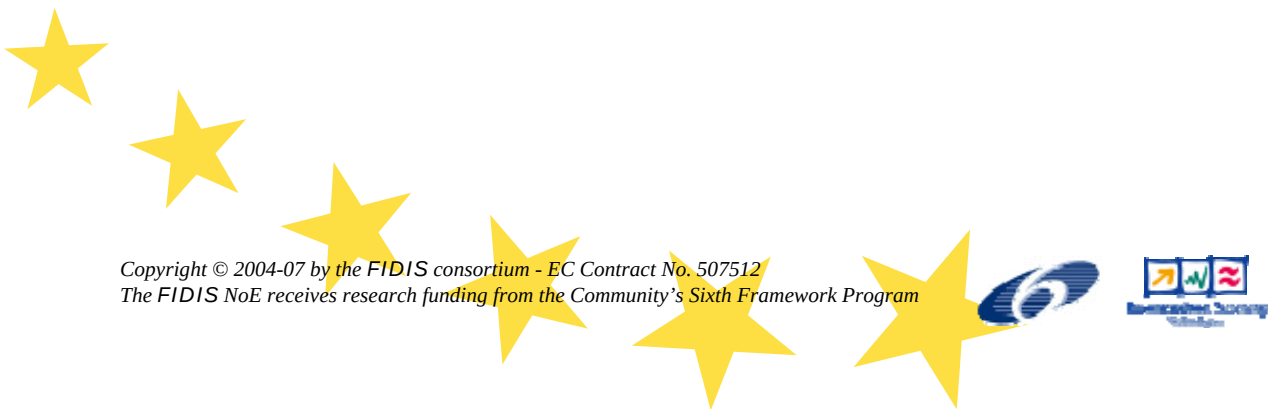
FIDIS

Future of Identity in the Information Society

Title:	"D7.8: Workshop on Ambient Law"
Author:	WP7
Editors:	Mireille Hildebrandt, Els Soenens (Vrije Universiteit Brussel)
Reviewers:	Bert-Jaap Koops (TILT)
Identifier:	D7.8
Type:	[Final]
Version:	1.0
Date:	Thursday, 15 February 2007
Status:	[Final]
Class:	[Public]
File:	D7.8 Workshop Ambient Law'

Summary

The third workshop of Work package 7 on 'A Vision on Ambient Law' (D7.8) was organized at the Vrije Universiteit Brussel on January 26th 2007 as preparation for deliverable 7.9. This report records the decisions taken during the workshop regarding the relevant issues, and takes note of the proposed structure of the report on 'A Vision on Ambient Law', as agreed during the meeting. It also contains a list of participants, the program of the workshop, the slides of the presentations and the working document that was sent round for discussion.



The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	31.01.2007	• Initial release (Els Soenens, VUB)
0.2	02.02.2007	• Integration of notes Anna Moscibroda and Mireille Hildebrandt (Mireille Hildebrandt, VUB)
0.3	05.02.2007	• Adjustments (Bert-Jaap Koops, TILT)
0.4	05.02.2007	• Final version to participants
0.5	13.02.2007	• Final version to Denis Royer

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 Executive Summary	Mireille Hildebrandt (VUB)
2 Decisions made during the workshop	Mireille Hildebrandt, Bert-Jaap Koops (VUB)
3. Participants	Els Soenens (VUB)
4. Annex I: Program	Els Soenens, Mireille Hildebrandt (VUB)
5. Annex II: Slides presentations	Els Soenens (VUB)
6. Annex III: Discussion Paper	Mireille Hildebrandt (VUB)

Table of Contents

1 Executive Summary

This report summarises decisions taking during the January 26th 2007 workshop, preparing the D7.9 report on 'A Vision on Ambient Law'. It relates the provisional structure of D7.9 and the way the contributors will cooperate. It also contains the preliminary documents, such as the program, the list of participants, the discussion paper and the slides presented during the meeting.

2 Decisions made during the workshop

2.1 Editors, Internal Reviewers, Contributions and Time table

Mireille Hildebrandt (VUB) and Bert-Jaap Koops (TILT) will co-edit Deliverable 7.9.

Claudia Diaz (KUL- COSIC) has offered to do the internal review.

