public utilities today. This development may result in a decreasing relevance of free and publicly available services and in a growing disparity between those who can afford the benefit offered by ambient intelligence and those who cannot.

---

[104] As presented in Cabrera Giráldez, M., and C. Rodríguez Casal, "The role of Ambient Intelligence in the Social Integration of the Elderly" in G. Riva, F. Vatalaro et al. (eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human – Computer Interaction*, IOS Press (Studies in New Technologies and Practices in Communication, 6), Amsterdam, 2005, pp. 265–280.

[105] See, for instance, Cabrera Giráldez and Rodríguez Casal, 2005, and Korhonen, I., P. Aavilainen and A. Särelä, "Application of ubiquitous computing technologies for support of independent living of the elderly in real life settings" in *UbiHealth 2003: The 2nd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications*, Seattle, 8 October 2003.

[106] See, for instance, Fujawa, J.M., "Privacy Made Public: Will National Security Be the End of Individualism?", *Computers and Society*, 35, No. 2, 2005.

Extrapolating from current developments, we can assume that bus drivers (like other traffic participants) will be supported by numerous AmI applications to make driving more efficient and less stressful. Avoidance of traffic jams will be one of the most popular applications (which would not be surprising considering the experiences made in the late 20th century). As some of these services lend themselves to business models, quality and speed of traffic information services differ according to the price consumers are willing to pay.

AmI technology also supports passenger activities such as individualised entertainment (video, music, interactive games) and "edutainment" like an electronic tour guide, which gives explanations about the scenery outside (augmented by videos and other multimedia).

AmI technologies will be an important element in large cities' efforts to come to grips with unbearably high traffic volumes and recurrent congestion. Traffic management systems constantly monitor and manage traffic flows according to predetermined parameters through centrally controlled traffic signs, traffic lights and other electronic means of traffic management. Certain vehicles such as ambulances, streetcars, buses and taxis are granted priority rights. Traffic management systems can be deceived, however, by illegal hardware and software.

Scene 4: Emergency situation

Public authorities have established AmI-supported emergency systems with automated information chains from the individual person and vehicle to the emergency services (police, ambulances, hospital).[107] This has become a complex system, since heterogeneous actors and systems have to communicate seamlessly. Given the fast development of technology, different national standards and health systems, this system remains imperfect – services cannot be offered to all citizens in the same way. In addition to the problems associated with operating efficiency, health and emergency services become increasingly differentiated from basic to premium services, creating an "AmI divide". For whatever reasons (e.g., because they are using older equipment, live in regions without technical coverage, or even have opted out), people who remain outside the system are at risk of not being provided with the most basic services.

As for other applications, AmI-enabled emergency systems may be driven by market forces making differences between people who can afford a premium service and those who cannot. While this is already taking place in the existing health insurance system, it is a sensitive issue who is actually driving the development: the insurance companies and health care suppliers who are under constant pressure to act economically and efficiently or citizens (represented by the government) who set the rules and define boundaries for AmI health care services.

[107] Savidis, A., S. Lalis, A. Karypidis et al., *Report on Key Reference Scenarios*, 2WEAR Deliverable D1, Foundation for Research and Technology Hellas, Institute of Computer Science, Heraklion, 2001.

In addition, identities can easily be mixed up if the link between a person and his/her personal device is dissociated (e.g., by picking up the wrong HMD).

Scene 5: Ambient intelligence and medical care

This scene reveals vulnerabilities like those in the emergency situation. Hospitals ask for a complete disclosure of health information (regardless of the need for the actual treatment) in order to be on the safe side and avoid liability. This raises a question about who is in control of the system and who establishes the rules that apply to denial of services.

In order to reduce possible interference with medical procedures and to protect patients' privacy, all mobile communication devices are required to be turned off within hospitals.

3.3.4 AmI technologies and devices

This scenario makes reference to several AmI technologies:

- Sensors and actuators
  - Embedded in the environment and in objects and attached to people, such as an impact sensor for accident detection and body sensors measuring the vital parameters of the elderly (or people with health risks)
  - Detectors of drugs and explosives
  - Positioning
  - Biometrics
- Interfaces
  - Portable screens
  - Augmented reality displays (such as bus windows)
- Intelligent algorithms for
  - Priority-based traffic routing
  - Routing of network traffic in emergency situations
  - Processing of health data in real time
  - Detection of persons with highest health risks or best insurance
- Communications networks enabling seamless service by heterogeneous devices with or without central control providing greater coverage (especially for emergency communication):
- (Personal) Health Monitoring Devices (HMDs), which are health-related personal intelligent devices and which could be combined with other multifunctional devices such as Personal Wrist Communicators.

3.3.5 AmI applications

Scenario 2 refers to various AmI-enabled applications including the following:

- *Personal communication management system*, like that described in ISTAG's "Dimitrios Scenario",[108] controls the communication of the elderly couple based on the context, e.g., it denies communication in the emergency when communication with the authorities has priority and at the hospital where mobile communication devices are not allowed. On the other hand, it proactively sends messages to family members and recognises people close by ("friend locator").
- *Support system for elderly people* helps to enable an independent life to an advanced age. This system reminds users about tasks to be done and objects to taken with them. When coupled to a health monitoring system, it also supports a healthy lifestyle.
- *Check-in and security procedures* for public transportation are technically integrated to a large extent, combining access controls with identification procedures (supported by biometrics and central databases) and security protocols. If operating accurately, the system speeds up regular check-in procedures and helps to detect potential security risks.
- *Personal health monitoring systems* survey vital parameters of people with certain risks such as high blood pressure or diabetes. The collected data can be used either by a physician for routine examination or in an emergency. The personal health monitoring system may be linked to a health insurance database and a communication system.
- *Public traffic management systems* collect information about the current traffic and support road users either collectively or individually. The business models may vary from free public information to pay-per-advice models.
- *Automated emergency alarm systems* can detect accidents and the urgency of the situation (especially if coupled with the personal health monitoring devices of the drivers and passengers). The rapid alarms and automated requests for assistance improve the quality of the medical system and help to reduce traffic casualties.
- In a *seamless medical information system*, all relevant information is collected, including personal medical history items such as prior illnesses, treatments and medication as well as up-to-date vital information and information about health insurance.

3.3.6 Drivers

Each of the AmI technologies mentioned in the scenario has been driven by a set of two or more interdependent factors. Analytically, the following drivers can be distinguished:

[108] ISTAG, Scenarios, 2001.

- *Political* – The introduction of some of the most important AmI applications in the scenario has largely been driven by political objectives such as reducing the risk of terrorism (security), improving the efficiency of the health care system (emergency), and the improvement of the traffic situation in urban areas (public infrastructure).
- *Commercial* – Numerous AmI services such as the "friend-locator", multimedia applications on the tour bus, individually tailored traffic information and automated communication links are primarily driven by profit motives and the (successful) development of business models.
- *Diffusion* – Especially in mass consumer markets, high penetration levels of basic communication technologies constitute an important vantage point for the demand for complementary services such as video-based communication or automated and personalised information exchange.
- *Accountability* – Both the boarding procedures at the bus terminal, which proved to be quite humiliating for one of the group members, as well as the fact that hospital patients are required to disclose their complete personal health data are based on the institutions' objective to reduce liability as far as possible.
- *Illegitimate personal advantages* – As AmI technologies regulate access to scarce goods, people may be motivated to seek personal advantages by circumventing standard procedures and/or by using technical solutions to deceive the system (in the scenario, a young person hacks into the traffic management system). Perpetrators might take into account possible hazardous consequences (because they seek to cause those consequences) or they might not (because they are ignorant of the consequences).

3.3.7 Issues

In view of the above-mentioned vulnerabilities of ambient intelligence in travel/mobility and health care applications, we can identify certain issues that are critical for AmI applications that rely on large-scale public infrastructure and have largely the character of a public utility:

3.3.7.1 Dependence

Automated alerts are not necessarily beneficial – they may even cause more confusion because alerts reach the addressee immediately, but direct communication with the victim is often no longer possible.[109] The promise of permanent accessibility leaves the user helpless when communication is needed but not possible.

[109] Savidis et al. assume in their scenarios that the personal communication device is deactivated for public communication in order not to disrupt emergency relief activities.

3.3.7.2 Privacy

What is the necessary degree of disclosure of information? In a normal situation even the disclosure of simple data (e.g., location) may violate privacy, whereas in other cases, the revelation of more information of the same kind may be warranted. Thus, the degree of information disclosure depends on the person, context and situation, which poses a challenge for the design of adequate communication rules.[110]

3.3.7.3 Loss of control

If certain activities rely on the proper operation of technical systems, a feeling of uneasiness and loss of control may occur if it is not transparent to the citizen why a certain decision is made, especially when common sense suggests a different decision.

3.3.7.4 Risk and complexity

If AmI systems that are vital for the public (such as in emergencies) are known to be vulnerable or that do not cover the whole population, a "conventional" back-up system, which provides at least a basic level of service, is needed.

3.3.7.5 Safeguards

Responsibility is moved to the weakest link in the chain, normally the citizen. In cases in which users do not adapt fully to the system requirements (e.g., provision of data), a liability may be generally refused – even if it has nothing to do with a certain damage or harm.

3.3.7.6 Exclusion

Services regarded as public utilities today may become commercialised tomorrow. Even if the common welfare is increased, there is a risk of more inequality and even a loss of benefits for certain social groups.

3.3.7.7 Identity

The loss and/or confusion of identity may not only be the result of malicious identity theft, it can also occur by mistake if the identification of a person is merely based on a detachable personal device.

---

[110] This issue is discussed extensively in Waldo, James, Herbert S. Lin and Lynette I. Millett (eds.), *Engaging Privacy and Information Technology in a Digital Age*, National Academies Press, Washington, DC, 2007. http://books.nap.edu/openbook.php?isbn=0309103924.

3.3.7.8 Crime and complexity

Complex and distributed technical systems may offer new opportunities for illegal activities. This not only applies to property offences and terrors, but also to misdemeanours and regulatory offences as well. Especially in those cases in which sensitive elements of the public infrastructure (e.g., traffic management) increasingly rely on AmI technology, even minor violations of the rules can unintentionally cause severe damage.

3.3.8 Legal synopsis

3.3.8.1 Bus accident caused by hacker

The traffic accident in Scenario 2 is caused by a kid who illegally used software for priority vehicles like ambulances and police cars. The scenario raises interesting questions about who is liable and to what extent, since many actors are involved: the kid who hacked into the traffic management system, the developer of the hacking tools, the traffic system controller, service providers, the bus driver and still others. The scenario also raises question about the applicable jurisdiction for prosecuting those liable.

Criminal law aspects

Currently, there is no binding European regulatory framework determining jurisdiction in criminal matters. Member States are free to choose their own rules. The rule of territory is basic: states incriminate actions that happen on their territory. The notion of territory is, however, open to interpretation. Many Member States broaden their jurisdiction by using expansive criteria such as the criterion of ubiquity. The result is that for transborder crime, several Member States find themselves competent at the same time for the same facts. This process is not a process of legislation, but of case law.

There is a tendency in the case law of national judges to interpret the principle or ground of territorial jurisdiction extensively. Belgian judges, for example, are not, except for explicit statutory provisions, competent in extraterritorial cases. Legal practice shows that judges give great leeway to Belgian legal authorities when crimes are committed outside Belgium territory but impinge on Belgium interests. The legal situation in Belgium and the Netherlands, and a country such as Chile that also belongs to the civil-law tradition is very similar. In all these countries, there are several accepted theories, criteria or answers to the *locus commissi delicti* question, namely, the question to what extent a wrongful act can be considered to fall within the territorial jurisdiction of a state. Within the Dutch and Belgian traditions, the following accepted criteria are applied:

- Activity criterion – the territory where the activity took place is the relevant one
- Criterion of the instrument of the crime
- Criterion of the constitutive consequence
- Ubiquity criterion – the *locus delicti* is every country where one of the constitutive elements of the crime can be located; thus, an offence may fall within the jurisdiction of more than one country.

Unlike in Germany and France, neither the Dutch nor the Belgian Criminal Codes contains a real choice for one of these criteria; the issue is left to the courts. An analysis shows that whatever criterion is applied, it is almost always easily possible for a judge to declare himself or herself competent and to hold that the events took place on "his" or "her" territory. The ubiquity criterion, in particular, by now the most successful criterion within the civil-law tradition, enables a flexible approach towards the *locus commissi delicti* question. It allows countries to prosecute persons spreading computer viruses or racist information from computers abroad, or persons who "call" in by telephone from abroad when this conversation forms the starting point for a crime. The flexibility of the ubiquity criterion explains without any doubt the total absence of jurisdiction provisions in the Belgian and Dutch Computer Crime Acts.

To avoid conflicts of jurisdiction, an international solution is preferable. Currently, there is no such thing as a stringent set of rules with regard to determining territory. A small paragraph in the Cybercrime Convention tries to remedy this conflict by imposing a guideline that "the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution".[111] A bit firmer is Article 10 paragraph 4 of the **2005 EU Framework Decision 2005/222/JHA on attacks against information systems**, requiring the Member States concerned to co-operate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. "To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate co-operation between their judicial authorities and the co-ordination of their action. Sequential account may be taken of the following factors:

– The Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2
– The Member State shall be that of which the perpetrator is a national
– The Member State shall be that in which the perpetrator has been found."

Although these guidelines are not legally binding, there is some wisdom in them. Future experiences will indicate whether more stringent rules are needed.

It is also important to focus on the different possible defendants. The hacker can be difficult to track. He commits criminal offences defined in the Cybercrime Convention, such as "illegal access", "illegal interception", "data and system interference" and possibly "computer-related fraud". The producer, seller or distributor

[111] See Article 22 of the Cybercrime Convention.

of hacking software might also fall under the scope of the Cybercrime Convention which provides for criminal offences including the misuse of devices, i.e., the intentional production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing an illegal access or interception or a data or system interference. Simple possession of such devices might also constitute a criminal offence (see Article 6 of the Cybercrime Convention).

Both the Cybercrime Convention and the Framework Decision 2005/222/JHA provide for the criminal liability of legal persons. Article 8 of the Framework Decision obliges each Member State to take the necessary measures to ensure that legal persons can be held liable for offences defined in a framework decision, also when committed due to lack of adequate supervision by a person under its authority. Article 9 contains specific penalties for legal persons.

Determining the applicable jurisdiction in criminal affairs is still a complex affair, waiting for an international solution.

Civil law and liability aspects

In the scenario, a number of service providers are involved in the accident, such as the traffic light network provider/operator. The traffic management system company had to guarantee that its system was sufficiently protected against hacking attacks. Since a minor was able to hack into the system, the question arises whether the company did enough in that respect.

It will be difficult to determine which of the various service providers involved in the traffic management system should be held responsible for the security problem. Normally, the person harmed by the security failure would have to find the specific provider who did not provide sufficient protection and to prove that this provider committed the fault, which caused the specific damage. This is difficult to prove. The strict liability regime under the Directive on liability for defective products,[112] however, allows the victim only to prove that the product (here the traffic management system) was defective and that it caused a damage. Since it was relatively easy for a hacker to access the system, the condition of proving defect might be fulfilled. Moreover, the Directive on liability for defective products contains rules that allow the victim to react against the supplier of the defective good, when the producer cannot be found. When the damage is caused by defects in the products or services of different suppliers, Article 5 makes it possible to claim all of the damage from one of the suppliers. This is important since it would be difficult for the victim to prove to what extent the different producers are responsible for the damages and to act against every producer involved. However, the Directive is not applicable to services.

As far as the European legal framework for liability is concerned, harmonisation at EU level is very limited. Thus, the national law will apply in most cases. However, some specific provisions on the liability of electronic service providers

[112] See section 3.2.8.3. above for more on strict liability under the Directive.

have been established in the Directive on electronic commerce.[113] This Directive limits the liability of intermediary service providers in three specific situations. Article 12 provides that in case of mere conduit (the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network), the service provider is not liable for the information transmitted. In the case of "caching" (i.e., when an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service), the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making transmissions of information to other recipients more efficient upon their request. In the case of "hosting" (i.e., when an information society service is provided that consists of the storage of information provided by a recipient of the service), the service provider is not liable for the information stored at the request of a recipient of the service. Liability is excluded in such cases, unless certain conditions are broken.[114] Article 15 provides that the intermediary service providers have no general obligation to monitor the content of the information transmitted.

The exceptions to the general liability rules apply only in the case of transmissions of information via a network. The exceptions will not be applicable when a system malfunctions because of a security flaw.

The law on liability is only partially harmonised on the European level (e.g., by the Directive on liability on defective products). Thus, liability is mostly regulated by national laws of the Member States. The question then arises which Member State's laws are applicable to the liability cases arising from the cross-border situations.[115] In the case of the accident in this scenario, we might have to deal with both, the extra-contractual liability (e.g., of the hacker or the traffic management system company) and the contractual liability (e.g., also of the traffic management system company).

As far as the contractual liability is concerned, the law applicable is indicated by the **Rome Convention on the law applicable to contractual obligations**.[116]

According to the Convention, the parties to the contract can choose which law will be applicable (Article 3 of Rome Convention) under the contract. Usually, the service providers impose the choice.

