available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy, trust and policy-making: Challenges and responses

David Wright[a], *Serge Gutwirth*[b], *Michael Friedewald*[c], *Paul De Hert*[b], *Marc Langheinrich*[d], *Anna Moscibroda*[b]

[a]*Trilateral Research and Consulting, London, United Kingdom*
[b]*Center for Law, Science Technology & Society Studies at the Vrije Universiteit Brussels, Brussels, Belgium*
[c]*Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany*
[d]*Faculty of Informatics, University of Lugano, Switzerland*

Keywords:
Ambient intelligence
Profiling
RFID
Data Protection
Privacy
Information Society Policies

ABSTRACT

The authors contend that the emerging ubiquitous Information Society (aka ambient intelligence, pervasive computing, ubiquitous networking and so on) will raise many privacy and trust issues that are context dependent. These issues will pose many challenges for policy-makers and stakeholders because people's notions of privacy and trust are different and shifting. People's attitudes towards privacy and protecting their personal data can vary significantly according to differing circumstances. In addition, notions of privacy and trust are changing over time. The authors provide numerous examples of the challenges facing policy-makers and identify some possible responses, but they see a need for improvements in the policy-making process in order to deal more effectively with varying contexts. They also identify some useful policy-making tools. They conclude that the broad brush policies of the past are not likely to be adequate to deal with the new challenges and that we are probably entering an era that will require development of "micro-policies". While the new technologies will pose many challenges, perhaps the biggest challenge of all will be to ensure coherence of these micro-policies.

1. Introduction

More than a century ago, Warren and Brandeis defined privacy as the right to be let alone and their concern about privacy was prompted by a new technology, i.e., photography.[1] Their perceptions then have some interesting parallels with today when some have expressed concern about Europeans (and perhaps especially the British) living in a surveillance society. It has often been noted in recent times that Londoners are photographed more than 300 times a day on average. There are surveillance cameras on the London Underground, on the buses, in shops, in office buildings, on the streets.[2] While there

[1] Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, No. 5 [15 December 1890].

[2] The UK Information Commissioner warned Parliament that the UK was in danger of "sleep-walking" into a surveillance society. Doward, Jamie, "Data tsar attacks surveillance UK", *The Observer*, 29 April 2007. http://observer.guardian.co.uk/uk_news/story/0,,2068077,00.html. A similar warning came from a parliamentary committee in June 2008. See House of Commons Home Affairs Committee, *A Surveillance Society?* Fifth Report of Session 2007–2008, Volume I, HC 58-I, London, 20 May 2008. http://www.publications.parliament.uk/pa/cm/cmhaff.htm.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2008.11.004

are more surveillance cameras (''spy drones'',[3] microphones[4] and loud-speakers are being introduced too) in London than anywhere else, other cities are also adopting similar technologies and for similar reasons.[5] While facial recognition technologies have not yet developed to the point where it is routinely possible to identify anyone who is captured on a video, we can suppose that day will come, and perhaps sooner than some might think.[6] But concerns about living in a surveillance society melt away in the face of a terrorist attack or a terrorist attempt such as those in London in July 2005 and, more recently, the failed attempts in Cologne in July 2006 and in London and Glasgow in June 2007. Then, the public is relieved that there *are* surveillance cameras and that they help to identify would-be terrorists quickly.

Similarly, there are concerns that more than 4 million people in the UK populate the national DNA database, but that database has been instrumental in apprehending many rapists, murderers and other evil-doers, sometimes many years after a crime has been committed.

Others may express concerns about a national network of digital medical records, its potential for abuse (especially discrimination if insurance companies are able to tap into it), but if it can save lives, lead to faster and more accurate treatment, then how should policy-makers and health authorities respond?

At the same time, many citizens voluntarily provide personal information to commercial social networking websites such as Facebook, MySpace and Bebo, often disclosing very private details (party pictures,[7] confessions[8] or their love life[9]) without realising[10] (or caring[11]) that this information not only may be disclosed to a potentially very large audience, but also indexed[12] and thus becomes trivially locatable. The same people who think little of exposing themselves on social networking websites would probably be mightily upset if intruders stole their identity by capturing their personal details from their computers. Similarly, some people are prepared to give away personal data in exchange for the perceived benefits of a supermarket loyalty card, even though they object to being sent unwanted advertising in the post or being spammed every time they open their e-mail programs.

Beyond the voluntary exchange of personal data, people are sometimes compelled or virtually compelled in some circumstances to surrender their personal data in order to gain something. To get a mortgage, borrowers must provide the lender with lots of personal data. It can be argued, of course, that borrowers have a choice here – they can choose not to give up such data, but the downside is that they do not get the mortgage.[13] Even if the lender (or the airline or supermarket chain) sets out its privacy policies on its website, can it be trusted? Moreover, how many of us have the time or inclination to read through (let alone scroll through) long and detailed privacy policies? And, even if we did, how many can actually understand them?[14]

These and many other examples highlight the difficulty in developing privacy-protecting and trust-enhancing policies. It may even be difficult to write domain-specific policies, because even within the same domain, differing circumstances may call for differing privacy protections.

There are lots of ambiguities, uncertainties and risks today concerning our privacy and trust, but in a ubiquitous Information Society, these ambiguities, uncertainties and risks will multiply many times over. When virtually every

[3] Orr, James, and agencies, ''Police send 'spy drone' into the skies'', *The Guardian*, 21 May 2007. http://www.guardian.co.uk/crime/article/0,,2084801,00.html.

[4] Johnston, Philip, ''Big Brother microphones could be next step'', *The Telegraph*, 2 May 2007. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/02/nbigbro02.xml.

[5] See, for example, Smith, Stevie, ''New York to introduce 3,000 new surveillance cameras'', Monstersandcritics.com, 10 July 2007. http://tech.monstersandcritics.com/news/article_1328226.php/New_York_to_introduce_3000_new_surveillance_cameras_.

[6] Face recognition was tested by German authorities in the Mainz Railroad station in 2007. While protests of privacy advocates and supervisors had little impact, the project was quietly terminated when it turned out that face recognition technology did not provide the expected recognition rates in realistic environments. Weimer, Ulrike, ''Augen des Gesetzes'', *Die Zeit*, 5/2007, 25 January 2007. http://images.zeit.de/2007/05/T-Biometrie.

[7] See, for example, Foster, Patrick, ''Caught on camera – and found on Facebook'', *The Times*, 17 July 2007. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2087306.ece.

[8] See, for example, Czekaj, Laura, ''Workers fired over Internet postings'', *Ottawa Sun*, 17 January 2007. http://cnews.canoe.ca/CNEWS/Canada/2007/01/17/3394584-sun.html.

[9] See, for example, Beal, Andy, ''Your Online Identity Could Ruin Your Love Life'', *Marketing Pilgrim Website*, 10 April 2007. http://www.marketingpilgrim.com/2007/04/your-online-identity-could-ruin-your-love-life.html.

[10] Gross, Ralph, and Alessandro Acquisti, ''Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook'', Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, UK, 2006.

[11] See, for example, discussion posts at http://internetducttape.com/2007/03/08/how-to-use-facebook-without-losing-your-job-over-it/.

[12] See, for example, Zimmermann, Kate, ''Facebook Opens to Search Indexing'', *SearchViews Website*, 5 September 2007. http://www.searchviews.com/index.php/archives/2007/09/facebook-opens-to-search-indexing.php.

[13] See Gutwirth, Serge, *Privacy and the information age*, Rowman & Littlefield, Lanham, 2002, p. 53: ''Before granting a loan or credit, a banker will want to know whether the client makes enough money, lives frugally, how money is spent and other information on the individual's personal life. A salesman must be sure a client is creditworthy. A life insurance salesman wants to limit any risk and will inquire about the health and medical history of a prospective client. Home owners look into the social habits and creditworthiness of potential tenants. The list goes on and all these examples have one common denominator: the lopsided balance of power forcing the weak party to surrender information. The banker and insurance salesman do not have to shed any personal information. It is one-way traffic forcing the weak party, either legally, contractually or out of sheer need, to surrender privacy.''