Final version to European Commission	1st July 2007
Comments by internal reviewers	15th June 2007
Final draft report (eds.)	1st June 2007
Final draft contributors (all)	10th May 2007
Abstracts contributions (ICPP/SIRRIX, ICRI, VUB, TILT)	1st April 2007
Semi-final draft scenarios (Reading, ICCS, SIRRIX)	15th March 2007
Comments other contributors (all)	7-15 March 2007
First draft scenarios (Reading, ICCS, SIRRIX)	7th March 2007
Sketch of the needed scenarios (eds.)	1st February 2007

2.2 The Structure of the Report 'A Vision on Ambient Law (AmL)' D7.9

2.2.1 Chapter 1: A vision of Ambient Law, conceptual exploration

(Mireille Hildebrandt, VUB; Bert-Jaap Koops, TILT)

In the deliverable, the concept of Ambient Law will be broader than data-protection legislation, and focus on embodying legal norms in technology in the context of Ambient Intelligence in general.

Mireille: Draft concept Ambient Law

'A technological inscription of legal norms that makes possible:

- to implement mandatory parts of e.g. D 46/95 EC
- to trace – via M2M communication – how which personal data are being processed
- to negotiate – via M2M communication – about the exchange and processing of personal data, while staying within the limits of mandatory data protection legislation

In other words: using the technology against which data protection aims to protect in order to achieve effective protection.'

Technological embodiment of legal norms in a constitutional democracy demands specific checks and balances at three different levels:

- the level of legislation (which is both legal and political). At this level, the use of specific technologies to support or enforce legal rules needs democratic legitimisation and needs to fit constitutional demands;
- the level of administration (which is both legal and governmental). At this level, the use of specific technologies to support or enforce legal rules needs to comply with the principles of fair and transparent administration;
- the level of adjudication (which is legal, political, and governmental, because it determines the scope of the law). At this level, the use of specific technologies to support or enforce legal rules must be made contestable.

Major issues arising in the context of cooperating objects in networked environments that allow real-time autonomic profiling in order to seamlessly adapt the environment to a user's anticipated preferences include:

- unfair discrimination (unfair due to the fact that citizens are not aware of who knows what and who decides on which basis);
- the autonomy trap (refined segmentation allows manipulation whenever the user is not aware).

2.2.2 Chapter 2: Scenario I: User Control & Data Minimisation

2.1 Development of the scenario

scenario I is user-centric: the user is empowered in AmI, carrying a device with which to control the environment, for example, by determining which data can be exchanged between user and environment. This may be a ‘privacy-friendly’ and perhaps a commercial doom scenario. Key concepts are 'data minimisation', 'contextual integrity', 'partial identities' (pseudonyms).

2.2 Assessment of existing legal framework (focus on personal data)

ICRI: Focus on Access to Personal Data, Consent, Purpose Limitation Principle. Some observations about the (lack of) enforceability and effectiveness.

2.3 Assessment of existing PETs

ICPP (together with SIRRIX?): anonymisation, pseudonymity, unlinkability, history management, privacy-preserving datamining, trusted computing. Some observations about the reliability of these technologies and their actual application; notes on the (lack of) socio-economic incentives to actually implement wide-spread use of these technologies.

2.4 How to achieve AmL in this scenario

VUB, TILT: the question is whether this is an AmI scenario at all: the intelligence seems to be with the user, not with the environment. Depending on the degree of adaptation and anticipation of preferences, this may or may not be called an AmI scenario. If we can call this AmI, AmL will be established through the architecture of user control.

2.2.3 Chapter 3: Scenario II: Provider Control & Data Maximisation

3.1 Development of the scenario

scenario II is provider-centric: AmI is controlled by the providers of services (and goods, if there still are goods by then). The environment knows exactly who is where and will interact without consent, and perhaps without knowledge, of the user. Data flows freely between users and their devices, service providers, and perhaps third parties as well. This may be a 'user-friendly' and commercial Walhalla scenario. Key concepts are 'data optimisation', 'networked environment' and 'distributed intelligence' (the intelligence flows from the interconnectivity).

3.2 Assessment of the existing legal framework

ICRI: attention to the opposing logic of data minimisation (in data protection legislation) and data maximisation (needed to achieve data optimisation in the scenario of ubiquitous, interoperable, real time and autonomic adaptation of the environment), analysis of the applicability of the directive on telecommunications and its effectiveness within this scenario, analysis of the data retention directive and the framework decision on data protection in the third pillar (police and judicial cooperation in criminal matters). Attention must be on the knowledge that is generated and applied: (how) does the legal framework protect against unfair use of such knowledge, (how) does the legal framework empower citizens (facilitate user control).