If the law applicable to the contract has not been chosen by the parties, the contract is governed by the law of the country with which it is most closely connected. The Rome Convention in Article 4 contains the presumption that the contract is most closely connected with the country of habitual residence (or central administration) of the party who is to effect the performance of the contract. Specific rules cover the carriage of goods. An AmI service supplier could have his habitual residence or central administration anywhere in the world and he could choose this place based on how beneficial the law is for him.

---

[113] Directive 2000/31/EC, pp. 0001–0016.

[114] See Articles 12–14 of the Directive on electronic commerce.

[115] On private international law issues (applicable law, jurisdiction), see section 5.3.11.2.

[116] 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.

There are, however, exceptions to these general rules in case of specific contracts such as consumer contracts and individual employment contracts.

Article 5 of the Rome Convention deals with consumer contracts. It reiterates the principle that consumers cannot be deprived from their national consumer protection by the choice of law made in a contract. The consumer enjoys the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence, though under conditions: "(1) if in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract, or (2) if the other party or his agent received the consumer's order in that country, or (3) if the contract is for the sale of goods and the consumer travelled from that country to another country and there gave his order, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy." Article 5, however, does not apply to a contract of carriage or for the supply of services where the services are to be supplied to the consumer exclusively in a country other than that in which he has his habitual residence. It shall, however, apply to a contract that, for an inclusive price, provides for a combination of travel and accommodation. This article is clearly built on the notion of habitual residence. In an AmI world, however, the notion of habitual residence might be flexible, which might make it difficult to apply these rules.

If the bus driver made a mistake, he might be liable towards his employer. Presumably both are situated in the same country, Germany, so German law would be applicable. If not, Article 6 of the Rome Convention contains specific rules on labour contracts. The European Union has recently adopted a regulation which unifies the rules on the law applicable to non-contractual obligations, the so-called Rome II Regulation.[117] The basic rule under the Regulation is that the law applicable should be the law of State where the direct damaged occurred (*lex loci damni*).[118] However, the Regulation allows for exceptions to this general rule. Such "escape clauses" seek to provide a more adequate solution in cases when the tort or delict is mostly connected with the country other than the one of the *lex loci damni*. This will be the case when both parties have their habitual place of residence in the same State. Moreover, if it is clear from the circumstances of the case that the tort or delict is manifestly more closely connected with the law of the country other than that of the *lex loci damni* or of habitual residence, the law of this other country should apply.[119]

Special rules apply in the case of some specific torts or delicts, e.g., in the case of product liability or in the case of infringements of intellectual property.

---

[117] 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

[118] Article 4 (1) of the Rome II Regulation.

[119] Article 4 (3) of the Rome II Regulation.

The parties can choose the law by agreement, though some limitations are provided.[120]

The Rome II Regulation excludes from its application a number of fields, inter alia, the law on companies and non-contractual obligations arising out of the violation of privacy and rights relating to personality, including defamation.[121]

The Regulation shall apply from January 2009.

The competent court in this scenario would be determined by the **Brussels Regulation**.[122] As in the case of applicable law, the parties have the possibility to determine in their contract which courts will be competent (Articles 23 and 24). The basic principle of this Regulation is that a defendant can be sued in the Member State of his domicile (Article 2). If the defendant is domiciled outside the European Union, this Regulation will not provide a solution for problems of jurisdiction (Article 4). In such situations, national legislation will determine the adequate forum. Article 2 has another disadvantage. When a user wants to sue an AmI services supplier, the service supplier will have the advantage of being sued at home. He might determine his domicile to ensure a beneficial jurisdiction.

In addition to this general principle, the Regulation contains a number of special jurisdiction rules, including those applicable to contracts, tort, and consumer and labour contracts. In matters relating to a contract, a person may be sued in the court of the place of the performance of the obligation in question (Article 5). In an AmI world, it will be difficult to determine the place of performance. In a certain sense, the contract is performed worldwide and this does not allow one to determine the competent court. Article 5 section 1 (b) specifies that in the sale of goods or services, this term should be understood as the place in a Member State where, under the contract, the goods are delivered or services provided (or should have been delivered/provided). In an AmI future, it might be difficult to determine where the goods or services were delivered and thus difficult to determine one single competent court. This scenario provides a case in point, i.e., a tour bus and its customers travelling around different countries.

The court competent to deal with extra-contractual issues, such as the liability of the hacker and the traffic management company towards the users, is the court of the place where the harmful event occurs (Article 5(3) of the Brussels Regulation).[123]

The damage caused by the hacker is not limited to Italy. Hacking is a criminal offence and Article 5(4) of the Brussels Regulation provides that a civil claim for damage or restitution which is based on an act giving rise to criminal proceedings

---

[120] Article 14 of the Rome II Regulation.

[121] Article 1 of the Rome II Regulation.

[122] 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.

[123] See also ECJ, Case 21/76 *Bier* v. *Mines de Potasse d' Alsace* [1976] *ECR* 1735, where the European Court of Justice stated that the place where the harmful event occurred should be understood as the place where the damage occurred or the place where the event having the damage as its sequel occurred.

can be brought in the court seized of those criminal proceedings, to the extent that that the court has jurisdiction under its own law to entertain civil proceedings. Since several persons might be coresponsible for the accident, there could be several parallel proceedings. Since this would make the issue more complex and expensive for the parties, Article 6 provides for the possibility of consolidating claims so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings, in the court of domicile of any of the (many) defendants. This allows the plaintiff to sue the different defendants before one single court. However, not all claims from the same factual situation may fulfil conditions set up by the Article 6. To offer an extra protection to the consumer, Article 16 of the Brussels Regulation provides that: "A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled." The bus customers can start proceedings in their own courts, which can be an important advantage. Provisions on the jurisdiction for consumer contracts apply when both parties are domiciled in EU Member States. However, the jurisdiction may also be established if the dispute arises out of the operation of a branch, agency or other establishment of the dependent in the Member State.[124] Despite such provisions broadening the scope of application of the Regulation, a substantial number of businesses offering services to EU consumers stay outside the reach of the Brussels Regulation.

Specific jurisdiction rules are provided in case of individual employment contracts.

3.3.8.2 Lack of interoperability

Seniors are involved in the accident while travelling through Italy. A woman dies because her health monitoring system is not compatible with the local health network system and her injury is not detected in time. In an AmI world, interoperability is crucial.

To ensure that information society systems and networks are compatible, international standards are created. An important legal instrument to ensure the creation of uniform standards and technical regulations is the **Directive on technical standards and regulations**,[125] which regulates some aspects of standardisation in the Union. It provides that national authorities and the European Commission should inform each other about new initiatives in the field of technical standards and norms (Articles 2–4). This should guarantee the necessary level of transparency between

[124] Article 15(2) of the Brussels Regulation. It is possible that, in the future, the localised web page would be understood as the establishment in the undertaking of this particular provision. See Schaub, Martien, "European legal aspects of E-Commerce", *Europa Law*, Groningen, Netherlands, 2004, p. 147.

[125] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, *Official Journal* L 204, 21 July 1998.

the different competent bodies in the European Union. The Directive also established a standing committee, consisting of representatives of the Member States and, as chairman, a representative of the Commission, to ensure that the national interests of Member States are taken into consideration in new standards initiatives. Technical standards and regulations could, however, constitute barriers to the free movement of AmI services. That is why they are only allowed "where they are necessary in order to meet essential requirements and have an objective in the public interest of which they constitute the main guarantee". The Directive foresees a detailed information procedure that aims at meeting those criteria.

Member States also have the obligation to ensure that their standardisation bodies do not take any action that could prejudice European standardisation initiatives. When a Member State wants to create new technical regulations, Articles 8 and 9 provide detailed information and co-operation procedures, to ensure compatibility with EU and other national initiatives.

All of this should guarantee that the European Commission and the Member States work together in the most efficient way and are aware of each other's initiatives. If it were to work optimally, all national systems should interoperate and be based on compatible standards and regulations. Similar standardisation initiatives exist at the international level.[126] The issue of standardisation and interoperability is of major importance for AmI applications. When standards have been achieved, stringent regulations should be imposed, at least on sensitive AmI services such as health and general alarm systems, to ensure compliance with the standards and regulations throughout the European Union.

Regarding the important – for AmI, necessary – interoperability of software programs, the **Software Directive**[127] obliges Member States to protect computer programs by copyright and asserts that only a specific expression and not the underlying ideas and principles of any element of the computer program are protected. Some limited exceptions to the exclusive right of the rights-holders are foreseen.[128] The Directive also contains a provision on decompilation in order to

---

[126] Important standardisation initiatives regarding privacy have been taken by the Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS) of the World Wide Web Consortium seeking to develop a single vocabulary through which a user's privacy preferences and the site's practices are articulated, enabling the negotiation of privacy requirements between them, and to provide for secure transmission of a standard profile of personal data. See WP 29 Opinion 1/98 on Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS), adopted 16 June 1998.

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

[128] Exceptions to the exclusive rights of the copyright holders are: (a) reproduction, translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, where these acts are necessary for the use of the computer program (…) including for error correction; (b) making a back-up copy; (c) to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program (Article 5 of the Directive). These exceptions seem to be insufficient to allow the free use of computer programs required in an AmI world. Also, they can only be invoked by the lawful acquirer, which is a vague term and which could lead to important restrictions.

avoid a situation where copyright could hinder interoperability. Article 6 says that the authorisation of the rights-holder shall not be required where reproduction of the code and translation of its form are indispensable to obtain the information necessary to achieve interoperability between an independently created computer program and other programs, subject to conditions, inter alia: these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so, and these acts are confined to the parts of the original program necessary to achieve interoperability. Information acquired in accordance with these provisions should not be used for goals other than to achieve the interoperability, and should not unreasonably prejudice the rights-holder's legitimate interests.

There has not been much case law based on this Directive. A Dutch court, however, recently decided that the Dutch copyright law (implementing the Software Directive) obliges application service providers to copy the data, which are processed in one program, to a script that makes it possible to process the same data in another program. In this case, a school wanted to change the software program without losing the data, and the Court decided that the first software provider was obliged to make a script that translates the data into the other program.[129] There have been many criticisms of this judgment because the Software Directive focused on the interoperability of software, not the interoperability of data. But this exactly highlights an interesting issue for AmI: to what extent are licensors of software programs compelled to deliver the data, processed in their programs, in a script that allows processing the data in another program? This is also important from the data protection perspective, in particular for the data subjects who, according to Article 12 of the Data Protection Directive, have an access right to the data, namely, a right to communication "in an intelligible form of the data undergoing processing and of any available information as to their source". This is also important for anyone who needs to use (personal) data and other information processed in any other processing system.

Another case that relates to interoperability is the Commission Decision of 24 March 2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft) in which the Commission decided that on the basis of Article 82, Microsoft abused its dominant position "by deliberately restricting interoperability between Windows PCs and non-Microsoft work group servers, and by tying its Windows Media Player (WMP), a product where it faced competition, with its ubiquitous Windows operating system". The Commission imposed a fine of €497 million and the following remedies on Microsoft: (1) the obligation to offer an unbundled version of Windows (a version of Windows without Windows Media Player) ("unbundling of WMP" remedy); (2) the obligation to make available to its competitors certain technical interface information necessary to allow non-Microsoft work group servers to achieve full interoperability with Windows PCs; this having to be done on reasonable and non-discriminatory terms ("interoperability remedy"). The findings of the Commission were upheld by a judgment of

[129] Rb. Leeuwarden 25 May 2005 Openbaar onderwijs Zwolle/Pendula. http://www.rechtspraak.nl.

the Court of First Instance in September 2007.[130] Such similar, specific interoperability remedies might be necessary in AmI. Lack of interoperability can preclude individuals from obtaining the services they wish to enjoy and result in serious harm to them, as shown in the scenario.

There is no doubt that the technology can facilitate the life of the individuals. Well functioning emergency systems may save lives. On the other hand, creating standards is costly and raises the question of who will bear the costs of such developments. Companies might be less willing to contribute to the development of standards because they will not receive the expected return on investment and might still be liable for the good functioning of their standardised product. In the scenario, a woman was not provided with a compatible device. In more extreme situations, a whole country or continent may not be able to afford these technologies. This highlights the digital divide issues of affordability and discrimination, which may be reinforced by the introduction of new and costly technologies. Sensitive AmI services and technologies could be treated as public or universal services, which should be available to all. The topic is high on the European agenda. There have been research activities relating to accessibility, under the eEurope 2002 Action Plan.[131] The Council also adopted a resolution on e-accessibility in December 2002. The eEurope 2005 Action Plan[132] seeks to ensure that peoples with disabilities and other disadvantaged groups can participate in and have equal access to major innovations in online public services, covering e-government, e-learning and e-health, and to create a dynamic, accessible e-business environment.

The **Universal Service Directive**[133] recognises the need to provide universal services to citizens at an affordable price. Such affordable price is set within each Member State and may depart from those resulting from market conditions. Member States are obliged to ensure access to those services (at affordable prices) to all end-users. However, the scope of the Directive is limited to electronic communication networks and services (and a few other services, e.g., the Directive mentions access to public pay telephones and uninterrupted access to the emergency services free of charge). They include the guarantee that at least one undertaking provides access to the public telephone network following a reasonable request of the quality allowing speech and data communications (including Internet access), and takes into account prevailing technologies available to the majority of end-users. Member States may decide to make additional services publicly available on their own territory.

The Directive makes provision for a review of the services in light of economic, social and technological developments. Any change of scope in universal services is subject to availability of services to the substantial majority of the population,

[130] Case T-201/04, Microsoft [2007].

[131] http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf

[132] http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf

[133] 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, *Official Journal* L 108, 24 April 2002.

and must consider whether the lack of availability of such services creates the risk of social exclusion of those who cannot afford them. Changes in the scope of the universal services or in the technology cannot produce disproportionate financial burden on the undertakings providing services. Costs of such changes must not fall unfairly on consumers in the lower income brackets.

The scope of this Directive is limited and obviously not adjusted to the AmI environment. Nevertheless, consideration should be given to vital AmI services and technologies, such as those that may play an important role in future emergency service being available to all individuals in a non-discriminatory, reasonable and safe way.

3.3.8.3 Access refusal as a result of data mismatch

One of the seniors, who wanted to participate in the journey, was refused transport because of problems with his identification.

In the AmI world, new tools and methods for identification will be developed, manufactured and implemented. In the scenario, the public transport relies on biometric identification. No identification system, however, is perfect; each is subject to errors to a greater or lesser extent. The data controller takes the risk for and bears (some of) the consequences of the errors. Today, errors seem to be accepted as a fact of life, however undesirable, as they can cause harm to people, especially when identification systems become much more prevalent than they are today.

The problem spotlighted by this scenario is caused by a mismatch between personal data held by the individual and information held on a central server. We do not know why such an incompatibility of information occurred. The information on the central server has been collected, acquired and processed under the responsibility of the data controller. It might be difficult, however, to identify who is the data controller in such a situation, and thus who is liable. One should again examine the obligations of the data controller under the Data Protection Directive to see if they provide for legal protection in such a situation. Article 17 of the Directive obliges the data controller to protect the data against destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing of such data.[134] A mismatch does not automatically imply destruction, loss, alteration, unauthorised disclosure or access. So it is difficult to find protection in the security and confidentiality obligations of the Directive (and of the Privacy & Electronic Communications Directive).

The Data Protection Directive also requires collected information to be accurate and up to date. Compliance with those requirements is an important protection of the

[134] Article 17 says that "the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

data subject's privacy. Correctness of the processed data is obviously crucial. Be that as it may, however, the obligation to keep personal data accurate and up to date is difficult to achieve but crucial for an AmI world where the accuracy of the processing depends on the accuracy of the data. The mismatch in this case could be a consequence of an update of Michael's personal data that occurred just an hour before. Lack of interoperability may also cause mismatch that lies outside the responsibility of particular data controllers. Indeed, the scenario shows that the data controller tries to avoid any responsibility and puts the burden on the users of the system.

Refusal to provide the service (to Michael) may also be the consequence of defective services, hardware or software. It causes harm to the data subject. Who is liable for such damage? In the scenario, the security personnel try to eliminate their liability for the damage caused by shifting the liability to the group. The problem, however, might have been the result of an error in the central server of the security service itself. Article 12 of the **Directive on liability for defective products** states that the liability of the producer of a defective product (the security control system) may not be limited or excluded by a provision limiting or exempting him from liability. The Directive may provide the grounds for Michael's claiming damages if he had been refused and not permitted to participate in the trip, and if the refusal had been caused by a malfunction of the server.

The protection of the consumer[135] against unfair provisions in contracts is provided by the **Directive on unfair terms in consumer contracts**.[136] This Directive covers "the abuse of power by the seller or supplier, in particular against one-sided standard contracts and the unfair exclusion of essential rights in contract". It only applies to contracts between sellers or suppliers and consumers (natural persons) and, in particular, only to contractual terms that have not been individually negotiated by the parties. In an AmI world, consumers will become increasingly dependent on services and there is a significant risk that the suppliers of AmI services will obtain an even stronger power position and will abuse it. Thus, the supplier should also not be allowed to unfairly limit his liability for security problems in the service he provides to the consumer. This supplier should not be allowed to set out privacy conditions that are manifestly not in compliance with the generally applicable privacy rules and that disadvantage the consumer.