[14] A recent study in the US found that people with a high school education can easily understand only one per cent of the privacy policies of large companies. Story, Louise, ''F.T.C. Member Vows Tighter Controls of Online Ads'', *The New York Times*, 2 November 2007. http://www.nytimes.com/2007/11/02/technology/02adco.html?ref=technology.

manufactured product is embedded with an electronic tag (an RFID or a particle of ''smart dust''), when ''things'' can communicate and network, the complexities we face today will seem as nothing, as simplicities and trivialities compared to the world we can see rapidly approaching. When ''intelligence'' is embedded in everything, negotiating privacy rights with service providers will not be practicable or feasible, at least not in many circumstances.

Further complicating the picture is the value of privacy protection and enhancing trust. Some service providers today view measures to protect privacy and enhance trust simply as regulatory barriers. And it is easy, unfortunately, for many policy-makers, regulators and other stakeholders to agree with them, especially when there is a determined effort to reduce red tape, to ''free'' enterprise, to improve the competitiveness of European industry, especially against industries in other countries that do not adhere to European values.

2. Shaping policies

It is perhaps stating the obvious to say that new and emerging technologies, especially those that are leading us towards the ubiquitous Information Society, present fundamental challenges to notions of privacy and trust, however these are defined and whoever might hold such notions. These developments require policy-makers, industry and other stakeholders to assess existing policies and safeguards and, if necessary, build in new ones that will better protect the privacy and preserve the trust of citizens. This is not to say that curbs or restrictions need to be placed on the technologies or their further development. Society's attention should rather be on how those technologies are used, to which needs and prospects they respond, who uses them and for what purpose.

Shaping policies is becoming more difficult as new technologies make their way to the marketplace. RFID tags are a good example. While they make eminent economic sense in terms of tracking inventory and product flow, for simplifying passage through subway turnstiles, of implementing road tolls and much else, they have prompted privacy fears and trust concerns too. Will RFID help increase the efficiency of data mining and data aggregation operations and thus reveal more about the products we buy or use, or where we have been? Can we really trust the shop owner or corporate marketing department that RFID tags will be disabled once we have bought a new jumper? Will the widespread adoption of RFID fan mission (or function) creep? Will purpose limitation principles prevail?

RFID tags are just one of an array of new technologies that will populate the world of ambient intelligence. Like many others, ambient intelligence (AmI) technologies, developed for one purpose, may be ''re-purposed'', i.e., used for a purpose other than that for which they were developed. Re-purposing is already a well-known phenomenon in database management.

Policy-making is an exercise in trust, just as surely as having confidence in supplying Amazon or e-Bay with our credit card details. Stakeholders need to trust policy-makers, and policy-makers need the trust of stakeholders if new policies are to be developed to protect privacy or to fairly trade it off against some perceived greater social good.[15]

3. Policy-making challenges

In this section, we identify various social, political, technical and economic challenges to privacy policy-making posed by the development and deployment of new information technologies, notably in the emerging world of ambient intelligence.

3.1. *Societal challenges*

A significant number of challenges to privacy policy-making are primarily *societal* in nature. Here are some examples:

- Reconciling or at least dealing with the differing interpretations of privacy and trust among different stakeholders and the differences in interpretations and attitudes over time.[16]
- Engaging stakeholders, including the public, in cases where privacy rights are at stake. Given the changing interpretations of privacy, engaging stakeholders cannot be a one-off exercise. The fact that stakeholder consultation may be necessary in some instances raises the usual questions about how extensive the consultation should be, appropriate consultation mechanisms and alternatives to counter consultation fatigue among stakeholders. In fact, engaging

[15] Or even trade-offs within families, e.g., the father who uses GPS to track where his teenager is when the latter borrows the family wheels for a night out on the town. See, for example, Olson, Elizabeth, ''Peace of Mind When They Ask to Borrow the Car'', *The New York Times*, 3 November 2007. http://www.nytimes.com/2007/11/03/business/yourmoney/03money.html?_r=1&ref=technology&oref=slogin.

[16] Three drivers of changing interpretations of privacy are

- technologies – existing, new and emerging technologies for collecting and analysing personal information from multiple, disparate sources are increasingly available to individuals, corporations, and governments;
- societal shifts – changes in social institutions, practices, behaviour;
- discontinuities – events and emergent concerns that transform debate about privacy in a very short time (and thus do not allow for gradual adjustment to a new set of circumstances). The most salient example in recent years concerns the events of 11 September 2001, which transformed the national environment and catapulted counterterrorism and national security to the top of the public policy agenda.

See Waldo, James, Herbert S. Lin and Lynette I. Millett, *Engaging Privacy and Information Technology in a Digital Age*, Computer Science and Telecommunications Board, National Academies Press, Washington, DC, 2007, p. 3. The authors also note elsewhere (p. x) that ''the notion of privacy is fraught with multiple meanings, interpretations, and value judgments . nearly every thread of analysis leads to other questions and issues that also cry out for additional analysis – one might even regard the subject as fractal, where each level of analysis requires another equally complex level of analysis to explore the issues that the previous level raises.''

stakeholders should go further than consultation; stakeholders should be participating in framing the issues, questions and responses.
- Developing and strengthening trust-enhancing mechanisms and analysing their applicability to different stakeholder groups, different domains and differing circumstances.
- Understanding stakeholder (including the public) perceptions of trustworthiness and how such perceptions can be accommodated or changed.
- Making trade-offs (balancing competing interests) between privacy (and trust for that matter) and other values and societal demands (e.g., between individual privacy and collective security). In some sense, privacy and trust are also competing values: privacy entails secrecy while trust thrives on openness and transparency.
- The fact that trade-offs are sometimes necessary should not be taken to mean that trade-offs are *always* necessary. In some cases, careful design and planning will minimise the trade-offs that are needed to attend to societal needs without compromising personal information.[17]
- The nature of public debate – ''Debate should avoid demonization. Most threats to privacy do not come from fundamentally bad people with bad intentions. Demonization tends to make compromise and thoughtful deliberation difficult.''[18]
- Combating the exploitation of the privacy of the young and disadvantaged – Are rules needed, now or in an AmI future, to govern so-called behavioural or personalised advertising that (intentionally or unintentionally) exploits the privacy of the young or disadvantaged (as well as the rest of us), not only when we are sitting in front of a computer or using a mobile device but when we are moving through some embedded environment? Should consumers be able to filter such personalised advertising, so that they receive only those adverts in which they think they might be interested?
- Will the lack of personal data lead to discrimination and/or widen the digital divide?[19]
- Building trust in the ubiquitous Information Society will be a challenge for the foreseeable future. Those who have experienced online identity theft (a growing percentage of the population) may be more reluctant to engage in e-commerce. More evidence is needed on this point – it is possible, even likely, that those who have been victims of online identity theft continue to use online services that require personal data, notably one's (new) credit card number. Why? Perhaps because they have accepted that identity theft is just another risk that one encounters in our increasingly interconnected and inter-dependent world.

Is privacy like virginity – once lost, it can never be recovered?[20] How should we prepare for a scenario that suggests that with ubiquitous networking the notion of privacy will become a historical relic – i.e., there will be so many devices collecting, storing and processing our data and tracking everything that we do that people will have virtually no guarantee of privacy? Arguably, there is so much personal data ''out there'' *already* that people's expectations of privacy are actually unrealistic now. Our focus may need to shift from expectations of privacy to how data about us are used.

3.2. *Political challenges*

Some of these challenges will require shifts in policy frameworks. European policy already faces challenges, for example:

- Achieving coherence in privacy protections among the Member States.
- The need to take account of the differences in contexts and yet to ensure coherence in policies applicable to the differing contexts.
- Raising the bar for privacy and data protection between Europe and non-European States.
- Framing privacy impact assessments (aimed at determining what is at stake and who the interested parties are[21]). Privacy impact assessments should consider both the tangible and intangible impacts, for example, including ''chilling'' effects.
- Curtailing or dealing with or making explicit instances of mission (or function) creep. This occurs when data collected for one purpose can be re-used for another purpose, which may or may not have been recognised at the time of the data collection. In some cases, the function creep (or re-purposing, as it has also been termed) originates from a third party, for example, when intelligence agencies or law enforcement authorities want access to telecom customer records or library records.
- The adequacy of privacy policies, both governmental and non-governmental, including public understanding of those policies.
- Ambient intelligence will bring much closer the convergence of the virtual and real worlds (Second Life gives us a taste of such convergence).[22] How should privacy principles (whatever they might be) apply in a converged world?