3.3 Assessment of relevant PETs and TETs

ICPP/SIRRIX: analysis of the opposing logic of data minimisation and data maximisation, exploration of the idea of TETs that provide citizens with knowledge of the knowledge that is used to influenced their behaviour; exploration of the issue of M2M communication between user and service provider and the ensuing problems of HMIs.

3.4 How to achieve AmL in scenario II

VUB and TILT: to what extent could M2M negotiation empower users in an AmI environment and how does this relate to AmL? What other AmL ways are there of checking the provider-controlled power to make decisions on citizens and consumers, without losing the AmI potential of this scenario?

2.2.4 Chapter 4: Scenario III: Distributed Intelligence & Minimisation of Knowledge Asymmetry

3.1 Development of the scenario

scenario III is a mix: in acknowledging that hiding data can make the environment less intelligent, while unlimited access to data can make individual citizens vulnerable to undesirable profiling, this scenario aims to achieve some kind of balance by minimising knowledge asymmetry.

3.2 Assessment of the legal framework

ICRI: which legal rights and obligations should be invented or adjusted to allow this scenario to take on, especially regarding the knowledge (profiles) that are used to influence people; (how) could these rights be effective without risking the intelligence of the environment?

3.3 Assessment of PETs and TETs

ICPP: which balance of PETs and TETs could create the right balance between protection & empowerment of citizens on the one hand and the intelligence of the environment on the other?

3.4 How to achieve AmL in scenario III?

VUB and TILT: how to combine user-empowerment, M2M negotiations, flexibility, and citizen's control with an intelligent environment that needs randomised data to prevent loss of intelligence with all the ensuing issues of discrimination based on false positives and false negatives?

2.2.5 Concluding Chapter

(Mireille Hildebrandt, VUB and Bert-Jaap Koops, TILT)

3 Participants to the Workshop

Ammar Alkassar	Sirrix
Claudia Diaz	KUL - COSIC
Serge Gutwith	VUB
Mireille Hildebrandt	VUB
Bert-Jaap Koops	TILT
Eleni Kosta	KUL - ICRI
Martin Meints	ICCP
Anna Moscibroda	VUB
Ronny Saelens	VUB
Wim Schreurs	VUB

4 Annex I: Program 26th January 2007

(Disseminated 26th January 2007 to the contributors)

Contributors:

VUB (1,5), Mireille Hildebrandt, Serge Gutwirth, Ronny Saelens, Anna Moscibroda

TILT (1), Bert-Jaap Koops

KUL - ICRI (0.5), Eleni Kosta

KUL – COSIC, Claudia Diaz

ICPP (0.5), Martin Meints

ICCS (0.5)

Reading (0.5)

Sirrix (0.5) - Ammar Alkassar

Conference Room: M.420

Campus VUB Etterbeek

Pleinlaan 2, 105 Brussels - Etterbeek

After being refreshed with coffee VUB and TILT will take the lead on what Ambient Law (AmL) means, what should be its object and how it can achieve this. This will include a discussion of the relationship between law and technology, especially regarding the impotence of present-day administrative law to adequately regulate profiling.

After another coffee 4 parts or elements of AmL will be discussed (see below). This discussion will benefit from cross-disciplinary introductions. We invite all participants to prepare presentations on this, or at least contributions to a brain storm. To appetize you, we have attached provisional names to these subjects, please do not hesitate to change your contributions. We need unconventional but rigorous brains here!

At 16.00 we will discuss the structure of the report and the distribution of tasks, closing the meeting at 17.00.

9.15: Coffee and registration

9.30: Introduction to Ambient Law

(Mireille Hildebrandt, VUB)

10.00: Regulating Technologies

(Bert-Jaap Koops, TILT)

10.30: coffee

11.00: I Technological embodiment of mandatory data-protection legislation

Assessment of the relevant norms: ICRI, VUB, TILT

Technological implementation: ICPP, Sirrix, VIP,

12.00: II Technological transparency tools to detect the types of profiles that may be applied

Assessment of necessary legal norms (not yet part of positive law): VUB, TILT

Technological articulation: COSIC, Sirrix, ICPP, Reading

13.00: lunch

14.00: III Machine to machine (M2M) communication to negotiate with the service provider about the level of anonymity and unlinkability