The Directive imposes mandatory rules for consumer protection, inter alia, that contracts should be drafted in plain, intelligible language, that the consumer should be given an opportunity to examine all of the terms and that, if the terms are in doubt, the interpretation most favourable to the consumer should prevail. It might be difficult, however, to implement those mandatory rules in an AmI world where a large number of transactions will be concluded instantly and continuously. The Directive includes provisions to avert the risk that the consumer may be deprived of protection under the Directive when the other contracting party designates the law of a non-member country as the law applicable to the contract. The Directive contains a list of examples of

[135] Some issues of consumer protection are also covered in section 3.2.8.6.

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

unfair terms. Although consumer protection organisations can ask for the annulment of unfair terms before the competent courts, the Directive does not, however, entail prior verification of the general conditions in individual economic sectors.

3.3.8.4. Disproportionate request for personal information

After the accident, medical help is given to the seniors. A hospital requires mandatory access to the complete medical record of a slightly injured patient. When the patient refuses to give access to his complete record, he is obliged to sign a statement waiving the hospital of any liability for any impairment from the treatment.

This part of the scenario highlights two major problems of data protection in AmI. First, the principle of "proportionality" (a cornerstone of data protection law) is questioned. Second, the concept of "consent" and how consent takes place should be examined in the context of AmI, which may curtail our freedom of choice in many situations.

The Data Protection Directive endorses the principle of proportionality, laid down in the first internationally binding document regarding data protection, namely Treaty 108 of the Council of Europe (1981). The principle of proportionality in the Data Protection Directive states that "the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

Despite its importance, this principle risks being eroded in a fast society with constant data processing and systems capable of intelligent processing and using large amounts of personal data. In other words, disproportionate data processing often takes place. There is not much case law in which one can find out what "proportionate" data processing is and what it is not. In addition, it is very difficult to define the exact meaning of "proportionate". On the one hand, there are too many diverse situations in which processing takes place, so that one particular situation might require more data processing for one reason or another. On the other hand, a definition of what is proportionate and what is not, somehow takes away the right of an individual to decide himself who can have access to his personal data and how long they may be stored and processed. Some persons might even find advantages in a vast and extensive processing and storage of their personal data.

Data protection officers do not often use the possibility to check the proportionate character of data processing by data controllers. Actually, there might well be too much data processing taking place in AmI to realise an effective control. In addition, many data controllers are exempted from notification of the processing to the data protection office, so that *a priori* control of the data controller seems to be very complicated.

This brings us to the second issue, which is that of the consent of the data subject: Processing of personal data must be "legitimate". This is stated explicitly in Article 7 of the Directive. Beyond a series of exceptions that we will not address here (processing necessary for the performance of a contract or for compliance with a legal obligation to which the controller is subject or in order to protect the vital interests of the data subject), legitimacy is based on three general principles.

The first concerns processing operations to help fulfil government tasks and pursue the public interest by the authorities themselves or others working for them. A government data processing has to meet the criteria of the legal framework of the specific administrative authority and comply with its statutory powers. On top of that, each action by the authorities has to meet the criteria of the public interest. Mutatis mutandis, this also applies to the processing operations that the authorities manage or delegate. As a result, government data processing is not justified when it is not necessary for the exercise of a specific power of the administration concerned. It is just as unjustified when government data processing operations constitute a disproportionate invasion of privacy, since protection of privacy is, to a great extent, part of the public interest. There should be less invasive methods available to achieve the same goal. In addition, governmental data processing also has to respect Article 8 of the ECHR. The restrictions set out in the second paragraph of that article fully apply. This implies, that apart from the aforementioned legality and proportionality requirement, governmental data processing must be necessary in a democracy and be "in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or the protection of the rights and freedoms of others". This means that a processing operation is not justified simply because it is executed by or for the government. National rules need to make this meticulously clear. They have to ensure and encourage that the judges and the specially created supervisory authorities consider the interests of every side in every situation.

A second legitimacy principle primarily concerns the private processing of personal data. Article 7(f) of the Directive says that "processing is necessary for the purposes of the legitimate interests pursued by private interests, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". Again, two aspects intertwine. In the first place, the ultimate purpose of the processing should be lawful. If the processing is undertaken by a legal person, its corporate purposes will be taken into account as an additional touchstone. Legal persons can only undertake actions to achieve the goals laid out in their articles of association. The processing operation has to be congruent with those. Second, the processing operation must be clearly necessary and indispensable to achieve the set purpose of the processor. Is it possible to achieve that purpose through other means? In regard to privacy, is this the least harmful way? Proportionality is essential. The interests at stake have to be carefully balanced. In each case, the concrete interests facing each other have to be carefully evaluated. A purely commercial purpose that results in an invasion of privacy (e.g., the processing of personal data for direct marketing sales) has to be judged differently (and more severely) than data processing necessary to maintain public health, freedom of speech or, for that matter, the running of a sports club.

The third legitimacy principle is consent. Article 7 (a) states that "personal data may be processed only if the data subject has unambiguously given his consent". Consent is taken to mean "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2 (h)).

Processing personal data is thus justified if the data subject clearly gives his/her consent after being informed of all aspects of the processing operation: the delineated and justified purpose of the processing operation, the categories of personal data to be processed, possible third parties that will have access to the information, who is responsible, his/her rights, etc. The unambiguity and specificity of the consent and the complete information on which it is based will need to be proved by the processor in case of conflict.

The consent criterion engenders a number of difficulties. First, the freedom of choice is often limited and relative in reality. Not everyone in our society has the same possibilities. Data processing is mostly entrenched in relationships in which the data subject is the weak party and the data flow is often one-way. Most of the time, the data subject needs something (e.g., credit, health insurance) and is almost forced to give consent. In the end, consent is often turned into a pure formality without offering any guarantee. Second, the general framework of the Data Protection Directive leaves doubt about what processing operations can be justified solely based on the consent of the data subject. If no consent is given, the other legitimacy grounds in themselves seem to span the whole range of possibilities (especially Article 7 (f) discussed above). Unless one assumes that such consent would legitimise disproportionate and illegitimate processing – which is questionable. It is problematic to invoke the consent of a data subject in order to justify a disproportionate processing. In penal law, the consent of a victim does not erase the criminal character of an action. Mandatory secrecy is not affected when a party gives consent to make something public. The mutual consent between parties on illegal agreements does not yield a legal agreement. As a result, the unambiguous consent of the data subjects is only one of the aspects that affect the considerations of the different interests.

Where sensitive personal data are involved, such as health-related data, things are even more complex because the Data Protection Directive has created a special regime. Indeed, Member States must *proscribe* the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Article 8(1) of the Data Protection Directive). In those cases, a fundamental data processing prohibition applies because it endangers not only privacy, but also the principle of non-discrimination. Yet this fundamental ban also allows for exemptions. The processing of sensitive data is then possible, inter alia, when the data subject has given his explicit consent.[137] Thus, the "explicit consent" to the processing of such sensitive information would make it legitimate. The hospital example shows that this consent is often not

[137] Article 8 allows other exceptions for processing of sensitive data, i.e., those where the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law; or is necessary to protect the vital interests of the data subject; or is carried out, with appropriate guarantees, by a foundation, association or other non-profit-seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to its persons or those who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without consent; or relates to data made public by the data subject or is necessary for legal claims. The Member States can add extra exemptions to the general prohibition.

freely given because the data subject is in a subordinate situation. He is subject to the power of the data processor and controller, who possess a good or a service one wants. In this scenario, the data subject is dependent on the hospital (and therefore will mostly give disproportionate access to his personal data), but also the hospital is dependent on the insurance companies that require hospitals to enforce access to the complete records of their patients (and therefore the hospitals will mostly ask for disproportionate access to the personal data).

Article 8 of Data Protection Directive provides the rule that the prohibition on processing of sensitive data does not apply in a case "where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy". That might imply that a patient would need to grant access to his medical records by the hospital, to enable the latter to provide him with the treatment. In any event, the hospital is still obliged to respect the proportionality principle and not to process more data than necessary. However, the hospital is deciding what is proportionate under the circumstances rather than the patient. In an optimal situation, the hospital treating minor injury should be able to obtain access to only a portion of the patient's medical record as necessary to treat the case.

The non-discrimination principle is well established in the European law. Articles 21 and 23 of the Charter of Fundamental Rights of the European Union prohibit discrimination based on grounds such as sex, race, colour, nationality, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.[138] The non-discrimination principle is also in the EU Treaties (Article 6 of the Treaty on European Union by reference to respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms,[139] Articles 7, 12 and 13 of the Treaty establishing the European

[138] The Charter of Fundamental Rights of the European Union is not legally binding, but it is already referred to in the case law of the Court of Luxembourg. See García, R.A., "The General Provisions of the Charter of Fundamental Rights of the European Union", Jean Monnet Working Paper 4/02, www.jeanmonnetprogram.org.; Eriksen, E.O., J.E. Fossum and A.J. Menéndez (eds.), *The Chartering of Europe: The European Charter of Fundamental Rights and its Constitutional Implications*, Verlag, Nomos, Baden-Baden, 2003; Peers, S., and A. Ward (eds.), *The European Union Charter of Fundamental Rights*, Hart Publishing, Oxford, 2004; Heusel, W. (ed.), *Grundrechtcharta und Verfassungsentwicklung in der EU*, Bundesanzeiger, Köln, 2002; Band 35 in Schriftenreihe der Europäischen Rechtsakademie Trier.

[139] This Convention, signed in Rome on 4 November 1950, recognises the principle of equal treatment in Article 14, which prohibits the discrimination on any grounds such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status in enjoyment of rights protected by the Convention. All Member States are Contacting Parties to the Convention. Any discrimination on the basis of the same grounds in enjoyment of rights set forth by law is also forbidden under Protocol No. 12 to the Convention. According to the protocol, no one shall be discriminated against by any public authority on any grounds such as those mentioned above.

Community) and in a wide range of EU legislation implementing those provisions. Non-discrimination is a fundamental principle of the European Union. Provisions establishing this principle prohibit using some of the characteristics (grounds for prohibited discrimination as enumerated in the legal documents) in decision-making. This principle would apply to decisions taken in the AmI environment as well, including automated decisions. Non-discrimination provisions do not prohibit the use of such data for other purposes (data collection, profiling), nor do they address possible use of such characteristics, but only the decision actually made. Those aspects are remedied to some extent, however, by data protection legislation, which establishes a prohibitive and more severe regime for the processing of sensitive data not as an expression of the will to protect privacy, but to remedy the danger of discrimination that may arise from the processing of such sensitive data. On the other hand, antidiscrimination law could also have the ability to fill gaps in the legal provisions of more specific instruments (such as data protection law). Prohibition of discrimination applies to all situations based on the forbidden criteria, not only in the case of identifiable individuals (which is a limitation the data protection law) but also anonymous members of a group (group profiling).[140]

3.3.9 Conclusions

The scenario about ambient intelligence in travel and health applications makes clear that even in fields with a quasi-public character, it is not self-evident that all citizens will benefit from the deployment of ambient intelligence as envisioned by policy-makers and scientists.[141] In fact, the complexity of large-scale technological systems for traffic management and public health shows that careful steps have to be taken in order to balance public and private interests – ranging from government, commercial network and service providers to the individual citizen and civil society as a whole.

It is a great challenge to avoid unjustified and excessive drawbacks or benefits for any of the affected parties. The challenge requires a blend of legal, organisational and technical measures. On the technological level, interoperating systems with a high degree of dependability (supplemented in part by independent fallback systems) are needed when the individual or society as a whole depends on an operating system. On the organisational level, measures are needed to make (public) services transparent and trustworthy. Finally, the legal framework and the

[140] 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.

[141] See, for example, IST Advisory Group, *Ambient Intelligence: From Vision to Reality*, Office for Official Publications of the European Communities, Luxembourg, 2003. http://www.cordis.lu/ist/istag – reports.html. See also Emiliani, P.L., and C. Stephanidis, "Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities", *IBM Systems Journal* 44, No. 3, 2005, pp. 605–619.

regulation of important public services have to be adjusted to new circumstances. This also means that existing networks and constellations of societal actors need to respond accordingly.

3.4 Scenario 3: What's an AmI data aggregator to do?

3.4.1 The scenario script

3.4.1.1 Introduction

The Data Mining Corporation (DMC) has an almost perfect business model. It collects data about individuals from hundreds of sources[142] and then sells the aggregated data back to many of those sources. Its principal sources (and clients) include insurance companies, retail chains, media conglomerates, credit-reporting agencies, mobile phone companies, law enforcement agencies, customs and immigration authorities, and intelligence agencies.

The advent of ambient intelligence technologies – including RFIDs, networks of sensors and actuators, fourth-generation (4G) mobile, surveillance and biometric technologies, and software that learns from our past behaviour and preferences to predict what we will want or will do[143] – has enabled DMC to construct detailed files on virtually every person in the United States, western Europe and other developed countries.[144] DMC knows what products we buy, services we use, who we are in contact with, where we are at any point in time, and so on. DMC can confirm whether we are who we say we are and what sort of activity we've been engaged in. Linking together many different databases and processing the acquired data using its own proprietary algorithm has enabled DMC to create such fine-grained profiling that it is the envy of its few remaining competitors.

Although DMC is a relatively new company, it has grown quickly. Among the ways it has managed to sidestep legislative and regulatory constraints on transfers

---

[142] Data aggregators today mine data from thousands of sources. For example, see O'Harrow, Robert, *No Place to Hide*, p. 124: "LexisNexis, a subsidiary of the UK-based Reed Elsevier Group, maintains billions of records, including media reports, legal documents, and public records collected from thousands of sources around the world."

[143] cf. Biever, Celeste, "RFID chips watch Grandma brush teeth", NewScientist.com news service, 17 March 2004: "Tiny computer chips that emit unique radio-frequency IDs could be slapped on to toothbrushes, chairs and even toilet seats to monitor elderly people in their own homes. Algorithms on the PC use 'probabilistic' reasoning to infer what the person is doing. For some tasks, merely picking up an object such as a toothbrush is enough."

[144] See, for example, O'Harrow, p. 222: "HNC … monitors 90 per cent of all credit cards in the United States and half of those in the rest of the world … using artificial intelligence to seek out indications of fraud and deceit." See also Solove, Daniel J., *The Digital Person*, p. 20: "Wiland Services has constructed a database containing over 1,000 elements, from demographic information to behavioural data, on over 215 million people."

of personal data is through mergers with or acquisitions of companies with their own extensive databases. It is headquartered in Miami, but now has major subsidiaries in London and Tokyo. It is listed on the New York and London Stock Exchanges and is considering a listing on the Tokyo Stock Exchange.

Scene 1: Management board meeting

The company secretary places his hand on a fingerprint reader outside the boardroom and then stands close to the iris scanner. The boardroom door opens and he enters. As he does so, the lighting and the air conditioning automatically come on and are set at his comfort levels, which are known from his previous activity in the room. A second later, the door slides open and the DMC president walks in. The sensors and actuators in the boardroom slightly adjust the air conditioning and lighting to the midpoint between the president and secretary's preferences. The president nods a slight greeting to the company secretary who can see his boss is preoccupied. A few seconds later, the vice presidents enter one by one and take their seats, and the lighting and air conditioning sensors and actuators make further adjustments to the collective mid-point levels.

The vice president for media relations has not arrived. The president is petulant. "Where's MacDonald?" she barks at Alvin, the holographic embodiment of DMC's embedded intelligence. The boardroom video screen switches from the agenda and shows MacDonald's office. He is heard and seen finishing off a telephone conversation with a journalist. He gets up from his desk and leaves his office. As he does so, another camera in the hallway shows him going down a corridor. His position co-ordinates, accurate to less than a metre, shown in the lower left-hand corner of the boardroom screen, change as MacDonald approaches the boardroom. He is seen putting his hand to the fingerprint reader, but the reader does not respond. He tries unsuccessfully to rub some ink from his finger, and then leans close to the iris scanner, which does respond, but he is still not admitted to the boardroom since he must have positive responses from both systems. The impatient president commands Alvin to open the door and finally McDonald is admitted.

"Okay, let's get on with it," says the president. "Show me today's agenda," she instructs the computer. The agenda appears on a large wafer-thin video screen on the wall opposite the president. Three items are listed:

Data from developing countries. (Switzer)
Theft of data, 29 June 2017. (Perrier)
Considerations re listing on the TSE. (Hausmann)

Kevin Switzer, vice president for operations, speaks. "We've had complaints from the Customs and Immigration folks about the shortage and reliability of our data on people coming into the States.[145] *It mainly concerns people from*

[145] See O'Harrow, p. 48: "For years, the credit bureaus had been dogged by complaints. Information in their reports was chronically incorrect. They routinely failed to correct mistakes, and seemed arrogant when individuals called."

developing countries. With our profiling technologies, we are able to identify anyone who might be a security risk or disposed to anti-social behaviour. Unfortunately, most developing countries have no AmI networks, which makes it impossible to build up the same kind of detailed profiles of individuals like we can here in the US, Europe or Japan. So the immigration authorities have been making threatening noises about refusing entry to people from countries without AmI networks."