[17] Waldo et al., p. 5.

[18] Waldo et al., p. 13.

[19] The third SWAMI dark scenario suggests that immigration from developing countries to developed countries could be curtailed if the developing countries do not have AmI networks in place because it will not be possible to assess whether a given immigrant represents a security risk. See, Wright, D., S. Gutwirth, M. Friedewald et al., *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008. An abridged version of this scenario and its analysis can be found in Wright, David, et al., ''The Illusion of Security'', *Communications of the ACM*, Vol. 51, Issue 3, March 2008.

[20] See O'Harrow, Robert, *No Place to Hide*, Simon & Schuster, New York, 2005, p. 107: ''We have created a unique identifier on everybody in the United States'', said [Ole] Poulsen, the company's [Seisint Inc.] chief technology officer. ''Data that belongs together is *already* linked together.'' [Italics added.]

[21] A privacy impact assessment could start off with three basic questions:

- What is the information that is being kept private (and with whom is that information associated)?
- From whom is the information being withheld?
- What purposes would be served by withholding or not withholding the information, and whose interests do those purposes serve?

[22] See, for example, Johnson, Bobbie, ''Police arrest teenager over virtual theft'', *The Guardian*, 15 November 2007. http://www.guardian.co.uk/technology/2007/nov/15/socialnetworking.news.

- Deciding the most appropriate mechanism for dealing with privacy issues. Some issues can be left to common sense or courtesy (supported by education and the media), others can be dealt with by incentives (e.g., if you want a contract or grant from the EC, then you must address the privacy implications of your proposed project), while still others can be subject to legislation.[23]

Of particular interest will be challenges created by the friction between national security and personal privacy, such as the following:

- Examining how much freedom of choice individuals have in their decision-making when their privacy or personal data are involved. For example, a prospective immigrant or visitor may need to supply his or her medical records or submit to health checks if he or she wants to enter a country. Biometric data are increasingly required to travel from one country to another, which some have criticised not just on privacy grounds, but on cost.[24]
- Avoiding chilling effects. For example, would people attend a political rally or protest demonstration if they knew facial recognition technology and surveillance cameras could identify them? Will people be more circumspect in what they say or communicate if they know that everything they say or write is being or could be monitored?[25] If someone does not agree to supply certain personal data (e.g., in an application for employment or to attend a university or to get health insurance), will they automatically become suspect?

Equally important is the issue of enforcing privacy and data protection policies and laws, where issues such as the following arise:

- Enhancing the enforcement of data protection rules and rights. Are the powers of the data protection authorities proportional to their mission (or are they just paper tigers)? How should data subjects be practically empowered to claim their data protection rights and obtain their respect?
- Liability and restitution issues. Who is to be held liable for a privacy infringement? Who should make restitution or be penalised? What is an appropriate penalty? How adequate are the liability rules? How easy or difficult is it for individuals to press for restitution?
- Dealing with friction and jurisdictional issues between organisations, levels of government and sectors. Some government departments and/or agencies may clash on how they should deal with certain privacy or data protection issues. For example, the UK Information Commissioner recently told law enforcement authorities that they must delete or expunge certain personal data from their databases.[26] With adoption of the EU's Data Retention Directive (2006/24/EC), European legislators gave greater weight to the arguments of the security forces about the need to force telecom companies to retain customer billing data in case such data might be needed in the fight against terrorism than to the data protection authorities who regarded the Data Retention Directive as curtailing the Data Protection Directive (95/46/EC).

3.3. *Technical challenges*

The fast-paced development of technology will in itself create a range of challenges to our notions of privacy and trust, such as these:

- Recognising and understanding the potential impact of new technologies (such as AmI) on privacy, e.g., new algorithms that might assist data mining and data aggregation to compile profiles on specific individuals using what heretofore was thought to be non-identifiable data.
- Will a fully deployed AmI world make opt-in infeasible? How will it be possible, even technically possible, to opt in to an environment embedded with a multiplicity of networking sensors serving a multiplicity of different purposes?
- The adequacy of standards and guidelines (e.g., those of the ISO or OECD) in an AmI world.
- In an AmI world, how will we define what are ''appropriate technical and organisational measures to protect personal data''?[27]

[23] Waldo et al., pp. 6–7, distinguish five types of policy actions – i.e., limits on the information collected and stored (data minimisation), limits on outsider access (access control), prevention of internal abuse (insiders taking advantage of their position), notification and correction.

[24] In the UK, all foreign nationals will have to carry biometric ID cards from 2008 and from 2010 all UK passport applicants will be issued with them, and by 2017 all UK residents will be on a national identity database. Johnston, Philip, ''All UK citizens in ID database by 2017'', *The Telegraph*, 6 March 2008. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/03/06/nid506.xml. But the move has faced heavy criticism. ''The introduction of identity cards and biometric passports has been denounced as 'a vast waste of taxpayers' money' after the release of a Government estimate putting the cost of the scheme at more than £5.6 billion over the next 10 years.'' Press Association, ''£5.6bn ID cards estimate criticised'', published in *The Guardian* 8 November 2007. http://www.guardian.co.uk/uklatest/story/0,,7061225,00.html. There have been many stories like these.

[25] Rasch, Mark, ''No email privacy rights under Constitution, US gov claims'', *SecurityFocus*, published in *The Register*, 4 November 2007. http://www.theregister.co.uk/2007/11/04/4th-amendment_email_privacy/.

[26] Ford, Richard, ''Police told to erase 'irrelevant' crime records'', *The Times*, 1 November 2007. http://business.timesonline.co.uk/tol/business/law/public_law/article2781344.ece.

[27] Article 17.1 of 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 and on the free movement of such data. Official Journal of the European Communities of 23 November 1995 No L. 281, p. 31. This paragraph reads as follows: ''Member States shall provide that the 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.''

- Malware (spyware, spamming, etc.) will continue to pose threats to privacy and undermine trust in the AmI world just as it does today.
- If one assumes an Internet of things, when all products are embedded with intelligence, how valid will the fair information and data protection principles be? In meshed networks of smart dust, even the notion of centralised databases and data controllers may change.

3.4. *Economic challenges*

Last, but not least, economic issues will provide a set of formidable challenges, as solutions will only be as good as their economic feasibility. Economic challenges include the following:

- Analysing and articulating the economics of privacy and trust.
- The need to convince industry that investments in privacy-enhancing mechanisms are justified and are in industry's own interests.
- Dealing with information and power asymmetries.
- Who should deploy privacy-enhancing technologies, both network based and user based? Will they be affordable? Will they be adequate to the task(s)?

Many of the above challenges to privacy and trust posed by the ubiquitous Information Society apply to a variety of domains, of which we can identify three different types: namely, domains of place, application (or functional) domains and organisational domains. Domains of place include the home, one's workplace, and one's vehicle. Application or functional domains include the financial services domain, travelling (or mobility), shopping and the crime prevention domains. Organisational domains include industry, government, the media and academia (or education) domains. In developing new privacy and data protection policies, policy-makers need to consider the differences in these domains. For example, an RFID policy that requires shop owners to ''kill'' an RFID tag attached to clothes once they are sold to consumers will need to factor in differences in the mobility domain where those citizens carry embedded travel cards (such as London Transport's Oyster card) and biometric passports.

While a particular response to one or more of the challenges identified above could be appropriate in one domain, it may not be appropriate in another. Even within the same domain, there may be differing contexts where the application of one response may not be appropriate in another context.

4. Responding to the challenges

In this section, we provide some examples of measures or possible responses to the challenges mentioned above. It is important to note that no single measure will adequately respond to the challenges to privacy and trust posed by the ubiquitous Information Society. Rather, some combination of measures will be needed and the combinations can be expected to vary according to the situation or the domain.