"So what are you doing about it?" asks the president.

"Well, I think we have a golden opportunity here. We can offer to set up AmI networks in those countries as long as we, I mean DMC, are the ones to collect and process the data. You'd think most countries would jump at the chance to have networks put in place at virtually no or little cost to them, but some of the countries are quibbling with us."[146]

"Quibbling?" asks the president, "What do you mean?"

"Quibbling about control of the data. They say if we control the data, it's tantamount to signing their sovereignty over to us. But we've been working on a deal where we copy for them the data we collect… well, some of it, at least. Our intelligence agencies would not want us to hand over everything, and we don't have to either. We can offer the raw data to the developing countries, but certainly not the processed data. Developing countries will never know how we've processed the data, especially since we do the processing here in the United States or in the UK, i.e., outside their jurisdiction. They'll have to settle for what we give them."

"Okay, that sounds good to me. Any objections?" she asks the others who remain silent. "No? Okay, then, Jacques, it's your turn. What's the latest on the theft or whatever it was at our London office?"

But before Jacques Perrier, vice president for security, can respond, the company secretary leans over and whispers something to the president. "Yes, you're right." The secretary stops the boardroom monitoring systems from recording more of the discussion on this subject.

Perrier shifts uncomfortably in his chair. "Well, as everyone here knows, we have a regular monthly audit of DMC's data processing activity. From the last audit two weeks ago, we discovered that there had been a second back-up of data immediately after the first. These back-ups are made every day. Sometimes there's a problem and a second back-up is made. It's not that unusual, but since it's not supposed to happen, we always check them out. The second back-up was anomalous too because it wasn't the whole of the database and didn't get backed up to the usual destination. In other words, we assume it was backed up locally …"

---

[146] See O'Harrow, p. 186: "On June 1 [2004], the government granted the contract for a massive expansion of US Visit to Accenture. The deal, worth up to $10 billion, will bring together an array of information and surveillance industry contracts. … In the coming years, Accenture will be helping to build sprawling computer networks and identity systems to enable the government to track foreign visitors to the United States. The company aims to create digital folders containing visitors' fingerprints, photographs, and details about their travels. The new systems will also rely on radio frequency identification and face recognition software."

Hausmann intervenes, "By locally, you mean to another computer here in the building?"

"Yes, except that none of the computers here show any evidence of having been the destination for the second back-up. That means some portable device with an optical connector was used."

"You mean like a memory stick?"

"Something like that."

"I presume you know who made the second back-up?" asks the president.

"Umm … uh … yes. It seems likely that it was three of my staff who were responsible for doing the regular back-ups that night. We wanted to ask them about this second back-up, but they had left on holidays a few hours after the second back-up was made. They were supposed to have returned from holidays three days ago, but they haven't reported for work and they haven't answered our calls."

The president is getting angry. "So you mean your staff have copied part of our database and walked off with it?"

Perrier is visibly squirming in his seat. "That's what it looks like."

"And how many records do you think were copied?" she asks.

"Uh … It's bad, I'm afraid." Perrier coughs. "My guys think about 16 million."

"Outrageous," says the president, slapping the table. "And why don't you know where they are? Surely you can track them via their location implants. Everybody has to have a location implant. It's a condition of employment in our company, just like any critical infrastructure like banks, nuclear power companies, etc."

"Yes, we've been checking their location data, but so far nothing," says Perrier.

"They could have been surgically removed," says Switzer. "What about the data from the AmI systems? Have you checked the sensor networks in the homes and cars of those three employees?"

"Yes," says Perrier. "Like other employees, they've agreed that we can check their home systems and we've done that. There's obviously nobody in their apartments, and their cars have been stationary since they left on holidays …"

"And what about the surveillance systems?" asks the president. "You can't go anywhere in London without being caught by surveillance cameras hundreds of times a day."

"Yes, we've been reviewing the data from the surveillance systems too," says Perrier. "But they haven't shown up on those either. We've also been checking with the airlines and railways and car rental agencies to see where they might have gone on holidays. Now we know they left for Costa Rica, but then the trail goes cold. As Kevin has just pointed out, the developing countries don't have the kind of AmI infrastructure needed to track people, so they could really be anywhere. We've also been checking with the mobile telecom companies too, but so far, there's been no data recovered on use of their mobiles."

"I don't understand how they could have got past our own security systems," says the president. "We have access control to prevent employees from unauthorised copying or manipulation of data."

"That's true," says Perrier. "The snag is that they were authorised. Quite a few employees have partial access, so if three or four with access to different bits

collaborate, as these three appear to have done, they are able to get virtually full access to the data."[147]

"Even so," asks the president, "how did they get the data outside our headquarters?"

"With today's technology, it's easy to copy vast amounts of data in seconds onto high capacity optical storage devices no larger than a deck of playing cards, which makes them easy to conceal on the way out of the building. It's hard to break into DMC offices, but it's not hard to get out."

The president: "Are there any indications yet of what they might do with all this data?"

Perrier: "No, not yet, but there are several likely possibilities, of course. They could use the identity information to commit all kinds of fraud on a huge scale without leaving any trails retraceable to them. Or they could simply sell it. There are lots of digital sites that deal in stolen data. You can easily get $100 these days for each ID.[148] *Or they could sell it to an insurance company or an intelligence agency, although we've pretty much already cornered those markets. Or they could sell it to some terrorist organisations. Or they could try to blackmail us, and we'd either have to pay up or risk the bad press we'd get if people find out just how much data we've been able to collect about them since AmI technologies became so widespread, and some of that data, as you know, has not always come from legitimate sources. Or they could blackmail victims with the knowledge they've derived from our profiles."*

"Or maybe they won't do any of those things," adds MacDonald. "Maybe they just want to make a political statement."

"What do you mean?" asks the president.

"They may feel they have a social obligation to show how extensive our data aggregation practices have become since the introduction of AmI networks and how easy it is to pilfer the data we collect," says MacDonald. "If we were exposed, it would be a complete disaster. Among other things, it would show our clients that the profiles of our own people were not reliable because we were not able to predict that these few rogue employees were going to abscond with copies of our files."

The president snorts. "If they have 16 million records and they could get $100 for each record, I doubt they're very interested in political statements."

Max Court, DMC's general counsel, speaks up. "If we were exposed? Are you suggesting we should withhold information about this theft from the police and those whose files have been copied?"[149]

---

[147] A Computer Security Institute study found that 70 per cent of all computer attacks came from insiders. See Schneier, Bruce, *Secrets & Lies*, p. 189.

[148] See Zeller, Tom Jr., "Black Market in Stolen Credit Card Data Thrives on Internet", *The New York Times*, 21 June 2005: "A 'dump', in the blunt vernacular of a relentlessly flourishing online black market, is a credit card number. And what Zo0mer is peddling is stolen account information – name, billing address, phone – for Gold Visa cards and MasterCards at $100 apiece."

[149] Some state governments in the United States have passed legislation recently (e.g., California law SB1386, effective July 2003) that forces organisations to inform individuals whenever there has been a privacy breach, and makes organisations liable for improper use of information. In October 2005, a US Senate committee was considering new legislation for a Personal Data Privacy and Security Act. The bill requires that, on discovering a data breach, any agency or business entity that "uses,

"Of course," says MacDonald. "It's obvious, isn't it? I'd hate to imagine what it would do to our share price and our plans for a listing on the Tokyo Stock Exchange."

The president takes a deep breath, as if she were trying to control her temper. "You've got to find those three," she says to Perrier.

"Yes, mam. I know."

She turns to Frank Hausmann, her chief financial officer. "Okay, Frank, what's your advice about the listing on Tokyo?"

MacDonald interrupts before Hausmann can respond. "I'm sorry to interrupt again, but I was just talking to a journalist from The Financial Times*. That's why I was a bit late for the start of the meeting. She rang about our intentions re the listing on Tokyo. I don't know how she knew that we were even thinking about it. I didn't confirm or deny anything. Then, she asked whether we were complying fully with the Safe Harbour Agreement. Of course, I said we were, but then she posed some very pointed questions about the security of our data. I began to wonder whether she knew about the theft …"*

"So, Madame President, before I give my views on the Tokyo listing, I'd like to know if we are going to put out a statement about this theft. It'll make a difference about the timing," says Hausmann. "Are we going to inform those people whose records have been compromised? Are we going to tell the media?"

"We can't inform the individuals, because we don't know, at least not yet, whose records have been compromised," says Perrier.

"It's for you to decide what we should do," says MacDonald to the president.

Scene 2: The Old Bailey, two years later

BBC 1 news presenter: "And now we go to our reporter, Miles Davenport, who's been at the Old Bailey today, attending the trial involving the Data Mining Corporation and its directors. What's the latest, Miles? Has the jury returned with a verdict?"

Miles Davenport: "Thanks, Serena. No, the jury hasn't returned yet, but an announcement is expected in the next few minutes."

BBC presenter: "Miles, can you just recap for our viewers what this trial's been all about? And why is it so important?"

Miles: "Sure, Serena. As you know, this case has had all the elements of a Jeffrey Archer thriller. It's involved high technology, secretive corporations, the world of intelligence, consumer activists, and high-level calls between the president of the United States and our prime minister. Even the European Commission has got into the act.

"It all started about two years ago when The Financial Times *broke a story about the theft of personal information on 16 million people in the United States and the UK. All these personal data were held by the Data Mining Corporation, an Anglo-American conglomerate most people had never even heard of.*[150] *DMC had*

---

accesses, transmits, stores, disposes of or collects sensitive personally identifiable information" notify "without unreasonable delay" any US resident whose data were subject to intrusion. As of mid-2007, the bill had not yet been adopted by the Senate.

[150] See O'Harrow, p. 34: "Acxiom is not a household name. But as a billion dollar player in the data industry, with details about nearly every adult in the United States, it has as much reach into American life as Pepsi or Goodyear. You may not know about Acxiom, but it knows a lot about you."

been growing like a powerhouse through mergers and acquisitions, until it had become the world's largest data miner. It turns out that DMC had been profiling virtually everyone in the United States, Europe and many other countries around the world. They have the world's fastest and most powerful computers with billions and billions of records from all sorts of services, including governments.[151] *DMC had been processing all these records from different sources, including the latest ambient intelligence networks, and linking them together so that it was able to build up comprehensive profiles on every one of us.*[152]

"Then, according to the FT, DMC discovered that someone had broken into its supercomputers and copied data on a lot of people. For a few weeks, DMC didn't say anything to anybody,[153] *but then there was a big spike in the number of identity theft cases. People with credit cards were seeing all kinds of purchases on their monthly statements for stuff they hadn't bought. A lot more people and companies were reporting that they were being blackmailed with threats of releases of embarrassing information unless they paid up. The FT got wind of this big increase in credit card fraud and extortion, and was able to trace the source back to a theft of data from DMC.*

"At first, DMC denied everything; then they said they wouldn't comment on it, because the theft was under police investigation. But by then, the DMC share price was plummeting on Wall Street and in London, and DMC had to call off plans for a listing on the Tokyo Stock Exchange. For a while, it looked like DMC was going bust, but the US government stepped in and propped up the company.[154] *The President said that national security was involved, and they could not allow the company to go bust. People began badgering the Prime Minister about it. They had no idea just how pervasive ambient intelligence had become …"*

BBC presenter: "Personalised services are great, of course; they save us lots of time. And so are the improvements in our security, knowing when we are near known criminals or people disposed to terrorism, but isn't there a dark side?"

Miles: "Well, according to civil libertarians, yes, there is. And that's partly what's been coming out in the trial of DMC. Companies like DMC hold a lot of data

---

[151] See Solove, p. 5: "Federal, state and local governments maintain public records spanning an individual's life from birth to death. These records contain a myriad of personal details. Until recently, public records were difficult to access. … But with the Internet, public records are increasingly being posted online, where anybody anywhere can easily obtain and search them." In addition, those bent on identity theft can make use of freedom of information laws. See Solove, p. 150: "The vast majority of FOIA requests are made by businesses for commercial purposes."

[152] See O'Harrow, p. 49: " 'InfoBase Enhancement' enables Acxiom to take a single detail about a person and append, on behalf of its customers, a massive dossier. This generally happened without the individual ever knowing about it."

[153] See Krim, Jonathan, "Consumers Not Told Of Security Breaches, Data Brokers Admit," *The Washington Post*, 14 April 2005.

[154] See Safire, William, "Goodbye To Privacy", *The New York Times*, 10 April 2005: "Of all the companies in the security–industrial complex, none is more dominant or acquisitive than ChoicePoint of Alpharetta, Ga. This data giant collects, stores, analyses and sells literally billions of demographic, marketing and criminal records to police departments and government agencies that might otherwise be criticized (or de-funded) for building a national identity base to make American citizens prove they are who they say they are."

about all of us. And we have to trust them that our data are safe, secure and accurate. But now we know that our data are not secure.

"Questions have also been raised about the accuracy of the data. People are entitled to see their records, but most people didn't even know about DMC, let alone the fact that they had built up such extensive records on every one of us.[155] *So some consumer activist groups have banded together to sue DMC for negligence, for inadequate security of their records, for not complying with the Safe Harbour Agreement between Europe and the United States. It was one of the first class action suits in UK legal history. The European Commission has got involved too. They said that the Federal Trade Commission, which administers the Safe Harbour Agreement for the US, had not been ensuring proper compliance by American companies. The Commission has also said they were taking the US to the World Trade Organisation too, because a subsidy for DMC was against its rules. It's really turned into a big mess. After this six-month trial, and thousands of pages of testimony, the end looks to be in sight."*

BBC presenter: "Thanks, Miles, for that recap. Weren't there some other issues that came out during the course of the trial?"

Miles: "There certainly were, Serena. It was discovered that not only has DMC failed to protect our data, but they've actually been selling large chunks of it to governments and to other companies who in turn were using the data to spam just about everybody in the United States and here in the UK too.[156] *DMC claimed that they couldn't be held responsible for what their clients did with the data.*

"We also heard about fraud arising from identity theft. Some of the prosecution's witnesses said that even though their credit card companies limited losses to the first £50, fraudulent use of their cards and other personal data had knock-on effects. Credit-reporting agencies raised red flags, not only about the cards, but also about the actual card-holders. Some witnesses said they had been trying to get wrong information cleaned from their records for almost two years, and have yet to succeed.[157]

"Most witnesses said they've suffered from the stress involved in trying to recover their identities and sorting out the mess they've been put in.[158] *Some said*

---

[155] Schneier, Bruce, "The Future of Surveillance", *Crypto-Gram Newsletter*, 15 October 2003: "In the US, data about you is not owned by you. It is owned by the person or company that collected it."

[156] See O'Harrow, p. 135: "In 2002, the company [ChoicePoint] began allowing individuals to buy dossiers, including criminal checks, education records, and other personal details. ….Now everyone would soon be able to dig into the past of suspect acquaintances or employees."

[157] See Zeller, Tom Jr, "For Victims, Repairing ID Theft Can Be Grueling," *The New York Times*, 1 October 2005. The story reports cases where victims have been trying to overcome the consequences of identity theft for more than two years: "Victims are still left with the unsettling realization that the keys to their inner lives as consumers, as taxpayers, as patients, as drivers and as homeowners have been picked from their pockets and distributed among thieves."

[158] See Solove, p. 110: "Identity theft can be a harrowing experience. According to estimates, a victim typically spends over two years and close to 200 hours to repair the damage that identity theft causes." And p. 110: "Most identity thefts remain unsolved. Research firm Gartner Inc estimates that less than 1 in 700 instances of identity theft result in a conviction."

they've been stigmatised. We heard also about DMC selling their services to companies who wanted to check on prospective employees. We heard that in many instances the information was wrong, that the data coming from so many different ambient technology networks were often in conflict or didn't make any sense. DMC countered that its proprietary software contains an algorithm for comparing data from different sources to maximise reliability and its predictive capability,[159] *but under intense questioning from the prosecution, they admitted they could never eliminate unreliability nor could their predictions of who might be a terrorist or criminal be 100 per cent.*

"We heard about one case involving a senior civil servant whose name was put on a suspect list when it shouldn't have been. As a result of a compromised fingerprint, he couldn't even get into his own office after the fingerprint template had been disabled without his knowing it. Because he couldn't deliver an urgent file to his Minister, he became so stressed that he had to be hospitalised. His case illustrated the problem arising from different technologies no longer trusting the readings they were getting from other technologies.

"As a result of the media interest in this case, many more people are now aware of how pervasive the new ambient intelligence technologies have become and how it's more important than ever that they check out what these big data aggregating companies have on them, the sources they draw on and what happens to their personal data after DMC and its competitors have processed it. If any good has come out of this case, that's surely been it."

BBC presenter: "And the DMC directors, what's going to happen to them?"

Miles: "We should find out after the jury comes back with the verdict. The DMC president, however, has already resigned, but she went out with a golden parachute – a severance package that included a cool $100 million – and now she's apparently living in Costa Rica."

3.4.2 Analysis

3.4.3 The context

The scenario has two scenes, the first of which takes place in a corporate boardroom in the year 2017, the second outside a courtroom two years later. Hence, the scenario is in the business domain.

---

[159] See O'Harrow, p. 221: "CAPPS II, shorthand for the second-generation computer-assisted passenger screening program … would piggyback on the data revolution of the 1990s, using mountains of demographic, public record, and consumer files to pluck out terrorists from the mass of people who posed no threat at all. It was to be a perpetually watchful network that would electronically absorb every passenger reservation, authenticate the identity of the travellers, and then create a profile of who they are. Then it would examine that profile, instantly and relentlessly, looking for anomalies in behaviour or lifestyle that might indicate ties to terrorist groups."

The scenario concerns the theft (copying) of personal information held by a data aggregator (Data Mining Corporation) by three rogue employees. Theft of identity occurs now, but the difference between such crimes today and in the future is the scale of the data involved.[160] In the future foreseen by this dark scenario, it will be possible to gather orders of magnitude more information about virtually every person in the United States, Europe and Japan. Our reliance on AmI will have grown immeasurably. The future is also marked by an increasing concentration in the control of personal data. Thus, the risks to individuals are much greater when something goes wrong. By the year 2017, there will have been significant technological advances, but this scenario posits that there will have been little evolution in business ethics, management practices and public awareness.

3.4.4 AmI technologies and devices

The scenario makes reference to several AmI or AmI-related technologies, including:

- Biometrics, including a fingerprint reader and iris scanner, which serve security purposes in admitting entrance to a restricted area (the boardroom) by only those authorised to enter.
- Networked sensors/actuators, which are linked to the fingerprint reader and iris scanner and which activate the lighting and air conditioning in the boardroom based on the known preferences of those entering the boardroom. To deal with several competing individual preferences, the actuators calculate the mid-points of those in the room.
- Wafer-thin displays which can switch from textual information (the corporate management committee's agenda) to visual imagery from surveillance cameras which, at the same time, display the reference person's location co-ordinates in real time.
- Voice-activated access to an intelligent environment as shown in the board room meeting.
- Surveillance technologies which management can use to monitor employees, both in the office and outside (e.g., in their homes or cars). Surveillance technologies include video cameras, key logging software, biometrics and other networked sensors, as well as location implants and location-reporting devices, which employees are obliged to bear or wear as a condition of employment.
- Machine-learning technologies which analyse past behaviour and preferences in order to predict needs and to personalise services.
- Networked RFIDs, sensors and actuators for gathering data about people and the products they have or services they use.
- Fourth-generation mobile phones, which combine today's PDA capabilities with third-generation mobile technology (and much else).

[160] See O'Brien, T.L., "Identity Theft Is Epidemic. Can It Be Stopped?", *The New York Times*, 24 October 2004.

3.4.5 AmI applications

The AmI technologies referenced in the scenario are used in various applications, including:

- Security – Biometrics are used for admission to restricted areas such as the corporate boardroom as well as the DMC headquarters building. Access control technologies (e.g., biometrics) are used to govern who can have access or make changes to DMC's databases.
- Surveillance – The president and his corporate colleagues are able to watch MacDonald in his office and on his way to the boardroom. References are made to surveillance of employees outside the office as well. Sensors in homes and cars are networked and provide information to DMC senior management as to whether an employee is at home or in his or her car.
- Immigration control – AmI technologies enable the building up of much more comprehensive profiles of individuals, so much so that prospective visitors or immigrants from countries without AmI networks may not in future be admitted to the developed countries because, in the absence of AmI networks in their own countries, there is not enough information to assess whether the candidate is trustworthy or a security risk.
- Personalisation of services – AmI is used for personalisation of services such as lighting and air conditioning set to one's preferences as well as services provided by products and services such as PDAs and mobile phones. Personalisation of services also leads to time-savings since AmI networks can, for example, monitor the status of one's consumables (such as food and drink) and place orders with the supermarket as necessary.
- Targeted marketing – With more detailed data on consumers, retailers, media conglomerates and others are able to engage in targeted marketing with greater precision.
- Improved profiling – Insurance companies and credit-reporting agencies are able to assess individuals against insurable risks and creditworthiness. While this is good for the insurance companies and credit-reporting agencies, it may not be so good for individuals who may find it harder to get insurance or credit.
- Counterterrorism and policing – With more detailed data on individuals, intelligence agencies and police forces are better able to assess and counter terrorist risks and combat crime.
- Critical infrastructure protection – Although protection of critical infrastructure is only mentioned in passing in the scenario, AmI provides the means to better protect critical infrastructure (including the AmI networks themselves) from intruders (but not necessarily insiders) bent on damaging or undermining those networks.
- Computer communications – Fourth-generation mobile phones combine today's PDA capabilities with third generation mobile technology (and much else) and are able to interoperate with heterogeneous networks.

While several positive, socially useful applications are alluded to, there are some negative applications too. Among them:

- Spamming – The huge increase in data about individuals facilitates more precision in spamming and targeted marketing.
- Fraud – Similarly, the opportunities for fraud are improved because more detailed information is available to criminals.
- Blackmail – With more detailed information, criminals are in a stronger position to blackmail those whose data they hold.
- Discrimination – With more detailed information, insurers are able to discriminate against some people who pose higher risks than others. Conversely, the lack of information on some people (e.g., those from developing countries) means that they too could suffer discrimination, i.e., if they do not have an adequate data trail, they may not be admitted to developed countries.
- Terrorism – Terrorists have more opportunities and better information to impersonate others when they have access to the detailed data on individuals provided through AmI networks.

3.4.6 Drivers

The scenario hinges on the theft of data from DMC and the consequences of that theft. The drivers at work here can largely be derived from the motives and needs of the principal characters or groups of characters.

DMC has aspired to be the leader in its market, something it has achieved. DMC's success can be attributed to at least two or three key factors. One is that it has been able to aggregate more data on individuals than any other company. A principal source of these data is the AmI networks that are able to generate far more information than ever before on individuals, their behaviours, habits, contacts, comings and goings, purchases, etc. A second success factor is that DMC has developed an algorithm for sifting through and processing all this data so that it is able to sell its products and services to a wide range of clients. A third factor could be the quality and vision of its management, without whose leadership (and their business plan) it would not have been able to achieve such success.

For the management, one could conclude that they are primarily driven by the profit motive and a desire for scale (i.e., to be the market leader and, presumably, to swallow or overwhelm competitors) and to create a situation where their clients are dependent on DMC services and products.

A second driver must be market demand, i.e., there are many companies and governmental agencies that want the processed data that DMC has been supplying.

A third driver, not so dissimilar from the first, is that the data thieves are also impelled by the profit motive. In their case, however, one could conclude that they see an opportunity to make more money more quickly by copying files from the DMC database and selling it to fraudsters. Before the spike in reported instances of identity

theft, Perrier, DMC's vice president of security, speculates what the data thieves might do with the data, which points to drivers. He says the data thieves could sell the data to an insurance company or intelligence agency or to a terrorist organisation or blackmail DMC and/or the individuals whose data they have copied (i.e., the driver is to make money). MacDonald speculates that the data thieves might have committed their crime in the public interest – i.e., to make people aware of how much information DMC was collecting on them through the aggregation of data from AmI networks and to make people aware just how ill-protected and insecure their data are.

A fourth driver is respect for the law. This is indicated when DMC's general counsel expresses some disbelief at the suggestion that DMC should cover up the data theft from both the police and those whose files have been copied. As he makes only one intervention in scene 1, we might not want to attach too much importance to this driver. In scene 2, however, the court case indicates that respect for and redress through the law is a much stronger driver. The lawsuit against DMC is brought by consumer activists seeking restitution (= a fifth driver) for the aggravation caused to them through DMC's negligence.

Yet another driver can also be identified, i.e., the media's desire for a good story which has the benefit of raising public awareness about the pervasiveness of AmI and AmI's benefits (e.g., greater convenience through personalisation of services and improved security) as well as possible risks (encroachment on privacy, exploitation by terrorists, criminals, intelligence agencies, insurance companies, etc.).

3.4.7 Issues

The scenario raises several issues:

3.4.7.1 Digital divide

The developed countries have AmI networks and the developing countries do not. There is a risk that this will lead to discrimination against developing countries because the intelligence agencies and immigration authorities may not admit visitors and emigrants from those countries because they do not have the detailed information on those individuals like they do on individuals from developed countries and, consequently, are not able to assess whether individuals from developing countries are a security risk.

On the other hand, DMC executives see an opportunity to set up AmI networks in developing countries which could overcome the concerns of the intelligence agencies and immigration authorities, but potentially leads to another form of discrimination whereby the data arising from the AmI networks are processed by DMC in the United States. A sop would be given to the developing countries, i.e., the raw data, but the real juice is in the processing and exploitation of the data. Switzer mentions the fears of developing countries that they would effectively be transferring their sovereignty to the developed countries (if not to DMC).

3.4.7.2 Concentration of power

DMC is the clear market leader in the aggregation and processing of AmI-generated data. Its clients include a wide range of powerful clients – the media, retailers, credit-reporting agencies, immigration authorities, intelligence agencies, etc. When there is a risk that DMC might collapse as a result of the fall-out from the theft, the US government steps in to prop up the company on the grounds that, for security reasons, it cannot permit the collapse. This in turn leads to a dispute between the United States and the European Union as the latter claims that a subsidy violates WTO rules.

3.4.7.3 Lack of public awareness

Despite the convenience of the increasing personalisation of services and the enhancements in security that AmI has made possible, most people have not comprehended just how pervasive AmI has become, nor of the scale and volume of data being generated about them by AmI networks. Everything produced will have an AmI-networked microchip.

Most people are willing to trade some of their privacy for better security. The scenario suggests that terrorism has become sufficiently serious that the intelligence agencies and immigration authorities are becoming unwilling to admit foreigners unless they have detailed information on each individual. Similarly, DMC employees seem willing to have location implants and surveillance equipment installed not only in their offices but also in their homes and cars. Probably, they see this as beneficial in security terms.

In the scenario, public awareness is increased as a result of the investigative reporting and media coverage of the theft of data from DMC, the resulting trial and the high-level political intervention. Identity theft is not, of course, a new crime, but what is new about the DMC case is just how extensive are the data from AmI networks compiled and processed by DMC.

3.4.7.4 The illusion of security

It is ironic that DMC and its directors face a class action lawsuit on the grounds that they were negligent in securing personal data. It would seem DMC has many security measures. They have installed surveillance equipment, biometrics, key-logging software and other access control measures to protect the data they hold. One of the vice presidents says it is hard to get into DMC headquarters. But the question is: have DMC executives done enough? Did they think their profiling of their own employees was sufficiently watertight so that they did not need to fear theft by insiders? Maybe. We are told that it was hard to get into DMC offices, but not hard to get out. Also, the president seems surprised by a breach in DMC security. Furthermore, they do not know which specific files have been copied, only that about 16 million were copied. DMC's security defences seem primarily aimed at keeping people out, from preventing breaches at its perimeter. The company

seemed rather less focused on the enemy within, hence the three employees (who had authorised access to the data) were able to copy the files and exit the premises without having been challenged. Further, it seems relatively easy for them to have removed their location implants and to have disappeared without a trace.

3.4.7.5 Differences in legal regimes

In the first scene, MacDonald says he was questioned by a reporter about whether DMC was complying fully with the Safe Harbour Agreement. At this time (2007), there remains a difference between the privacy and data protection requirements in Europe and those in the United States. The Safe Harbour Agreement was supposed to ameliorate those differences, but questions have frequently been raised about its effectiveness and whether (some) companies are complying with the Agreement even if they say they are. The scenario suggests that DMC has largely ignored the Safe Harbour Agreement as it has sold data to a wide range of clients, including government agencies.

3.4.7.6 Honesty and trust

Given the lack of awareness of most people about the extensive records held by DMC, the issue of trust is not directly raised, but nevertheless it is an issue whenever a third party holds personal data, especially a lot of data as in the case of DMC. One would think that a data aggregator, processor and reseller like DMC would have some obligation to inform people whenever it sells data to others or takes over another company with personal data records. But this has not occurred. One could assume that some DMC clients such as the intelligence agencies and immigration authorities are content that individuals are *not* informed about what information DMC has on them.

In scene 1, we do not know the president's decision about whether to inform the police and individuals about the theft. Even so, MacDonald, the vice president in charge of media relations, does not hesitate in expressing the view that they should *not* inform the police or individuals. In any event, it seems DMC does not know (yet) whose records have been copied. In the United States, as mentioned in the footnote to Max Court's comment, California and a number of other states have strict laws requiring that companies *do* inform individuals when their data have been stolen or compromised – but that does not mean that they will. Compliance will depend as much on corporate culture and, especially, ethics as on legal deterrents. Senior managers must be seen to be fully compliant and to instil a culture of good corporate citizenship.

3.4.8 Legal synopsis

3.4.8.1 Global companies and local laws

DMC is active around the world. Which law will be applicable to which data collector and to which data processing? Is the Data Protection Directive 95/46

applicable outside the European Union? A second issue relates to the special provisions of the Directive concerning the transfer of personal data to third countries outside the European Union.

The first question is solved by Article 4 of the Data Protection Directive, which determines that the national law of the Member States will apply where the processing is carried out in the context of the activities of an establishment of the controller on the territory of that Member State. Such a requirement may often be fulfilled, even if we are not sure where the processing of data as such takes place. It may lead, however, to the application of many laws since most likely the data processor will be established in many states. Article 4 further stipulates that if the data controller is established on the territory of several Member States, he must ensure that each of those establishments complies with the obligations laid down by the laws applicable in each Member State. DMC has establishments in the United Kingdom, Japan and the United States. Article 4 (c) determines that if the controller is not established on Community territory, the national legislation of a Member State of the European Union will apply when the processor, 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. DMC could try to prove that the equipment in the United Kingdom is only used to transmit information to the United States or Japan, thus preventing the use of the Community legislation. However, the Article 29 Data Protection Working Party[161] interprets the term "equipment" broadly in the context of contemporary online services, covering, inter alia, personal computers which can be used for collecting data. Such interpretation broadens the application of the Data Protection Directive.

The personal data as well as the information and profiles deduced and extracted from the personal data are processed, transferred, licensed and otherwise traded on a worldwide level with hundreds of unknown clients. DMC grew through mergers and acquisitions and processes data (of European citizens) in many countries outside the European Union.

In regard to the second issue, Article 25 of the Data Protection Directive requires the third country to ensure an adequate level of protection of personal data before such data can be transferred to that country. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation.[162] Where, according to the Commission, a third country does not ensure an adequate level of protection, Member States should prevent any transfer of data to that third country. The Commission, on the other hand, may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international

[161] 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

[162] And, in particular, with regard to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures complied with in that country.

commitments it has entered into, particularly upon conclusion of the negotiations, for the protection of the private lives and basic freedoms and rights of individuals.

In execution of this Article, the European Commission has concluded the "**Safe Harbour Agreement**" with the United States, which aims to ensure the protection of personal data transferred from European Member States. Organisations that wish to obtain and maintain recognition of the fact that they ensure an adequate level of protection must subscribe to the principles provided in the agreement, reveal their confidentiality rules and fall within the competence of the US Federal Trade Commission (or any other body fulfilling a similar mission). When DMC transfers data from the European Union to companies in the United States, it must thus ensure that these companies have subscribed to the Safe Harbour Agreement. The European Commission decided in Decision 2000/520/EC of 26 July 2000 that the "Safe Harbour Privacy Principles" ensure an adequate level of protection for personal data transferred to organisations in the United States.

The issue of enforcement is a major problem in international relations. There has been criticism of the Safe Harbour Agreement. The main criticism is that it relies on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices.[163] Protection of personal data by the US administration was also tackled in relation to the processing and transfer of the passenger name records (PNRs) by airlines to the US Department of Homeland Security. Commission Decision 2004/535 EC of 14 May 2004, which stated that the US Bureau of Customs and Border Protection provides adequate protection of Passenger Name Record (PRN) data,[164] was annulled[165] by the Court of Justice. Following the Court judgment, negotiations began on a new PNR agreement, which the Council adopted.[166] However, both the European Data Protection Supervisor[167] and the Article 29 Working Party[168] expressed their lack of satisfaction with the new deal.

---

[163] http://www.privacyinternational.org/article.shtml?cmd[347] = x–347-82589& als[theme] = Privacy%20and %20Human%20Rights%202004#_Toc87939573

[164] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, *Official Journal* L 235, 6 July 2004, pp. 11–22.

[165] Joint cases C-317/04 and 318/04 *European Parliament* v. *Council* [2006]. See also Sturcke, James, and agencies, "US access to flight data unlawful," *The Guardian*, 30 May 2006.

[166] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) *Official Journal L 204/16, 4 august 2007*, pp. 16 , and Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), *Official Journal L 204/16, 4 august 2007,* pp. 18.