4.1. *Technical measures*

Minimising personal data should be factored into all stages of collection, transmission and storage.[28] The goal of data minimisation is to avoid as much as possible that data collected for one purpose are not used for other purposes; only data strictly relevant to the realisation of the legitimate objective may be processed. With regard to external dangers, the aim of the minimal data transmission principle is that data should reveal little about the user even in the event of successful eavesdropping and decryption of transmitted data. Similarly, the principle of minimal data storage requires that thieves don't benefit from stolen databases and decryption of their data. Implementation of anonymity, pseudonymity and unobservability methods helps to minimise system knowledge about users at the stages of data transmission and storage in remote databases, but not in cases involving data collection by and storage in personal devices (which collect and store mainly the device owner's data) or storage of videos.

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

Industry may resist many technological measures because they increase development costs, but safer, more secure technology should be seen as a good investment in future market growth and protection against possible liabilities. Consumers will be more inclined to use technology if they believe it is secure and will shield, not erode their privacy. Security guru Bruce Schneier got it right when he said that ''The only way to fix this problem [of bad design, poorly implemented features, inadequate testing and security vulnerabilities from software bugs] is for vendors to fix their software, and they won't do it until it's in their financial best interests to do so . Liability law is a way to make it in those organizations' best interests.''[29] Of course, when considering the policy options one needs to reflect on the disadvantages of stricter liability rules as well. Clearly, if development costs go up, industry will pass on those costs to consumers, but since consumers already pay, in one way or another, the only difference is who they pay.[30]

4.2. *Socio-economic responses*

Standards form an important privacy-protection measure in many domains.

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

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

[30] If lower cost, less secure technology results in more instances in identity theft, for example, consumers pay for the technology and ''pay'' for the losses they suffer from the misappropriation of their data. If consumers pay more upfront for more secure technology, they may incur fewer follow-on costs if the incidence of identity theft falls. However, the overall cost to consumers in either scenario may remain more or less the same.

While there have been many definitions and analyses of the dimensions of privacy, few of them have become officially accepted at the international level, especially by the International Organization for Standardization. The ISO has at least achieved consensus on four components of privacy, as follows:

- *Anonymity* ensures that a subject may use a resource or service without disclosing user identity.
- *Pseudonymity* ensures that a user may use a resource or service without disclosing identity, but can still be accountable for that use.
- *Unlinkability* ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- *Unobservability* ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.[31]

Among the ISO standards relevant to privacy are ISO/IEC 15408 on evaluation criteria for IT security and ISO 17799, the Code of practice for information security management. The ISO published its standard 17799 in 2000, and updated it in July 2005. Since then, an increasing number of organisations worldwide formulate their security management systems according to this standard. It provides a set of recommendations for information security management, focusing on the protection of information as an asset.[32] ISO 17799 was constructed against the backdrop of today's technologies, however, rather than AmI or ubiquitous networking. Hence, the adequacy of this standard in an AmI world needs to be considered. Nevertheless, organisations should state to what extent they are compliant with ISO 17799 and/or how they have implemented the standard.

The ISO also established a Privacy Technology Study Group (PTSG) under Joint Technical Committee 1 (JTC1) to examine the need for developing a privacy technology standard. This was an important initiative.

Promoting open systems and open standards at a European level could help to build a more trustworthy system, to mediate between public and private control over networked systems and, therefore, to contribute to security and privacy in AmI.[33]

Audit logs do not, as such, protect privacy since they are aimed at determining whether a security breach has occurred and, if so, what went wrong and who might have been responsible. Nevertheless, audit logs could play a role in protecting privacy: as a tool that warns about problems and certainly as a deterrent for those who break into systems without authorisation. In the highly networked environment of our AmI future, maintaining audit logs will be a much bigger task than now where discrete systems can be audited. Nevertheless, those designing AmI networks should ensure that the networks have features that enable effective audits.

Codes of practice and guidelines can be included in combinations of measures. Among the best and best-known are the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[34] which were (are) intended to harmonise national privacy legislation, its more recent *Guidelines for the Security of Information Systems and Networks*, its December 2005 a report on ''The Promotion of a Culture of Security for Information Systems and Networks'', its November 2003, 392-page volume entitled *Privacy Online: OECD Guidance on Policy and Practice*, which contains specific policy and practical guidance to assist governments, businesses and individuals in promoting privacy protection online at national and international levels. In addition to these, the OECD has produced reports on other privacy-related issues including RFIDs, biometrics, spam and authentication.[35]

Trust marks and trust seals are a form of guarantee provided by independent organisations that maintain a list of trustworthy companies that have been audited and certified for compliance with some industry-wide accepted or standardised best practice in collecting personal or sensitive data. Once these best practice conditions are met, companies are allowed to display a trust mark or seal that customers can easily recognise and that are intended to inspire consumer trust and confidence.[36]

Trust seals and trust marks are often promoted by industry, but empirical evidence gathered for a study published in 2005 indicated that even years after the introduction of the first trust marks and trust seals in Internet commerce, citizens knew little about them and none of the existing seals had reached a high degree of familiarity among customers.[37] Though this does not necessarily mean that trust marks are not an adequate measure for improving security and privacy in an ambient intelligence world, it suggests that voluntary activities like self-regulation have to be complemented by other measures.[38]

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

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

[33] Kravitz, D.W., K.-E. Yeoh and N. So, ''Secure Open Systems for Protecting Privacy and Digital Services'', in T. Sander (ed.), *Security and Privacy in Digital Rights Management*, ACM CCS-8 Workshop DRM 2001, Philadelphia, 5 November 2001, Revised Papers, Springer, Berlin, 2002, pp. 106–125; Gehring, R.A., ''Software Development, Intellectual Property, and IT Security'', *The Journal of Information, Law and Technology*, 1/2003. http://elj.warwick.ac.uk/jilt/03-1/gehring.html.

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

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

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

[37] Moores, T., ''Do Consumers Understand the Role of Privacy Seals in E-Commerce?'', *Communications of the ACM*, Vol. 48, No. 3, 2005, pp. 86–91.

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

In an attempt to reduce some of the uncertainties associated with online commerce, some websites acting as intermediaries between transaction partners operate so-called *reputation systems*. These institutionalised feedback mechanisms are usually based on the disclosure of past transactions rated by the respective partners involved.[39] Giving participants the opportunity to rank their counterparts creates an incentive for rule-abiding behaviour. Reputation systems are, however, vulnerable to manipulation[40] and may be subject to malicious attacks, just like any net-based system.

An alternative to peer-rating systems is *credibility-rating systems* based on the assessment of trusted and independent institutions, such as library associations, consumer groups or other professional associations with widely acknowledged expertise within their respective domains.

Another useful measure could be *service contracts* between the service provider and the user with provisions covering privacy rights and the protection of personal data and notification to the user of any processing or transfer of data to third parties. While this is a possible response, there are serious doubts about the negotiating position of the user. Also, from the service provider's point of view, it is unlikely that he would want to conclude separate contracts with every user. In a world of ambient intelligence, such a prospect becomes even more unlikely in view of the fact that the ''user'', the consumer-citizen, will be moving through different spaces where there is likely to be a multiplicity of different service providers. The consumer-citizen could have a digital assistant that would inform him of the privacy implications of using a particular service in a particular environment. If the consumer-citizen did not like the terms, he wouldn't have to use the service. Consumer associations and other civil society organisations (CSOs) could play a useful role as a mediator between service providers and individual consumers and, more particularly, in forcing the development of service contracts (whether real or implicit) between the service provider and the individual consumer. CSOs could usefully position themselves closer to the industry vanguard represented in platforms such as ARTEMIS[41] by becoming members of such platforms themselves. Within these platforms, CSOs could encourage industry to develop ''best practices'' in terms of provision of services to consumers.

Research and development (at least publicly supported R&D) must highlight future opportunities and possible risks to society and introduce them into public discourse. Every *research project* should commit itself to explore possible risks in terms of privacy, security and trust, develop a strategy to cover problematic issues and involve users in this process as early as possible.

Public procurement programs can be used to support the demand for and use of improved products and services in terms of privacy and/or identity protection.