[167] Letter of the European Data Protection Supervisor, P. Hustinx, to Dr. W. Schauble, Minister of the Interior [of the EU presidency], dated 27 June 2007. http://www.epic.org/privacy/pdf/hustinx-letter.pdf

[168] Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007 (01646/07/EN-WP138). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf

The Commission also decided that Argentina (Commission Decision C(2003) 1731), Canada (Commission Decision 2002/2/EC),[169] Switzerland (2000/518/EC), Guernsey (2003/821/EC) and Isle of Man (2004/411/EC) offer adequate protection. Only a limited number of countries have received such recognition. Transfer to African and other developing countries could pose problems, since they probably do not provide an adequate level of protection.

Article 26 provides for an exception: "A transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection, may take place on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case." These conditions are clearly not fulfilled in this scenario. "A transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may also be authorized where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses." In these last two cases, the Member State has to give permission, which DMC does not seem to have acquired.

3.4.8.2 Monitoring employees

The scenario shows that employees at the workplace are continuously monitored, with cameras installed everywhere and with location implants.

The issue of privacy in the context of professional activities has already been discussed.[170] People should not lose their privacy at the office or in a professional environment. Until now, the Court of Strasbourg has not decided a case of permanent monitoring at the workplace. Systems such as those using biolocation implants that allow a permanent monitoring, even when one is not working (e.g., to trace somebody who violates the security obligations), will likely be found incompatible with Article 8 ECHR, which not only protects the private life but also the family life and the home. Professional location implants that enable

[169] There are, however, questions whether Canada offers adequate protection.

[170] See section 3.2.8.1.

monitoring of an individual's behaviour at home and in one's private and family life will most probably be refused (mainly for being disproportionate).

Additional arguments for this reasoning can be drawn from the Data Protection Directive prohibiting excessive processing of data, and requiring the processing data to be "relevant" and processed for legitimate purposes (Article 6 of the Data Protection Directive). Indeed, it is difficult to imagine how permanent monitoring can be considered relevant, necessary for legitimate purposes and not excessive. The Directive also prohibits as a rule the processing of sensitive data. Permanent monitoring will reveal such data, e.g., the subject's going to certain hospitals or to locations such as churches or political meetings.

There seems to be no margin of negotiation if you want to be employed by DMC. Also, the so-called consent in an employment contract must be viewed in the light of Article 7 of the Data Protection Directive which provides that personal data may only be processed if the data subject has unambiguously given his consent. In this case, it could be argued that employees were forced to give their consent – i.e., if they wanted to work at DMC, they have to give their consent.

DMC needs to be sure that confidentiality is respected. Article 7 (f) provides that processing can be allowed when necessary for the purposes of legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject. There needs to be a balance between the legitimate interests of DMC and the fundamental rights and freedoms of the employees, including the right to privacy. Even if tough security measures are required (as in case of the critical infrastructures), one could still question whether such intrusive measures are necessary.

The data are collected for a specific purpose, to ensure the confidentiality and business interests of the company (Article 6 (b), though the legitimacy of such monitoring might still be questioned as less intrusive means can ensure confidentiality). The information obtained via the location implants could be used for totally different purposes. As a data mining company, DMC might use location implants to collect as much information as possible. This could happen without the consent of the employees or for purposes not previously agreed. There seems to be a problem with the principle of proportionality.

It should be added, as an example, that Belgium's Collective Labour Agreement no. 81 of 16 June 1998 explicitly prohibits permanent monitoring of employees. This Agreement was conceived as an additional tool to strengthen the existing Belgian data protection law of 1992, amended in 1998 to implement the Data Protection Directive. Harmonisation in this field is clearly needed.

The case of permanent monitoring will probably provoke a lot of reactions in the future. Although there is no general prohibition against it, we could assume that it will not become a general practice in the next decades, with the possible exception of certain groups.

3.4.8.3 Global interoperability

Most developing countries have no AmI or similar networks, thus building individual profiles is difficult, if not impossible. The immigration authorities of developed countries rely on such profiles, and threaten to refuse entry to people from countries without AmI or compatible networks.

Interoperability is of major importance within the EU countries, and globally too. The **Directive on technical standards and regulations**[171] provides a co-operation and information procedure in order to develop European standards. At an international level, similar standardisation initiatives have been and are being undertaken.[172]

The majority of those standards are created in the developed world and in many domains, it is expensive to comply with them. Developing countries, as mentioned in the scenario, may not be able to afford compatible technology. To ensure maximum interoperability, initiatives are needed beyond those aimed at the creation of common standards. Countries should be able to develop the necessary infrastructure to comply with them.

This is, however, only one aspect of the problem. A fully operational, interoperable AmI world would be a threat for a range of fundamental rights such as privacy, non-discrimination, free movement, the right to anonymity, sovereignty of developing countries, etc.

3.4.8.4 Trading of personal data and the role of the data subject

DMC has been trading data. Questions have been raised about the accuracy of the data, and people were unable to correct false information. In fact, most people did not even know about DMC, nor about the profiles the company had built. Data processed by DMC have not always come from legitimate sources.

Illegal acquisition of data refers to the issue of data laundering, which has already been discussed.[173] DMC sells data, which is often misused for spam and other types of fraud. All of this implies that DMC does not respect the fundamental data protection principles as expressed in the Data Protection Directive and the Privacy & Electronic Communications Directive.

Even at the first level of the collection of personal data (before DMC acquires and processes them into profiles), data controllers have an obligation under Article 10 of the Data Protection Directive to inform the data subjects of any processing of their data, about the purposes of the processing and transmission of

---

[171] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, *Official Journal* L 204, 21 July 1998.

[172] Interoperability and standardisation have been discussed above in section 3.3.8.2.

[173] See section 3.2.8.8.

personal data to third parties.[174] Any further information such as the recipients or categories of recipients of the data, the existence of the right of access and the right to rectify their data is only required "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected to guarantee fair processing in respect of the data subject."

When personal data are disclosed to third parties, Article 11 ("Information where the data have not been obtained from the data subject") provides that the controller or his representative must, no later than at the time when the data are first disclosed, provide the data subject with at least the following information, except where he already has it: "(a) the identity of the controller and of his representative; (b) the purposes of the processing; (c) any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject."

Let us assume the personal data are made anonymous before they were received by DMC (which is not the case in our scenario, as the data are used to screen visitors and immigrants from developing countries). In this case, the analysis is different, since data protection law does not apply to the processing of the anonymous data by DMC. Of course, the act of anonymising data is a processing that falls under the Data Protection Directive, but if other data controllers do the processing before DMC receives the anonymous data, DMC is not bound by the rules of the Data Protection Directive.

3.4.8.5 IPR and personal profiles

DMC owns all intellectual property rights to its databases and its profiles, built upon (anonymous or identifiable) personal data.

The databases owned by DMC and other companies are protected by intellectual property rights. The **Directive on legal protection of databases**[175] provides for double protection of databases: a copyright protection and a *sui generis* right for the database.

Databases are protected by copyright if they, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation.[176]

---

[174] The right to information is discussed in sections 3.2.8.4 and 3.2.8.7.

[175] 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.

[176] As the author of the databases, DMC has the exclusive right to carry out or to authorise: "(a) temporary or permanent reproduction by any means and in any form, in whole or in part; (b) translation, adaptation, arrangement and any other alteration; (c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community; (d) any communication, display or performance to the public; (e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b)" (Article 5 of the Directive on the legal protection of databases).

Copyright protection does not apply to databases of which the contents are not selected or arranged through the author's *own intellectual* creation.

In an AmI world, service providers will use massive databases. They will not only use the content, but also the structure or selection or arrangement of the databases. AmI services will require the linking and integration of many databases. The protection offered is extensive and it is impossible to require a permission to reproduce, translate and/or communicate database content every time again. Article 6 provides for some exceptions to the exclusive rights of the author: "The performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database." It is unclear what must be understood by "lawful user". Depending on the interpretation, it could limit the scope of the exception to a greater or lesser extent. Article 6 also provides for optional exceptions to exclusive rights: "(a) reproduction for private purposes of a non-electronic database; (b) illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved; (c) use for the purposes of public security or an administrative or judicial procedure; (d) other exceptions traditionally authorised under national law."

The database can also be protected by a *sui generis* right. In order to obtain this *sui generis* protection, the maker of the database has to show that "there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database." The terms extraction and reutilisation are defined in a broad way (Article 7).[177]

Article 7 states that the *sui generis* protection shall apply irrespective of the eligibility of the contents of that database for protection by copyright and by other rights. This implies that the maker can obtain the *sui generis* protection even when the content consists of personal data. Although the user does not have a property right over his personal data, the maker of a personal database can obtain an exclusive right over the database containing such data. Article 8 gives the lawful users of a database the right, when the database is made available to the public in whatever manner, to extract and/or reutilise insubstantial (small) parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. There are limits to this right: the user may not perform acts that conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database and may not cause prejudice to the holder of a copyright or related

[177] Article 7 (2) states: "(a) 'extraction' shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form; (b) 're-utilization' shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community; public lending is not an act of extraction or re-utilization."

right in respect of the works or subject matter contained in the database. Data protection will apply in cases where personal data are involved (which will not allow making such a database available to the public).

Article 9 provides for a number of optional exceptions, analogous to exceptions to the copyright protection of databases discussed above. Certain exceptions to the exclusive right of the maker of the database are thus provided, but they only apply to "lawful users" and, especially, to the lawful user of a database *made available to the public*. Consequently, for example, in the case of profiling, these exceptions are rather limited or even non-existing. The right to freely use publicly available databases might be in contradiction with the right to privacy which prohibits the owners of databases from making them public. In an AmI world where massive amounts of information and databases will be exchanged and traded, the protection of databases might thus turn out to be a burden.

Compared to the exclusive rights provided to the author or maker of the database, the exceptions are rather limited and do not provide a solution to the fact that service suppliers will not be able to ask the author of the database for permission every time. Databases containing addresses, locations, weather information, sports results, pollen information, medical data … they all need to be coupled and need to co-operate to make AmI work. This is not possible in an intellectual property right system where copyright and database owners impose unreasonable prices, limit competition and make exclusive contracts with one company (excluding the other). Making databases available to the public may be difficult to reconcile with privacy and data protection law.

The **Copyright Directive**[178] is another instrument that has an impact on the intellectual property rights that are important for AmI. The Directive harmonises the three patrimonial rights that a copyright holder can enjoy, namely, the reproduction right, the right of communication to the public and the distribution right. It also reassesses the exceptions to the exclusive rights of the rights-holder in light of the new electronic environment. It provides for an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public (and to the distribution right).

The harmonisation is not absolute, since most exceptions and limitations provided are optional. The Member States are not allowed to provide exceptions other than those enumerated. An important exception for information technology concerns the exclusive right of reproduction: it allows certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject matter to be made. The acts of reproduction concerned should have no separate economic value of their own.

---

[178] 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. The anti-circumvention provision of this Directive and the Software Directive was discussed under 3.2.8.2.

3.4.8.6 Data theft

Three DMC employees have illegally copied and made off with the personal data on a lot of people. For a few weeks, DMC didn't say anything to anybody.

The employees have possibly committed criminal offences as defined in the Cybercrime Convention, such as computer-related fraud; however, there is a lack of provisions in the Convention which would directly criminalise data theft. This act is most probably also punishable under the national criminal provision on theft. The Data Protection Directive, on the other hand, might also support a case regarding the liability of the data controller (who is obliged to ensure the security of processing).

The Cybercrime Convention and the Framework Decision 2005/222/JHA[179] both deal with the liability of legal persons, which could be invoked in the situation described in the scenario, as DMC could be accused of neglecting to take sufficient care to protect the databases from theft.

3.4.9 Conclusions

The principal conclusion we draw from this dark scenario and its analysis is that, although we can expect amazing advances in the development and deployment of ambient technologies, there is a risk that corporate ethics in the year 2017 will not be so different from those prevalent in the year 2007, which is to say that some companies will be good corporate citizens and some will not. Similarly, some companies will have rogue employees just as they do today who are capable of undermining the efficiency and credibility of new data-processing algorithms. A principal difference between today's world and that depicted in the year 2017 could be that security concerns about terrorism and antisocial behaviour will be such that unless individuals have really detailed profiles compiled from data from AmI networks, they may be barred from entering a developed country. Also, while people may welcome the convenience from personalisation of services and the ubiquity of surveillance technologies, they may be lulled into a false sense of security.

In view of the advances in surveillance technologies, biometrics and fourth-generation mobile systems, the AmI community, policy-makers and society must be alert to possible abuses of the technology. Consequently, it is important to build in safeguards that minimise the risks, even though it must be recognised that the risks can never be completely eliminated, no matter how strong and comprehensive the legislative and regulatory measures are.

[179] The Cybercrime Convention, offences defined by it and Framework Decision 2005/222/JHA are discussed above in sections 3.2.8.7, 3.2.8.10 and 3.3.8.1.

3.5 Scenario 4: An early morning TV programme reports on AmI

3.5.1 The scenario script

3.5.1.1 Introduction

In the TV studios of an early morning news and variety show, a reporter/presenter is interviewing people who have made the news.

"Good morning ladies and gentlemen and thank you for joining us here on The Breakfast Show. Our guests today include a researcher in the Antarctic and the winner of last month's reality gardening show. We'll also have the latest traffic forecast across the city, which appears to be normal considering yesterday's chaos. The CO^2 pollution levels are below the threshold so all cars are allowed to enter the city centre. First though, we are pleased to welcome to the studio Markos, an MEP and one of the founding members of APPAG."

Scene 1: The Anti-Personalised-Profiling Action Group (APPAG)

Breakfast Show Presenter: "Markos, thank you for taking the time to join us today. Tell us about APPAG and how it came about."

"First off, Alexandra, I'd like to thank you for inviting me. APPAG is something I feel quite strongly about and I'm glad to have the opportunity to share it with your viewers. The initials stand for Anti-Personalised-Profiling Action Group. I would like to stress right from the beginning that we are not against aggregated profiling per se. In fact, I was an early adopter of the 'always-on' movement some 10 years ago during the broadband Internet/mobile convergence era. I am also used to being watched and surveyed at all times because of my position as an MEP. But I think a lot of people simply do not realise how much personal information they are constantly giving out.[180] *APPAG wants to raise public awareness about this issue and wants to warn people that personalised profiling is simply too risky. I joined APPAG after some bad experiences."*

"What kind of bad experiences?"

"First of all, during our last holiday, my wife and I discovered that we did not have access to the same information and services as other hotel guests. For example, there was a jazz concert in town during sunset but we did not get any information about it. We only found out the next day. I was really angry because my avatar knows I like such events. Also, the excursion to the old Roman ruins was already fully booked. We could only participate when paying a premium. This is so unfair. And do you know

[180] Tuohey, Jasey, "Government Uses Color Laser Printer Technology to Track Documents. Practice embeds hidden, traceable data in every page printed", *PC World*, 22 November 2004. http://www.pcworld.com/news/article/0,aid,118664,00.asp. See also Jardin, Xeni, "Your Identity, Open to All", *Wired News*, 6 May 2005. http://www.wired.com/news/privacy/0,1848,67407,00.html

why? Just because the company that has the profiling exclusivity on our family recently merged with another company. Because we did not opt in to their new travelling module, they ignored the travelling preferences of my avatar. And then suddenly, you realise how dependent you have become on these things."

"But is that solved now?"

"Yes, but … it set me thinking. What happens if you decide not to do it? I began to make a point of switching off my AmI sensors in public places so that my preferences could not be revealed and monitored. I'll leave them on in the home where I control the environment, or at work where there are confidentiality clauses protecting us but the moment I step outside I switch them off. A cumbersome procedure, a real hassle, but it can be done. The downside is that I now find myself missing out on announcements – including the emergencies – or special promotions that I would have liked to take advantage of. Recently, I was in the airport where I actually found that I was banned from the frequent flyers' lounge because their sensors objected to my sensors opting out! Even though I showed them my card, they still wouldn't let me in. Can you believe that? Why should I be denied entry? Now I can see that if I have my AmI sensors off at the airport, there's a distinct risk that I'll be stopped and searched and maybe miss my flight."

"But why would you want to switch …?"

"Because I value my privacy. I think a lot of people simply do not realise how much personal information they are constantly giving out. What I object to is the personal nature of this profiling. Personalised profiling leads to a lack of freedom in making a decision. Have you heard about the companies with plans to 'personalise' their self-service restaurants based on their customers' medical history? Imagine, you would like to have a steak but they give you a salad instead. … And what if insurance companies get involved and start raising your premiums because they found out that you are not doing a lot of physical exercise?

"I understand companies collect anonymous information to better serve their clients or for particular marketing purposes although this also has caveats that one should look into. But it's the idea that you are being personally profiled wherever you go that really concerns me. It is the amount, quality and accuracy of data related to you that is generated and collected and archived for eternity that makes me shiver. How do you know the choice proposed by an avatar is a consequence of your preferences or simply the imposition of a commercial agreement?"

"What do you propose then?"

"Some believe that anonymity is the solution but I am not sure about that. The system needs your identity and you must give it in order to get access to the services. I think people should stop giving their data away for profiling purposes because once the system has them, the profile is built, improved, linked, added with other information. And you know what the worst thing is? Even if you refuse any profiling, and you want to act as if you are anonymous, you fall within a profiled category called 'the anonymous'. It is even one of the best profiled categories …! You just can't escape it any more."