Consumers need to be educated about the privacy ramifications arising from virtually any transaction in which they are engaged. Education campaigns should target different segments of the population. School-age children should be included in any such campaign. Any networked device, particularly those used by consumer-citizens, should come with a *privacy warning* much like the warnings on tobacco products.

There are various ways of *raising awareness*, and one of those ways would be to have some contest or competition for the best privacy-enhancing product or service of the year. The US government's Department of Homeland Security is sponsoring such competitions,[42] and Europe could usefully draw on their experience to hold similar competitions in Europe.

One of the best measures is *public opinion*, stoked by stories in the media and the consequent bad publicity given to perceived invasions of privacy by industry and government as well as hackers, identity thieves and other evil-doers. The bad press and negative public opinion that followed some high profile data losses, notably that of 25 million child benefit records in October 2007, has forced the UK government to take remedial measures, which may include strengthening the powers of the Information Commissioner's Office (ICO).[43]

4.3. *Legal and regulatory responses*

As the impact of new ICT technologies goes beyond national borders, several legal acts on data protection, e-privacy, e-commerce, etc., have been adopted at the EU level.[44]

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

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

[41] With a wide variety of stakeholders from industry, academia and government, ARTEMIS is focused on the development and deployment of embedded systems. The European Commission supported the platform which has now become a so-called Joint Technology Initiative (JTI). See http://www.artemis-sra.eu/.

[42] Lemos, Robert, ''Cybersecurity contests go national'', *The Register*, 5 June 2006. http://www.theregister.co.uk/2006/06/05/security_contests. This article originally appeared in *SecurityFocus*. http://www.securityfocus.com/news/11394.

[43] The ICO is due to begin using new powers to 'spot check' both public and private sector organisations in the event that a data breach is suspected later this year. Richards, Jonathan, ''Top officials to be held to account for data losses'', *The Times*, 22 April 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/article3797278.ece.

[44] The most crucial binding legal instruments adopted by European Union are 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 and on the free movement of such data [the Data Protection Directive], OJ L 281, 23/11/1995, pp. 0031–0050; 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, also known as the e-Privacy Directive), OJ L 201, 31/07/2002, pp. 37–47; Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 [the Data Retention Directive], OJ L 105, 13/4/2006, pp. 54–63.

However the legal framework as it exists now is continuously challenged by the fast pace of technological developments. The realisation of AmI will further emphasise even more the tension between existing regulation on privacy and data protection and the requirements of the new environment. AmI *needs* extensive data collection and profiling in order to make the user's environment to act in an intelligent way. Regulation that simply *prohibits* such extensive data collection and profiling practices is likely to interfere with the user-friendliness of an AmI world. Yet how are we then to ensure that we can benefit from new technology developments while still maintaining our privacy and security? How should we reconcile the different aims, needs and expectations when devising a well-balanced regulatory framework?

Several problems confront the current regulatory framework and require the policy-makers' reflection. The first lies in the definition of personal data as the criterion triggering the application of legal safeguards. The second relates to the paradigm of legal intervention (opacity of the individual or transparency of the processor). Then there is the problem of the relation between law and technology in regulating and enforcing privacy and data protection. A fourth legal issue concerns the balance between the general legal framework and the need for specific regulation addressing specific technologies. These issues are briefly tackled in the following subsections, which identify some of the problems and the legal tools that could be used to address them.

The first legal issue involves the *definition of personal data*. The Data Protection Directive defines personal data as ''any information relating to an identified or identifiable natural person (the 'data subject')''. In determining whether information concerns an identifiable person, one must apply recital 26 of the Data Protection Directive, which says that ''account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person''. Such a definition implies a broad understanding of the notion of personal data, which may consist of all sorts of information as soon as they relate to the individual.[45] Indeed, such a definition implies the necessity of a case-by-case assessment, an approach upheld in a recent opinion from the Article 29 Data Protection Working Party on the definition of personal data.[46]

When we apply such approach in an AmI environment, two problems come to light. First, with intelligence embedded everywhere, an Internet of things offers a huge increase in possibilities for collecting and aggregating data, and with the continuing advances in computing power, we will see similarly huge increases in data mining and analysis. Such being the case, heretofore ''anonymous'' data will be linked so that we face a prospect of virtually all data becoming personal data.[47] Such being the case, it is easy to foresee continuing disagreements over what information constitutes personal data, and thus whether the processing of such data should trigger the application of the data protection legislation. Indeed, such disagreements already occur now, as we can see in the case of RFID[48] and IP addresses.[49] Second, often the identity of the data subject is not needed in order to conduct commercially profitable operations using data which in theory does not relate to an identifiable individual, e.g., profiling or monitoring. Such operations use unique identifiers, e.g., an RFID chip's serial number, so that no direct link with the real identity of the person is made. Nevertheless, such operations could still constitute a threat to the interests of the individual since they enable profiling practices which, in turn, might become the basis for intrusive marketing or other manipulative actions. Other data creating problems are those produced and processed by trusted systems, e.g., the data generated by log files, watermarks and similar protection systems.

With the emergence of AmI, the definition of personal data needs to be reconsidered. How can policy-makers create a legal framework protecting private information in a way which shows resilience towards technological developments the capabilities of which are hard to anticipate? Can a distinction between personal and other data be sustained in an AmI world, since such a world can impact upon a person's behaviour without a need to identify that person?[50] Perhaps the time has come to explore the possibility of a shift from personal data protection to data protection *tout court*[51]: such a new generation of data protection rules would no longer take ''identifiability'' as a criterion, but it would rather be triggered when data and knowledge developed by AmI affect our behaviour and decisions, regardless of their capacity to identify individuals.[52]

A *second fundamental legal issue* concerns a proper balance between technology, privacy and security. The classical

[45] Article 2 of the Data Protection Directive defines an identifiable person as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his psychic, psychological, mental, economic, cultural or social identity.

[46] Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, 01248/07/EN, WP 136. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[47] Gonzàlez Fuster, Gloria, and Serge Gutwirth, ''Privacy 2.0?'', *Revue du droit des Technologies de l'Information*, Doctrine, 2008, pp. 349–359.

[48] Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 10107/05/EN, WP 105, 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

[49] White, Aoife, ''IP Addresses Are Personal Data, E.U. Regulator Says'', Associated Press, published in *The Washington Post*, 22 January 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html; Hansell, Saul, ''Google Says IP Addresses Aren't Personal'', *The New York Times*, 22 February 2008. http://bits.blogs.nytimes.com/2008/02/22/google-says-ip-addresses-arent-personal/index.html?ref=technology.

[50] One could envisage in the AmI world a supermarket trolley dispensing selected commercials to a user, dependent on the way and pace the victim (sorry, the consumer) shops his way through the shelves.

[51] Gutwirth, Serge, and Paul De Hert, ''Regulating profiling in a democratic constitutional state'', in M. Hildebrandt and S. Gutwirth, *Profiling the European citizen: Cross disciplinary perspectives*, Springer Science, Dordrecht, 2008, p. 289.

[52] Ibid., pp. 367–268; Gonzàlez Fuster, G., and S. Gutwirth, *l.c.*, p. 360. See also: Poullet, Yves, ''Pour une troisième génération de législation de protection des données'', *Jusletter*, Issue 3, 2005, 22 pp.

approach in privacy mainly focused on the use of *opacity tools* – tools proscribing the interference by powerful actors with the individual's autonomy. However, as has already been the case in data protection, the default position in the future will likely be the use of *transparency tools* – tools that accept interfering practices, though under certain stringent conditions which guarantee the control, transparency and accountability of the interfering activity and actors.[53] Where the goal is to control and channel the exercise of power rather than to restrict and limit it (which is the case in many, if not most, of the challenges arising in the new AmI environment), it would seem more fruitful to address the situation with regulatory transparency tools instead of prohibitive opacity tools.

In order to make transparency tools more than a nice theoretical construct, some practical issues have to be addressed.

How can policy-makers ensure that data processing rules are respected, especially those relating to the quality of the data and correctness of the information, and that the data subject's (limits to his) consent to processing is similarly respected? In an AmI world, this is obviously an issue of high complexity, since the concerned individuals very often remain unaware of a violation of their rights and even if they are aware of them, they may lack the technical means and legal support to oppose the difficult-to-identify wrongdoers. Thus, it would be useful to develop ways that would allow both the data subject to express his or her choices about what information he or she is willing to make available to whom and for what explicit purpose, and to develop mechanisms for monitoring the data processor's adherence to such choices. Some researchers have already proposed a solution by means of ''sticky policies'' that would ''follow'' the subject's data and that would provide clear information to data processors and controllers about which privacy policy applies to the data concerned.[54] Sticky policies would also facilitate the auditing and self-auditing of the lawfulness of data processing by data controllers.[55] As a retrospective measure, auditing enables the detection and reporting of abuses, which in turn provides the data subject the wherewithal to launch liability and damages claims. In addition, audits serve the data protection authorities for whom there is an urgent need to strengthen and internationally harmonise their powers, especially in light of the transnational or ''beyond borders'' character of the AmI world.

Proper control over the implementation of privacy policies and fairness of data processing in general needs to be strengthened. The *effective enforcement* of legal regimes on data protection, including effective *liability for breach of the privacy rules*, is crucial. Currently, Europe lacks a coherent legal framework for privacy liability. If our privacy is, in fact, infringed, the scope of the infringer's liability remains unclear. Guidelines and interpretations on liability would be welcome, as would measures to provide greater clarity and legal certainty for both users and data processors.

Consumer protection law could also be a useful tool in enforcing an adequate level of privacy protection. Consumer protection law defines the obligations of producers and the rights of consumers and consists of a set of rules limiting the freedom to contract in order to protect consumers against nasty producers. Generally speaking, consumer law has a few tools to foster its objectives. First of all, it imposes mandatory rules on the parties which cannot be contravened to the detriment of the consumer. To a great extent, this applies to certain contractual terms and practices. Furthermore, it provides for an obligation of information disclosure. Also, there are rules addressing issues of legal redress, which often involve engaging consumer organisations in dispute resolution procedures. Certain minimum standards of consumer protection have been harmonised at the level of European Union by specific regulations,[56] as well as by provisions in various legal texts dealing with other issues (e.g., data protection). Privacy threats arising from AmI technologies are not subject to all such legal provisions,[57] but the means mentioned above might well be an inspiration for comparable legal initiatives.

Especially relevant to issues of enforcement are *unfair commercial practices* and *unfair contractual terms*. The Unfair Commercial Practices Directive[58] contains a general ban on unfair commercial practices relating especially to the provision of information, representation, and commercial communication and so on. The unfairness of practices is assessed against the benchmark of the ''average consumer''. Member States are obliged to put in place effective sanctions against infringement of the Directive. In an AmI world, some data processing practices might be considered unfair because they are carried out without the knowledge of the concerned individuals. The

[53] See De Hert, Paul, and Serge Gutwirth, ''Privacy, data protection and law enforcement: Opacity of the individual and transparency of power'', in Erik Claes, Anthony Duff and Serge Gutwirth (eds.), *Privacy and the criminal law*, Intersentia, Antwerp/Oxford, 2006, pp. 61–104; De Hert, P., and S. Gutwirth, ''Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location based services and the virtual residence'', in I. Maghiros (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), Institute for Prospective Technological Studies (IPTS), Seville, July 2003, pp. 111–162. ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.

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

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

[56] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *Official Journal* L 095, 21/04/1993, pp. 29–34; 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, OJ L 144, 04/06/1997, pp. 19–27; Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, pp. 22–39.

[57] See, in particular, recitals 10 and 14, and Article 3 which restrict the scope of application of the Unfair Commercial Practices Directive.

[58] Directive 2005/29/EC.

Directive on Unfair Terms in Consumer Contracts[59] focuses on consumer contracts which are not individually negotiated, and particularly on pre-formulated standard contracts, which is essentially the case with most ICT products. The sanction against unfair terms is such that the consumer is not bound by them. From this perspective, contractual provisions that clearly encroach on consumer privacy and data protection rights could be regarded as unfair contractual practices. While the non-application of the contractual provision is not always the most useful remedy, other, more appropriate actions are penalties imposed on traders, damages and orders of cessation of the harmful practice, which are the remedies provided under other acts, notably the Unfair Commercial Practices Directive,[60] the Data Protection and e-Privacy Directives.[61]

Another issue is the transparency of processing. The current legal framework requires data collectors and data processors to inform the data subject that data are collected and to give him or her basic information about the data processing. It is questionable whether such *information requirements* truly enable the data subject to have a comprehensive view of the data processing and its implications. In any event, such an information requirement might be unworkable in the AmI future: both the data subject and the data processor could become overwhelmed by the amount of information they would need to exchange – which would prevent the data subject from obtaining any truly useful knowledge about what's really going on. Thus, how can one ensure that data processing is really transparent to the data subject?

First of all, it seems pretty evident that the data subject should be given access to information on data collection and processing practices that concern him. However, the data subject needs to be supported in the process of data management so that he or she could truly benefit from the information disclosed. The question thus is how to ensure a proper balance between the information which should be provided to the data subject and how to remedy the *information asymmetry* which we see already today (we are becoming transparent towards the data processors, but they remain opaque towards us)? This prompts a more practical question: how should information on data collection and processing be managed? One could contemplate a simplified way of providing (certain) information, such as simplified notices or pictograms that would inform the consumer-citizen that he is in the presence of RFID readers. The Article 29 Working Party has already provided useful guidelines and proposed multi-layer EU *information notices*.[62] Industry and law enforcement agencies should consider a similar approach for ambient intelligence. Moreover, one could think about providing machine-readable information which could be managed by *intelligent agents*, able to deal with the large amounts of data to be processed in an AmI world.

Another issue with regard to the transparency of data processing concerns the extent to which the data subject should have access to knowledge which has been derived from his personal data, i.e., his right and ability to access *profiles*. Such *access to profiles* (*profiling knowledge*) could be crucial for the data subject as it could enable him to understand why his environment undertakes certain actions; it could alert him to any improper information that could influence his profile or any improper operation which took place, and make him aware of the decisions that were made based on his profile. Such information could also help the individual in proving liability in case of damage. Thus, apart from technical and organisational problems, one should also address the purely legal question of how to reconcile the right to have access to profiling knowledge (which might be construed as a trade secret in some circumstances) with the intellectual property rights of the data controller.

A third major problem exists in the application of the *consent principle* in data protection law. In general, unambiguous consent is the precondition of legitimate data processing. In many situations, however, it remains unclear what unambiguous consent means, and how it should be expressed, especially when it needs to be given in respect of services based on personal profiling: how can one give informed consent when the scope of the data collection cannot be precisely foreseen by the parties.[63] Probably this points to the

[59] Directive 93/13/EEC.

[60] Article 11, para 2.

[61] Article 22 of the Data Protection Directive and Article 15 para 2 of e-Privacy Directive.

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

[63] The deployment of *service platforms* will make it even harder to anticipate the scope of use of data. *Service platforms* are the subject of research in EC-supported projects (such as the Wireless World Initiative project). Some of these projects have also undertaken research into privacy issues (e.g., Mobilife, SPICE) and they too have determined that there is a problem in requiring consent from the user each time his data are gathered. A simpler solution is to obtain the user's consent when the user subscribes to the platform's services. The service would still need to provide a clear indication of the implications of subscribing in terms of the user's privacy, and an explanation of the technical framework. See Moscibroda, Anna, Christoph Schnabel et al., *Legal and Regulation Issues*, SPICE Deliverable D1.6, May 2008. http://www.ist-spice.org/nav/deliverables.htm. It should be noted, however, that research aimed at reconciling views of both users and service providers, the technology and the legal framework is not yet mature enough to offer better solutions. The authors of the SPICE deliverable note that "The European legislator must face . changes in the development and use of profiling techniques and provide for an adequate regulation of profiling techniques. It should allow for using such techniques to provide personalised services and to support data subjects in organising their daily lives. The regulation must on the other hand guarantee that data subjects will at any point be in control of their profiles. It must be avoided that decisions on behalf of the data subject are made, that the data subject can neither control nor change. Also, the data subject must be aware that profiles about him/her exist, what they contain and what they are used for. The current situation in which profile processing is evaluated on basis of regulation not made to match the specific risks and advantages of profiling is unsatisfying" (p. 238). In any case, a thoughtful analysis of the results of such research, in conjunction with the extensive literature that deals with consent issues in general, seems more than desirable.

need to develop at EU level more concrete modalities and standards for a valid consent.