"You also say that we need to be careful when transferring human judgement and decision-making to computers."

"Yes, to give an example, a good friend was erroneously placed on a tourism black list. These lists are used by the major hotel chains to identify known troublemakers, people with bad debt or whatever the case may be. If you present yourself at a hotel reception desk without an advance reservation, the big hotel chains will run a quick profile on you. The problem is that that it takes time to go through the massive amount of data. As a result, an early warning system is set up that already gives suggestions after only five per cent of the data has been processed. Experienced hotel staff know how to deal with such preliminary profiles but in this case the lady in question was refused a hotel room. The situation was not rectified until the following day. In the meantime, my friend had to spend the night in a hotel that was dirty, noisy, dangerous and twice as expensive but it was the only one that accepted her cash and did not require the result of the standard profiling application. On top of this, her suitcase was stolen there. Who do you think is liable for that? Moreover, there will probably always be a record of this somewhere, even if it was cleared up the next day, and you never know if something similar might happen again. Not a very nice prospect."

"Tell us about what APPAG proposes?"

"Well, one of the fundamental areas we want to work on is the legal framework. Though the data protection act covers personal data, we feel that there is a grey area about what really constitutes personal data and under what circumstances data collection is legal. I would argue that many of your preferences and lifestyle choices are, in fact, personal data. Furthermore, as I said earlier, we want to raise public awareness about these issues. Many people do not know what information is being collected and do not even know they have the right to opt out. This must change."

Scene 2: AmI divides

"We now go live to New York where we are joined by Dr. Anthony Lazlo, a leading environmental scientist and pioneer of AmI for environmental protection who is very critical of current environmental protection programmes. Good morning, Anthony."

"Good morning, Alexandra, and thank you for the invitation to appear on your programme. I want to show you and your audience that our society is not making full use of the potential of environmental monitoring technologies but also that policy-makers need to understand that intelligent devices and intelligent agents alone are not going to solve the problem. The future simulations we will project are based on the widespread use of AmI sensors throughout Antarctica which have been collecting all sorts of information during the last 10 years."

"Can you tell us more in detail what you mean, Anthony?"

"Of course, and I will show it to your audience. Have a look at these images live from Antarctica, which has one of the harshest climates on earth. Within the GCP – the Global Conservation Project – we have spread thousands of sensors in the environment to constantly monitor climate change.[181] *That is because the costs of these tiny sensors – they are actually like smart dust*[182] *– have gone down drastically,*

[181] See Michahelles, F., et al., 2003.

[182] For details on the Smart Dust project, see http://robotics.eecs.berkeley.edu/~pister/SmartDust/

although it is still very expensive to cover such a big landmass, especially under inhospitable conditions. But it is necessary, as rising sea levels have caused much destruction in the last few years. Look also at the projected graph with the information we receive on the water temperature, sea level, air pollution, etc. Similar smart monitoring projects in sensitive zones all over the world would help us a lot in combating environmental hazards and disasters, and could save many, many lives."

"So why are we not doing it then?"

"Because there is not enough money for it. I mean, there is little commercial interest in this, so it needs to come from public funding, but political and governmental priorities are elsewhere. Now look at these images from a very different place, the hot and dry Saharan desert. These images came from a film shot by a camera crew that travelled recently to the region. Here, too, we can see environmental destruction. But here we do not have the technology to enable us to act quickly and remotely. But let me be clear about this. I'm not just talking about environmental issues. AmI technologies could have life-saving potential – if we were able to monitor the spread of certain viruses, for example, we could target immunisation programmes more effectively and stand a better chance of eradicating diseases. Medics working in the field here do not even have the latest 4G terminals with language translation and direct connection to medical laboratories."

"So you're saying more public money is needed?"

"Yes, but not only that. We want to draw attention to the fact that although in some places we have been able to use this technology and harness its full capabilities, there are many other regions in the world that could greatly benefit but which do not have the funds to make the necessary investment. That is not fair. It should not be like that."

"Thanks, Anthony, for drawing our attention to this issue. Any last messages?"

"Yes. It is not only about money nor only about technology. You can invest lots of money in technology implementations but if no political action is taken or if people and companies are not willing to change certain behaviours, then we are going the wrong way. All the money in the world would not be able to change that nor the most fantastic technologies."

"Unfortunately, we have to leave it there, Anthony. We now go to Iris for the most recent traffic information."

Scene 3: Public life disrupted by virus attack

"The traffic situation downtown is currently heavy but stable. The communication backbone seems to be coping today with the heavy traffic of all the machine-to-machine messages that maintain increased traffic throughput. Pollution levels are steady, the emergency response rate is up by a point, crime-monitoring is at alert level yellow, and the accident rate is close to zero. A distinct improvement compared to the situation at the same time yesterday. But let's talk to Peter, our correspondent at the city traffic office, for the latest news on yesterday's chaos."

"Good morning, Peter. Tell us what happened yesterday. Was it a virus attack?"

"Yes, it was. The city's intelligent traffic system went completely mad and the resulting traffic chaos was the worst we've seen in more than 15 years. Traffic lights kept on alternating every five seconds at random, for almost an hour. Cars were let

into the city centre without being automatically charged the congestion toll thus contributing to the general chaos; road works were wrongly announced creating queues of angry drivers complaining to technical staff and buses did not stop at (digital) requests. According to a traffic official, the centre's main server was attacked by a digital virus. Initially, the self-repairing anti-virus software was able to counter the attack and in order to completely eradicate the hybrid virus (or multipartite virus), the software had to search for, identify and download software updates. Unfortunately, an unknown Trojan was able to briefly take control of the traffic management system. Emergency back-up systems were able to restore control after 45 minutes, but the impact on the city traffic lasted for many more hours."

"Peter, what did traffic administration say about it? It was obviously a serious security breach."

"Well, during the crisis, it seems their primary goal was to restore the situation back to normal as soon as possible. Once that was accomplished, they started asking questions about the attack. Who perpetrated it? What was their objective? Was it a diversion for other types of attacks, such as crime, robbery, etc.? They are seriously considering the possibility that this may have been a malicious terrorist attack[183] *and are trying to find the missing links. Their specialists looked into the hybrid virus and the Trojan, and after analysis, they declared this morning that they were not dealing with a new-generation virus. The consequences would have been worse if this had been an attack using novel mutant type worms."*

"Is there a longer term impact of the attack?"

"Well, city officials aren't saying anything officially, but there's a rumour that the virus also caused partial loss of traffic data. That would mean that the traffic system has lost its intelligence and that it has to learn again to optimise traffic intervention measures. It could take up to two or three months, but again, this is an unconfirmed report.

"Officially, the city traffic experts say only the obvious, that security is critical in AmI environments like the traffic management system and that 'we' need to reduce the risks relating to the upgrading, maintenance and interoperability of such systems. Is that another way of saying they want more money? Who knows? Back to you, Iris."

Next, our events correspondent, Didi, is at the scene of yesterday's rock concert, where security fears prompted the evacuation of almost 50,000 people. Fans are now demanding their money back as it emerges mishaps with the technology used by event organisers may have been to blame.

Scene 4: AmI system aided mass risk management

"Here's Didi with our special report on the story." [Voiceover of report]

"Incidents in the past with big crowds led to the development of crowd management strategies supported by AmI technologies.[184] *AmI has proved to be effective in*

---

[183] Schneier, Bruce, "Identification and Security", *Crypto-Gram Newsletter*, 15 February 2004. http://www.schneier.com/crypto–gram–back.html

[184] Hogan, Jenny, "Smart software linked to CCTV can spot dubious behaviour", NewScientist.com, 11 July 2003. http://www.newscientist.com/article.ns?id=dn3918

facilitating intelligent communication among infrastructural elements (AmI sensors), event organisers, security managers and members of the crowd. Through the use of Edibles, Personal Wrist Communicators (PWC) and Disposable Wrist Communicators (DWC), crowds and individual movements are monitored continuously so that any incidents are noticed immediately.[185] *This time, however, the system did not function properly. The concert hall was evacuated completely because panic arose for no reason at all.*

"Last night, not everyone made the switch to 'Concert' mode. Early generation devices, very popular among the teenagers, were not sold with pre-prepared profiles and users of these devices had to create the profile manually; some did not do so. Other users simply did not download the concert profile as it was sucking up resources of their personal AmI devices. Thus, their AmI devices did not function properly. On the other hand, people with implants, through their intelligent proxies, were able to effortlessly negotiate, check and download the appropriate concert profiles. Also, people who had bought their tickets from ticket touts, habitually labelled 'clones', tried to mask their identity and assume the name corresponding to the ticket.

"The concert began with a great performance from The Tumbling Rocks. Suddenly people say they heard a loud bang. Witnesses at the scene described hearing something that sounded like an explosion. Others assumed this was just a part of The Rocks' act. Those members of the audience with personal devices running the concert profile instantly received 'no-panic' messages; others were not notified at all. The security resources control centre received various messages from the audience as well as from the arena AmI sensors and the ground patrol who immediately approached the scene. The first priority of the ground patrol was to arrest all 'clones' as a matter of precaution. In addition, a special report was sent to all emergency services that were on stand-by including the status of the AmI sensors in the area and the list of who was in the audience and of their personal AmI devices. An in-depth identification analysis of all clones was also initiated.

"Parts of the audience started moving away from the affected spot despite the fact that there was no cause for concern. Crowd behaviour monitoring devices detected this panic movement and the AmI system automatically initiated the evacuation plan for this part of the arena without alarming others. Then, confusion occurred as some people took decisions in spite of AmI recommendations while others were unaware of any abnormal occurrence. It was finally decided to evacuate the whole arena and the appropriate plan was put in motion. Apart from a few people being lightly injured and some 'clones' being arrested, the evacuation plans were executed perfectly. Even so, everyone felt disappointed and cheated that the concert had to be abandoned. Naturally, people want their money back."

Back in the studio, Alexandra thanks Didi for the report and passes on to her next guest, the winner of last month's reality gardening show. Life goes on even in AmI space.

---

[185] Upton, Mick, "Casual Rock Concert Events", June 2005. http://www.crowddynamics.com/Main/Concertrisks.htm

3.5.2 Analysis

3.5.3 The context

This scenario is intended to explore the implications of AmI technologies on a global scale and to consider risks for society as a whole. It highlights possible problems related to critical infrastructures, security and dependability. The scenario is composed of four interviews:

- The first deals with the application of personalised profiling in public spaces and voluntary exclusion from AmI services as a result of negative experiences (invasions of privacy, profiling, annoyance, etc.).
- The second tackles the issue of the digital divide.
- The third shows how AmI vulnerabilities and our dependence on critical infrastructure might affect public life.
- The last concerns application of AmI technologies for crowd management.

Scene 1

In this interview, a member of the Anti-Personalised-Profiling Action Group stresses the risks related to personalised profiling in public spaces as opposed to the milder risks as a result of aggregated profiling and underlines the lack of awareness of users and the lack of transparency on the part of service providers. Some critical situations are described:

- Being deprived of access to certain services or unable to get your leisure of choice
- Lack of freedom in decision-making
- Avoiding anonymity as it is a profiling category in itself
- The difficulty in recovering a "stable" (legitimate) situation as a consequence of transferring human judgement and decision-making to computers.

Scene 2

AmI technologies may contribute to improving the climate sciences,[186] by enhancing access to and integrating available information from sources such as electronic journals, satellite data, etc., including researchers in the global geoscience community and by enhancing virtual collaborations.

In addition, AmI technologies can help create a better understanding of climate change by enabling continuous monitoring and serving as an effective tool in reducing climate change impacts, such as natural disasters.[187] However, AmI

[186] Gettelman, A., "The Information Divide in the Climate Sciences", National Center for Atmospheric Research, May 2003. http://www.isse.ucar.edu/infodivide

[187] Müller, B., "Equity in Climate Change – The Great Divide", Executive summary, Oxford Institute for Energy Studies with the support of Shell Foundation. www.oxfordenergy.org/pdfs/great_divide_executive_summary.pdf

applications, installation and maintenance may have a prohibitive cost. The issue of digital divide at the global level is also addressed. The dark side has two manifestations: Not every country can benefit in the same way from AmI technologies, although the impacts are global. AmI technologies as such will not solve the digital divide problem. Effective distribution of organisational responsibilities and policy measures are needed as well.

Scene 3

This scene aims at raising awareness of our dependence on the infrastructure and the required level of security – a critical issue in AmI environments. Indeed, new technologies bring new vulnerabilities (as shown in the weakness of the self-repairing antivirus software). When they are exploited, the consequences (e.g., the traffic chaos caused by usurping control of the traffic management system) may be significant. A post-crisis analysis underlines the impacts and damages (e.g., loss of data) caused by this digital attack and the subsequent actions to be performed (e.g., application of learned lessons). With the complexity of the AmI environment and the increasing dependence on AmI-enabled services, security of systems becomes critical. They need to be protected from terrorists, common law criminals, hackers and software bugs.

Scene 4

The last interview recounts how continuous AmI monitoring of specific large public spaces such as a stadium and personalised communication to thousands of individuals may help risk management by establishing a direct channel of communication between people and event organisers in an emergency. The expected benefits are important, but the practice reveals some problems, such as inappropriate communication and confusion in the audience mainly due to lack of trust in the AmI suggestions. Even if the AmI system works as anticipated, the result might generate more inconvenience than benefit. In view of their ubiquity, AmI technologies and devices can help in risk management and crowd control, but challenges to their utility need to be pre-empted.

3.5.4 AmI technologies and devices

The scenario makes reference to several AmI or AmI-related technologies, including:

- Sensors
  - Tiny sensors (actually, smart dust) embedded in the environment with networking capabilities for monitoring climate change
  - Positioning
- Intelligent algorithms
  - Data mining (for providing personalised information such as about a jazz concert to hotel guests or for personalising self-service in a restaurant)

  - Self-repairing algorithms, e.g., to optimise emergency intervention in traffic management
  - Traffic-routing
  - Language translation
- Wireless and wireline communications networks enabling interworking of heterogeneous devices, including networked sensors, computers and diverse personal devices.

3.5.5 Applications

The AmI technologies referenced in the scenario are used in various applications, including

- Personalisation of services – AmI profiling aims at providing well-being and helping users in their everyday life. Several examples can be found in this scenario, such as hotel-restaurant services and establishment of a specific channel for emergency use.
- Environmental monitoring – AmI applications will enable continuous monitoring, even under hostile conditions, and provide information/data in order to help solve global problems.
- Traffic, emergency and crowd management – Because AmI technologies can provide more detailed, individualised, real-time location data from networked sensors, intelligent systems can be implemented for crowd configuration, proactive and adaptive evacuation and incident notification. The key technologies or devices in such management applications include:
  - Profiling (personalised or for a group), which can improve the responsiveness of the AmI environment.
  - Avatars used to encapsulate user experiences, preferences and wants.
  - Disposable (e.g., edible) communication hardware.
  - 4G terminals enabling language translation among many other services.
- Self-repairing antivirus applications – AmI technology makes it is possible to design self-learning intelligent systems.
- Security measures – AmI has the capability to support effective decision-making.

Because new technologies bring new vulnerabilities, some negative applications may arise, including

- Propagation of viruses – Inherent in the implementation of any AmI environment is the interoperability of different technologies. That interoperability requires metadata, and we could expect such metadata to be exploited or attacked by a new generation of powerful viruses, mutant worms that can adapt to network and device heterogeneity to spread and disrupt different AmI devices including back-up systems.

- Fraudulent gathering of personal information and profiles.
- Exclusion of people by placing them on a black list based on automatically gathered information.

3.5.6 Drivers

The four scenes in this scenario are impelled by several drivers, of which the following are the most important.

3.5.6.1 Individual and social concerns about the deterioration of the environment

As a consequence of this prevalent concern, individuals, scientists, social groups and others have begun using AmI to monitor changes in the Antarctic environment. It is simply beneficial to all to facilitate the use of such advanced technology everywhere.

3.5.6.2 The desire to control others and the external world

This driver makes use of technologies enabling monitoring, profiling and tracing. These technologies are based on an intensive collection of several types of data (location data, personal data, etc.). Generally, users are not aware of the collection processes. Consequently, two subsequent issues rise: difficulty in protecting personal data and loss of control.

3.5.6.3 The belief in technological progress

This driver is associated with the willingness of individual citizens and consumers to use and adapt their behaviour to the technological possibilities of AmI. Acceptance of and demand for AmI products and services will drive the development and provision of applications. Consumer understanding of the benefits of AmI applications and the effectiveness of human–machine interfaces are relevant issues.

3.5.6.4 Costs

The drive towards cost saving could give a boost to the implementation of AmI but maintenance and updating could be more costly than expected. Therefore, costs may be the source of the digital divide between countries and categories of users.