Finally, while *transparency* might be the default position in an AmI world, some *opacity measures* and prohibitions may be required to protect the individual from any form of dataveillance[64] in certain spaces or situations (e.g., no surveillance in bathrooms). The *digital territory* concept allows the individual to access – and stay in – a private digital territory of his own at (any) chosen time and place.[65] This private digital space could be considered as an extension of the private home. Currently, the law guarantees neither the establishment nor the protection of an online private space in the same way as the private space in the physical world is protected.[66] A set of rules could be envisaged to guarantee protection of our digital territories.

A third pivotal issue is the relation between legal and technological solutions in the area of privacy and data protection. Some checks and balances in using data should be put in place in the *overall architecture of the AmI environment*. A shift to *privacy-by-design* and privacy-enhancing technologies (PETs) seems necessary. Intelligent software agents could help the data subject to manage his or her data. Sticky policies, log files and watermarking techniques, already mentioned above, are among the technological responses that might help to implement legal safeguards.[67] It would help too if technology and/or system designers reflected on potential privacy and data protection requirements at the design and development stages, which might result in architectural choices that are more privacy-friendly (e.g., design choices could be as simple as giving users the option of enabling or disabling RSS feeds to their profiles). Regulatory authorities and/or industry leaders and/or other prominent stakeholders could usefully encourage or formalise such reflection on the legal privacy requirements during the design phase, especially if they were to treat such requirements as important as business or system requirements. Such development practices are already followed by some research consortia, and they seem to produce good results.[68]

A fourth legal issue that needs special consideration is the extent to which specific technologies need *specific legislation*. For example, specific legislation might be needed to govern the use of specific technologies such as implants and RFID technologies.[69] A more extensive reliance on ''soft law'' instruments or additional legislative measures might be envisioned. ''Soft law'' might be even more specific than statutes and more flexible, and hence better fitted to regulate fast-changing environments. Especially interesting are the codes of conduct developed by industry which promote practical actions in compliance with laws or which are created to pre-empt possible regulatory intervention. Such codes of conduct might be particularly interesting to the supervising data protection authorities as to whether they truly take all legal requirements into consideration. Presumably such codes of practice stimulate an exchange of views with regard to concrete practices (even before the actual harm occurs).

5. Improving the policy-making process

The development of a set of EU-level measures responding to the challenges to privacy and trust in the ubiquitous Information Society will need to be based on an assessment of all available instruments: social dialogue, fostering technical development, international cooperation and ensuring a regulatory framework enabling citizens, businesses and public entities to achieve the maximum of the potential benefits. *No single measure will adequately respond to the challenges to privacy and trust* posed by the ubiquitous Information Society. Rather, *some combination of measures will be needed* and the combinations can be expected to vary according to the situation or the domain. There is no easy answer to the question about which instruments will be best. The most suitable instrument (or

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

[65] Daskala, B., and I. Maghiros, *Digital Territories: Towards the protection of public and private spaces in a digital and Ambient Intelligence environment*, Institute for Prospective Technological Studies (IPTS), Seville, 2007. http://www.jrc.es/publications/pub.cfm?id=1474.

[66] Idem. See also Beslay, L., and Y. Punie, ''The Virtual Residence: Identity, Privacy and Security'', in I. Maghiros (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), Institute for Prospective Technological Studies (IPTS), Seville, July 2003, p. 67. http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html.

[67] However, information management tools in general also raise legal questions about how to treat the data generated by such systems. Profiles and automated decisions also impact privacy and trust. A comprehensive legal approach to the issue of profiling has not yet been proposed.

[68] We especially refer here to projects supported under the EC's Sixth Framework Programme: See, for example, Gaudino, Francesca, and Alkiviadis Psarras (eds.), *Assessment of the legal and regulatory framework*, DISCREET Deliverable 2101, May 2006; Koutsoloukas, Lefteris, and Sofia Kapellaki (eds.), *System Requirements*, DISCREET Deliverable 2102, June 2006, and He, Dan (ed.), *Regulatory and Performance Assessment*, DISCREET Deliverable 2402, March 2008, http://www.ist-discreet.org/; and Moscibroda, Anna, and Christoph Schnabel (eds.), *Legal and Regulation Issues,* SPICE Deliverable 1.6, May 2008, and Shiaa, M.M., and H. Demeter (eds.), *Final Reference Architecture*, SPICE Deliverable 1.8, May 2008. http://www.ist-spice.org/nav/deliverables.htm.

[69] See, respectively, European Group on Ethics in Science and New Technologies, ''Ethical Aspects of ICT Implants in the Human Body'', Opinion to the Commission, 16 March 2005. http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf and Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 10107/05/EN, WP 105, 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

combination of instruments) will depend on the particulars of the context.

In considering policy options, policy-makers must identify the nature of the personal information in question and relevant contextual factors. Considerations of personal information might include the following:

- *Data capture*, including the types of personal data, the circumstance and means of its capture;
- *Data storage*, including the duration the data will be retained, who can access it and the protections to be employed;
- *Data analysis and integration*, including the links that might be made to other data; and
- *Data dissemination*, i.e., who will have access to the data and what harms might result from inappropriate disclosure.

Contextual factors include the following considerations:

- The social and institutional context – for example, are the data provided voluntarily or are they required by law or are they acquired covertly or deceptively? Are rewards or benefits offered for sharing personal information? Is coercion used in the form of withholding benefits when personal data are not provided? Does the individual retain control over the initial and potential future uses of his or her data? Does he or she have the opportunity to review and correct data?
- Who are the stakeholders (including evil-doers) who are involved or might be involved in the collection, storage, processing or transfer of the data and what are the relationships between them?
- Who wants the data and why? Could the data be re-used for some other purpose?
- How are decisions made when there are competing interests regarding personal data, for example, public health needs versus individual privacy or national security versus individual fundamental rights?[70]
- Is the gathering of the data apparent and obvious to those whose data are collected? Could the collected data be used for or against others (e.g., relatives, friends or other members of a group)?[71]

All assessments and policy options need to be examined in terms of trust and trustworthiness, and indicators should focus on these dimensions as much as on whether a given technology, situation or set of circumstances in any context in any domain is privacy enhancing or privacy eroding.

There are many factors that affect trust, some of which are highly volatile. Generally, stakeholder beliefs, attitudes, behaviour and perceptions are slow to change, but discontinuities (a terrorist attack, an outbreak of avian flu among humans) can shift public (stakeholder) opinion rather quickly.

As trust is the glue that binds society together, policy options should be judged in part (but not the only part) in terms of whether they damage trust or offer gains. If a good option is judged negatively because it damages trust, then policy-makers need to scrutinise it more closely to see what can be done to improve trust or whether the option is truly optimal in the circumstances.

For each challenge and response, we need to identify who the key stakeholders are (who can take what response to each challenge) and to evaluate the responses according to various criteria, including effectiveness, credibility, trust, trustworthiness, time frame, impacts, rebound effects, etc.

5.1. *Policy-making tools*

In the rapidly approaching world of ambient intelligence, where policy-makers need to consider not only the adequacy of existing policies but also whether there is a need to develop new policies when new issues are spotted coming over the horizon, several methodologies or policy-making tools will be useful.

One is an analysis of privacy and trust issues (challenges) raised by ambient intelligence as reported in the *media, peer-reviewed journals (or books) and in project reports* and studies, how the privacy and trust issues are characterised, especially in the context of new technologies, and the risks that are implied or articulated.