3.5.6.5 The desire to live a private life

The right to privacy is an important driver as well as a key issue, particularly as it concerns the protection of personal data from exploitation (i.e., identity theft). Privacy is likely to play a key part in user acceptability of AmI applications and services. It will drive people to select (or not) products or services that offer privacy protection; it also forces manufacturers and service providers to build into their products and services privacy-enhancing technologies.[188]

3.5.7 Issues

3.5.7.1 Individual (personalised) profiling vs group profiling

The following remarks are based on a report from FIDIS, an FP6 Network of Excellence on the Future of Identity.[189] Individual and group profiling capacities have grown exponentially as a result of both the huge advances in technology and the increasing availability of readily processable data and traces. Today, an individual – consciously and unconsciously, voluntarily and involuntarily – leaves a vast number of electronic traces in his wake, which can be processed and correlated. The use of the Internet, mobile telephones, electronic financial systems, biometric systems, radio frequency identification tags, smart cards, ubiquitous computing, ambient intelligence and so forth, all participate in the spontaneous and automatic generation of data that can be correlated.

Profiling is a core application that operates by distilling usable information from a large amount of unstructured, raw information. Group profiling technologies build on sameness in the sense of similarity (categorisation); personalised profiling builds on sameness in the sense of unique identification or continuity with oneself. Group profiles are often used to identify persons or to attribute a certain lifestyle, health risks, learning capacity or customer preferences to a person. Even when a group profile does not necessarily apply to the individual members of the group, it may still be used based on the probability that part of the profile does apply. As a result, service providers, insurance companies, forensic agencies, fraud detection departments or agencies and even e-learning organisations use profiling technologies to identify and categorise their target populations. Individual profiles contain personalised knowledge about specific individuals, inferred from offline and online behaviour, registration of birth and/or biometric data.

---

[188] European Commission, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM (2007) 228 final, 2 May 2007.

[189] http://www.fidis.net.

The proliferation of automatically generated profiles could have a profound impact on a variety of decisions that influence the life of European citizens. At the same time, it seems unclear whether and how a person could trace back (identify or determine) the sources if and when decisions concerning her life are taken on the basis of such profiles.

3.5.7.2 Victimisation/democratic right not to be treated as a criminal

AmI technologies could jeopardise the presumption of innocence to the extent that decision-making is delegated to a computer or if a desire for anonymity is considered suspicious. In the interviews in scenes 1 and 4, we have two examples which illustrate this point: Anonymity profiling and arrest of the clones (one category of user).

3.5.7.3 Digital divide

The digital divide basically refers to the gap between those communities or groups that have access to the Internet, ICTs or any emerging new technologies and those that do not and to the disparities regarding the ability to use them or to learn how to use them. The digital divide is a societal, economic and political issue, all rolled into one. It raises several types of problems and difficulties involving costs, culture, organisation, education, acceptance, adaptation, geography and demographics.

AmI has the potential to bridge certain aspects of the current digital divide but at the same time, it can be assumed that in the future, other and new divides based on AmI technologies will emerge. Problems can be global (between different countries) or local (between different regions in the same country), as raised in scene 2. Not every nation or region benefits in the same way or to the same extent from technologies.

AmI may have the potential to exclude and/or include sections of society. Some concerns are raised about the potential of AmI to widen the digital gap between those with access to AmI and therefore to better services and improvements in standards of living in "smart homes" and those without such access ("digital hermits").[190]

AmI and related technologies could be used as a policy tool and specifically as a tool for innovative social welfare, to improve access to and provision of services for previously excluded or less included groups (e.g., the disabled, ill and elderly).

3.5.7.4 Dependency

Dependency grows when a technology is widely used. Users become dependent when they do not remain indifferent to the consequences of technology use. This

[190] FTC, "Future Threats and Crimes in an Ambient Intelligent Everyday Environment," supplied by Qinetiq and Transcrime for IPTS/JRC under contract 2215-2004-06-F7SC SEV GB, July 2005.

can be joyful when the technology works or frustrating when it does not. The consequences of dependency might affect users in an individual way as well as in an aggregated way. Interview one shows the frustration of a user when his avatar does not fulfil his expectations and in interview three, we see dependency on the system and the subsequent impact when something goes wrong (e.g., a traffic jam when a virus affects the system).

3.5.7.5 Loss of control

The feeling of a loss of control has two main sources: a misunderstanding of the context and a lack of training.

Misunderstandings can arise where there is lack of trust. Misunderstanding of context (prompted by either technical or human factors) can generate dark situations. Table 3.1 shows the different cases. Interview four illustrates the case of misunderstanding due to human factors when finally no problem has occurred.

Users often need training to master new devices and services, and this will also be true of AmI technologies because collectively they will create a technological revolution as a function of their ubiquity. Users lacking training lack awareness of the possibilities of the new technologies (services, preferences setting, etc.) and the associated risks. Without a minimum of training, users will likely encounter some problems in getting services that fulfil their expectations and/or they will be confronted with unwanted AmI behaviour. Consequently, frustration and a feeling of loss of control may arise. Interview one depicts situations of being deprived of access to certain services and being unable to get what one wants as leisure.

Another aspect of loss of control arises when trust is not established between the user and the technology. Trust reassures the user in his willingness to use the technology and in his acceptance of technological behaviour. Trust may be the result of a good knowledge of how the technology works acquired by training or directly as a result of a positive experience.

Loss of control appears when the interaction between the user and a technology is not optimised, transparent or easy (i.e., it is complex). Indeed, this interaction is

Table 3.1 Different cases of misunderstanding

Factors leading to misunderstanding	Context	
	Problem	No problem
Technical	AmI sensors are not able to detect the problem	AmI sensors detect a problem
Human	AmI sensors are able to detect the problem but the user misunderstands the alert messages	AmI sensors are able to confirm no problem exists but the users do not trust the AmI recommendations

a crucial point for new emerging technologies. Optimal user interaction with technology entails three related challenges:

- User knowledge, i.e., the user should know how to manipulate the technology and take advantage of the available services.
- "Near zero" configuration, i.e., only minimal interaction should be necessary to perform a task.
- Trust, i.e., there should be minimal annoyance, minimal limitation on the data needed to use or share a service, adequate protection of user rights, privacy, reputation, etc.

3.5.7.6 Function creep

"Function creep" is an important concern, i.e., that technology and processes introduced for one purpose will be extended to other purposes that were not discussed or agreed at the time of their implementation.

3.5.8 Legal synopsis

3.5.8.1 Personal profiling

Service providers collect huge amounts of information and share it with other companies to offer more personalised services. This scenario raises concerns about personal profiling and the lack of public knowledge about this issue. Even an association has been created to fight against it.

Here again, the data protection rules apply, according to the **Data Protection Directive**. Personal data must be collected and processed for a specific purpose (Article 6 (c) of the Directive). When a profile is built upon personal data, the data protection law applies whether the profile is an individual profile (related to an identifiable person) or a group profile (related to a group of anonymous persons). Making the personal data anonymous is a processing that also falls under data protection laws. When an individual profile or a group profile (composed of anonymous data) is applied to an identifiable person, the application of a profile might also be subject to data protection law, obliging the controller to process the personal data on a legitimate basis.

If the personal data are collected and processed, the data subject has a right to be fully informed about the purpose, all phases and contexts of such processing.[191] If a purpose of processing includes the transmission of data to third parties, Article 11 of the Data Protection Directive obliges the third parties – the new controllers – to provide the data subject with the same information about the data processing.[192]

[191] The right to information was already discussed in sections 3.2.8.4, 3.2.8.7 and 3.4.8.4.

[192] For a discussion on Article 11, see section 3.4.8.4.

Such information rights are important since they indicate that profiles may be created. A health insurance company might seek to collect all possible data on a data subject's health from different sources. In this case, the user should be informed about this activity, the purpose for which the data are being collected and what is going to happen to the data.

AmI service providers will also be collecting sensitive data, defined by Article 8 of the Data Protection Directive as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". However, the processing of such sensitive data is in principle prohibited; nevertheless, the Data Protection Directive does allow the processing of sensitive personal data in some exceptional situations, as previously mentioned in section 3.3.8.4.[193]

On the basis of the data gathered, the insurance company may automatically decide to raise its premiums. But even if the personal data have been lawfully acquired, Article 15 of the Directive grants every person the right "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." There is an exception, "if that decision 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".

On the basis of the information collected, the MEP in scene 1 receives personalised messages. Although some might be useful, the data subject should have the possibility to refuse some or all of these personalised messages. Such a right can be found in Article 14 of the Data Protection Directive.[194]

Personalised messages will often be commercial messages. There are issues regarding commercial communication, opt-in and opt-out rules, and the obligation imposed by law that requires commercial communication to be clearly identified as such. It might be very important to ensure the user understands the message and distinguishes between genuinely useful and manipulative information (as discussed in section 3.2.8.9).

The persons who collect, process and/or receive the personal data should guarantee that the data protection rules will be respected. Current solutions do not provide a proper balance between the risk arising from profiling, consent for data collection and workability of the system; it is probably not feasible to expect that consent can be obtained each time such data are to be collected. The obligation of the provider to act in accordance with the principle of proportionality may be

[193] On sensitive data, see also section 3.4.8.2

[194] "The data subject has a right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."

relevant in resolving the issue. Similarly, the right of the data subject to refuse personal messages is, in fact, limited by putting on him the burden of un-subscription and the risk of losing the information or service in which he may be interested.

3.5.8.2 Service refusal and incomplete personal profiles

Concerns are raised in scene 4 about possible service refusal as a result of an inadequate profile check and the consequent harm suffered by the person confronted by such a situation.

When personal data are collected and processed, Article 6 (a), (c) and (d) of the Data Protection Directive provides that the personal data must be processed fairly and lawfully and that they must be adequate, relevant, accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate or incomplete data are erased or rectified. Article 12 of the Directive also provides for the right to access and rectify data. It says that every data subject has a right to obtain from the controller "without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions". On the basis of Article 12 (b), the data subject has to obtain from the controller "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data". This makes it possible to correct an incorrect profile. Also, the data subject can ask on the basis of Article 12 (c) of the Data Protection Directive that any rectification, erasure or blocking carried out be notified to third parties to whom the data have been disclosed. Such guarantees do not, however, entirely protect the data subject against use of the incorrect profile, especially since enforcing such a right can be difficult for the average user, or he may not know that an incorrect profile is being processed before the damage occurs. However, Member States are obliged to determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and check that these processing operations are examined prior to their start. The supervisory authority is also obliged to carry out prior checks following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.[195] Nevertheless, an ex-post guarantee of the data subject's rights is also necessary. In scene 1, the MEP recounts the story about a friend who was refused a room because the hotel had inaccurate data about her and did not respect several of the conditions described above. Unfortunately, it will be difficult

[195] Articles 18, 20 and 28 of the Data Protection Directive.

to hold the hotel liable for the incorrect profiling, not only because the profiling error arose from different data providers, but also because the causal link between the error and the damage will be difficult to establish. The difficulties are compounded by the fact that evidential issues (procedures) as well as tort rules and prerequisites (as causation) are regulated by national laws. It will also be difficult to meet the traditional tort law preconditions in such situations. The crucial question is: who should be held responsible or liable for the damage caused by the use of incorrect data? The error could have been caused by input of incorrect information. Or the hotel might have created a bad profile through misuse of correct information. According to Article 23 of the Data Protection Directive, however, any person who has suffered damage as a result of an unlawful processing operation or violation of national data protection law is entitled to receive compensation from the controller for the damage suffered. This is a strict liability, but the national law may exempt the controller from this strict liability if he proves that he is not responsible for the event giving rise to the damage. This means that a reversal of the onus of proof may be foreseen: the data controller may be allowed to prove that he is not responsible for the damage

The creation of wrong profiles on the basis of a request for the service and an automated decision based on the profiles must be examined against the antidiscrimination rules.[196] Profiles or decisions based on inadequate criteria (health data, nationality, income, etc.) may lead to discrimination. However, it is difficult to determine when it is objectively justified to use such data and criteria and when they are discriminatory. Further clarifications will be necessary as we enter the AmI world.

3.5.8.3 Digital virus damages public transport system

In scene 3, someone creates a virus that causes chaos and damages to the transport system. The person who did so committed several offences as defined in the Cybercrime Convention.[197] The majority of the criminal offences defined in the Cybercrime Convention require proof that the perpetrator had the intent to commit the specific crime. When a virus is created, however, it could be argued that a specific aim or intention does not exist. That is why in some situations the specific intention should not be a precondition of (criminal) liability. Even when there was no malicious intention, the creator could still be liable for the civil damage caused.

The creator of the virus might be untraceable. Thus, the focus shifts to the question of whether the providers of the different traffic services were protecting their system sufficiently against these attacks. Problems will arise when trying to prove which service provider was responsible for which part of the damage. The principles set out in the Directive on liability for defective products[198] could solve part of this problem if it were applicable to services and software.

---

[196] On non-discrimination, see section 3.3.8.4.

[197] On the Cybercrime Convention, see sections 3.2.8.7, 3.2.8.10 and 3.3.8.1.

[198] For our discussion of the Directive on liability for defective products, see sections 3.2.8.3, 3.3.8.1 and 3.3.8.3.

3.5.8.4 Pseudonymous authentication

Temporary wireless pseudonymous authentication is possible thanks to new technology such as sensors and implants. In scene 4, implants were used for the crowd management application.

Only the issue of medical implants has been addressed in the European Union. The **Directive on the approximation of the laws of the Member States relating to active medical devices**[199] was intended to harmonise the level of safety by mandatory specifications relating both to the technical safety features and the inspection procedures for a number of medical devices, including active implantable medical devices. The Directive sets out strict rules. In an AmI world, however, implants might be used for non-medical purposes.

In scene 4, the concert organiser needs to ensure the safety and security of the people attending the concert. To this end, people carry chips that transmit an identity assigned to each person until the end of the concert. The chips enable concert-goers to remain anonymous and allow the concert organisers to check the behaviour of people at the concert. Thus, there is a balance between privacy and security, in keeping with Article 8 of the ECHR which protects the personal life of individuals. This protection implies the right to be anonymous. However, swallowing chips or using implants will not necessarily be regarded as a proportionate means to ensure safety. Less intrusive means (temporary chips in tickets or PDAs) could be envisaged, even if they might be less effective than intelligent implants[200] (as was the case in the scenario).

Even when technology seems to offer intelligent solutions to safety vs. privacy problems, the traditional logic of human rights law has to be applied, i.e., the principle of proportionality and necessity. The Luxembourg Court of Justice of the European Union has held in the Adidas case[201] that "It is apparent from both the abovementioned case-law and Directive 95/46 that protection for the sphere of private activity of natural and legal persons occupies an important place among the legal principles introduced by the Community legal order. However, that protection neither can nor should be absolute. The Court of Justice has held that restrictions may be imposed on fundamental rights provided that they in fact correspond to objectives of general public interest and do not constitute, with regard to the objectives pursued, a disproportionate and intolerable interference which infringes upon the very substance of the right protected."

The same spirit has inspired the authors of the Data Protection Directive. They did not consider the right to protection of privacy as absolute, which would mean a general prohibition on selecting and processing personal data. Rather than laying down an absolute prohibition, the Directive indicates the need to ensure a balance

---

[199] 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.

[200] The scenario mentions the possibility of a lawsuit for damages caused by the improper functioning of the crowd management application. For our discussion on liability and possible damages, see sections 3.2.8.3, 3.3.8.1 and 3.3.8.3.

[201] Case C-223/88 Adidas AG [1999] ECR I-07081.

between the interests involved and having particular regard to the principle of proportionality. The processing of personal data must therefore be carried out with the consent of the person concerned "or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person." The processing must also relate to data that are "adequate, relevant and not excessive in relation to the purposes for which they are processed."

Not all concerts create safety problems. The concert organiser will need to ask the people attending a concert for their consent to use intrusive technologies. New technological developments such as those described in the scenario offer possible solutions to the problems of striking a balance between traditional privacy and security. Their use has to be carefully assessed within the framework of human rights law. In countries such as France, the data protection authorities play an active role in seeking this balance and have implemented a licence system obliging those who are responsible for the processing to declare their processing and to obtain permission in advance.

3.5.9 Conclusions

The risk society is the key theme of this scenario. The four scenes depict dark situations, which stem from an inappropriate use, application or management of AmI technologies and which may generate a wide range of impacts on citizens, groups or even society. The four scenes raise private and public concerns, which have local and global scope. The scenes posit several problems related to the proliferation and protection of personal data, user acceptance, dependence, costs and enhancement or loss of trust. The scenario deals with issues including victimisation, digital divide, categorisation of users, dependency, loss of control and function creep.

All of these issues could lead to a major risk, that of an identity crisis. The risks at this level can be seen as a triptych:

- At an individual level, where you are unable to get what you want.
- At a social level, where you may be excluded because of the relatively high cost of new technologies.
- At a societal level, where one may be victimised through loss of social and legal recognition. This means:
  - One may become suspect by default, because acting anonymously may be considered as suspicious.
  - One may become an unrecognised person by law and may suffer impersonalisation and/or misrepresentation. Indeed, in cases of fraudulent usage of personal data, it would be difficult to recover a normal situation or reputation in view of the AmI environment's voracious appetite for personal data, a difficulty compounded where the individual lacks adequate legal resources.