A second is close *scrutiny of the privacy and trust policies* adopted in other countries and whether there are lessons to be learned for Europe (even though Europe is widely – but not uniformly – regarded as having more advanced policies than most other countries). For example, the US Federal Trade Commission has recently indicated that it intends to tighten rules governing ''behavioural targeting, the increasingly popular tactic of delivering ads to people based on what websites they have visited. In practice, the targeting issue goes beyond just Web surfing: Google's Gmail funnels ads to people based on key words in the e-mail messages they write, and MySpace helps marketers select ads for people based on the information about themselves they willingly post in online profiles.''[72]

A third is the use of *scenarios*, which should form an integral tool in privacy impact assessments and testing indicators. Scenarios should illustrate competing interests as well as the

[70] Notably those provided for by Articles 7 and 8 of the European Charter of Fundamental Rights (2000/C 364/01). 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'' and that ''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 which has been collected concerning him or her, and the right to have it rectified.''

[71] Adapted from Waldo, et al., pp. 306–307.

[72] Story, Louise, ''F.T.C. Member Vows Tighter Controls of Online Ads'', *The New York Times*, 2 November 2007. http://www.nytimes.com/2007/11/02/technology/02adco.html?ref=technology. But just a few days later, two large social networking sites, MySpace and FaceBook, showed off new ways to use information about their members to deliver targeted adverts. Story, Louise, ''Tracking of Web Use by Marketers Gains Favor'', *The New York Times*, 5 November 2007. http://www.nytimes.com/2007/11/05/technology/05myspace.html?ref=technology. See also Federal Trade Commission, ''FTC Staff Proposes Online Behavioral Advertising Privacy Principles'', FTC Press release, Washington, DC, 20 December 2007. http://www.ftc.gov/opa/2007/12/principles.shtm.

expected impacts from combinations of responses. Resource implications of any proposed new privacy policy are as important as the socio-economic impacts (Will a measure stultify or stimulate innovation? Will it help or hinder European industry?). Brief mini-scenarios may serve this purpose just as well as fully elaborated scenarios.[73] Mini-scenarios can be anchored in terms of existing policies and programmes, but can be constructed to be more hypothetical, more future oriented and based on what-if propositions. Waldo et al. advocate the use of ''anchoring vignettes'', which are very short (half a page or so) scenarios that serve to highlight specific privacy issues in specific contexts and circumstances and to help frame questions that might be asked about any given policy.[74]

It is possible to examine some number of scenarios and real contexts from different domains and to identify and assess common indicators or questions that one can pose in any set of circumstances that will help to illuminate the contours of the debate, of the issues that might be at stake in any situation. Identifying such indicators might not provide any ready-made signposts to a solution, but they could well help the decision-making process, especially by ensuring that stakeholders are aware of all the facts, so that they understand the difficulties in making a given trade-off – *and*, at the same time, ensuring that policy-makers are well aware of the views of stakeholders. In the end, a political decision is just that, a judgement call. In some instances, collective security will outweigh the individual's fundamental right to privacy and, in other instances, the individual's fundamental right to privacy will or should prevail (however well intentioned we might be, the more we undermine the individual's fundamental rights, the more democracy is undermined).

By examining some number of scenarios and real contexts from different domains, one could envisage a template (a dynamic template) or genus of typical options and indicators that can help inform debate in any situation, in any context. If policy-makers (and other stakeholders too, for that matter) are made aware of these various options and indicators before policy decisions are made, if they are brought into the debate, then it might help lower the risk of demonization.

A fourth is the use of context-sensitive *privacy impact assessments* to examine policy options, for each of which policy-makers will want to know: What does it cost? Does it solve certain problems totally? Are there remaining gaps (lacunae)? Are there rebound effects? Picking a policy option, even after a privacy impact assessment, may be difficult, because of the trade-offs between individual privacy and other societal values (especially national security). As Waldo et al. put it, ''Not only are these tradeoffs complex, difficult, and sometimes seemingly intractable, but they are also often not made explicit in the discussions that take place around the policies that, when they are enacted, quietly embody the value tradeoffs. Clarifications on these points would not necessarily relieve the underlying tensions, but they would likely help illuminate the contours of the debate.''[75] In other words, transparency in the assessment and decision-making process is vital even if it is not any easier to balance the competing interests or to arrive at a solution to the trade-off.

A fifth is *public opinion surveys and other stakeholder consultation techniques*. Protecting our privacy and enhancing trust will only be possible if all stakeholders are engaged. All stakeholders, including the public, including individuals, will need to do their bit. The European Commission's public consultation on RFIDs was a very good example in participatory policy-making.

6. Conclusions

With the emergence of ambient intelligence technologies, policy-making increasingly will need to be more contextual without jettisoning coherence.

If they do not already appreciate the fact, policy-makers will need to recognise that privacy and trust are context dependent, that they do not mean the same thing to all people in all situations, nor do all people attach the same value to these concepts, however they define them. Moreover, people's sense of privacy and trust – again however one chooses to define them – will continue to change over time.

Not only are broad brush policies not likely to work in an ambient intelligence environment, even domain-specific policies will be difficult to write, because even within the same domain, differing circumstances may call for differing privacy protections. As it seems increasingly necessary to consider many contextual and other factors to deal adequately with the many new privacy and trust issues arising from the introduction of ambient intelligence, one can envisage that policy-makers, in consultation with stakeholders, will need to develop a series of privacy ''micro-policies'' dealing with the particular set of circumstances involving new technologies. The Commission seems to recognise this. In a Communication in March 2007, it said it considered the Data Protection Directive to be technologically neutral and that its principles and provisions are sufficiently general, that its rules may continue to apply appropriately to new technologies and situations. ''It may be necessary, though, to translate those general rules into particular guidelines or provisions to take account of the

[73] For most privacy impact assessments, it will not be practicable to develop elaborated scenarios (where each is 10 or 20 or more pages in length, nor the detailed analysis of each, like those in Wright, Gutwirth, Friedewald et al, *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008). It would be far too time-consuming given the exigencies of policy-makers. Anchoring vignettes or mini-scenarios will be much more practicable for most policy-makers and for those preparing privacy impact assessments, especially when they want to engage stakeholders and when there are many different contexts and domains to consider.

[74] Waldo et al., pp. 85–86. See also the anchoring vignette website at http://gking.harvard.edu/files/abs/c-abs.shtml.

[75] Waldo, et al., pp. 24–25.

specificities involved in those technologies.''[76] The EC's RFID consultation and the Data Retention Directive provide us with a foretaste of such micro-policies. The snag for policy-makers, if not for the rest of us, is that such micro-policies cannot be developed in a vacuum: thus, the biggest challenge of all may not be the challenges posed by the new technologies, but ensuring some sort of coherence among these new micro-policies. With shifting attitudes and opinions, policy-makers will be standing on constantly shaking ground.

Acknowledgement

This paper is based on research that was partly supported by the European Commission under its 6th Framework Programme (contract IST-2004-006507). The views expressed are those of the authors alone and are not intended to reflect those of the Commission.

David Wright (*david.wright@trilateralresearch.com*) *Partner, Trilateral Research and Consulting, London;* Serge Gutwirth (*serge.gutwirth@vub.ac.be*) *Professor of Law, Center for Law, Science Technology & Society Studies at the Vrije Universiteit Brussels, Brussels;* Michael Friedewald (*michael.friedewald@isi.fraunhofer.de*) *Senior Researcher, Fraunhofer Institute for Systems and Innovation Research, Karlsruhe;* Paul De Hert (*paul.dehert@vub.ac.be*) *Professor of Law, Center for Law, Science Technology & Society Studies at the Vrije Universiteit Brussels, Brussels;* Marc Langheinrich (*Langheinrich@acm.org*) *Assistant Professor of Computer Science, Faculty of Informatics, University of Lugano (USI); and* Anna Moscibroda (*Anna.Moscibroda@vub.ac.be*) *researcher, LSTS Vrije Universiteit, Brussels.*

[76] European Commission, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, Brussels, 7 March 2007. Later on in the same Communication, the Commission reinforces the notion of ''micro-policies'', as we have termed them: ''Where a particular technology is found to consistently pose questions as regards the application of the data protection principles, and its widespread use or potential intrusiveness is considered to justify more stringent measures, the Commission could propose sector-specific legislation at EU level in order to apply those principles to the specific requirements of the technology in question. This approach was taken in Directive 2002/58/EC on privacy and electronic communications.''