Assessment of relevant legal norms: ICRI, VUB, TILT

Technological instrumentation: Reading, COSIC, Sirrix, VIP

15.00: IV Machine to machine (M2M) communication to negotiate about the application of profiles predefined by the (potential) client

Assessment of relevant legal norms (positive law and necessary legal norms): VUB, TILT

Technological embodiment: Reading, COSIC, Sirrix, ICPP

16.00: Structure of the report and division of tasks

17.00: End of the meeting

The actual program was adapted to accommodate emerging issues. The focus was (1) on the technological embodiment of existing legislation in the field of data protection (data minimisation and partial identities like pseudonyms, history management, privacy-preserving data mining PPDM)) and (2) on the need to envision new legislative and technological tools to counterbalance the unequal access to the knowledge contained in profiles.

It remained unclear/contested to what extent Ambient Intelligence can work in the case of data minimisation: does this necessarily make the environment less intelligent? For this reason, 3 scenarios were considered to be of utmost importance:

1. **scenario 1 is user-centric**: the user is empowered in AmI, carrying a device with which to control the environment, for example, by determining which data can be exchanged between user and environment. This may be a 'privacy-friendly' and commercial doom scenario (?). Key concepts are 'data minimisation', 'contextual integrity', 'partial identities' (pseudonyms).
2. **scenario 2 is provider-centric**: AmI is controlled by the providers of services (and goods, if there still are goods by then). The environment knows exactly who is where and will interact without consent, and perhaps without knowledge, of the user. Data flows freely between users and their devices, service providers, and perhaps third parties as well. This may be a 'user-friendly' and commercial Walhalla scenario. Key concepts are 'data optimisation', 'networked environment' and 'distributed intelligence' (the intelligence flows from the interconnectivity).
3. **scenario 3 is a mix**: in acknowledging that hiding data can make the environment less intelligent, while unlimited access to data can make individual citizens vulnerable to undesirable profiling, this scenario aims to achieve some kind of balance by minimising knowledge asymmetry.

The technical partners Reading, ICCS and SIRRIX should be able to provide relevant scenarios, possibly inspired by the scenarios already developed by SWAMI.

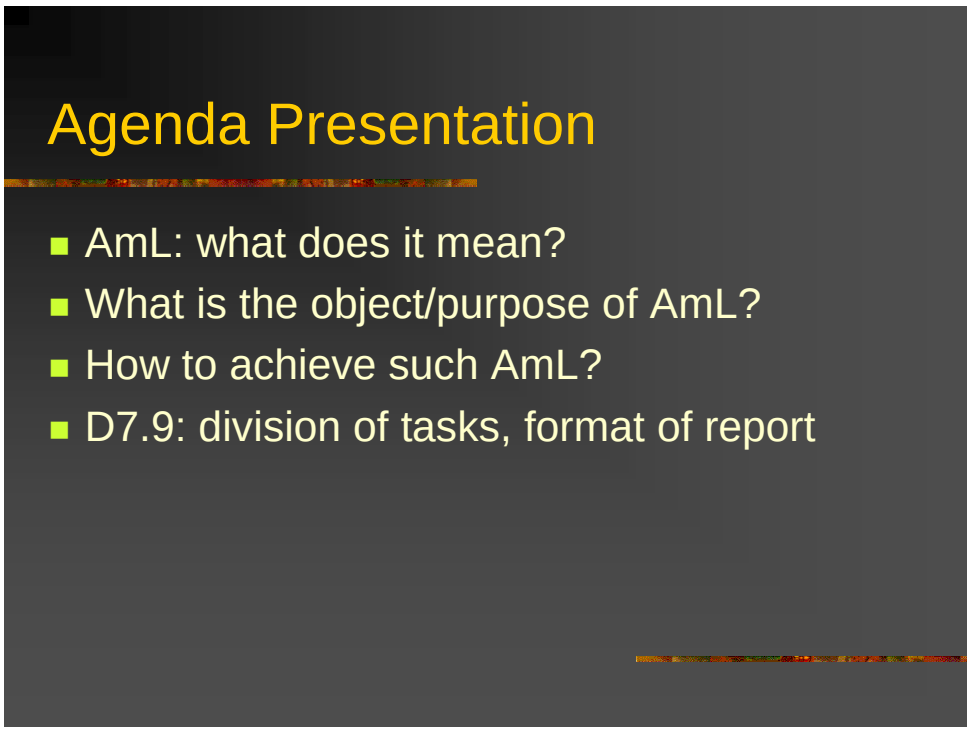
As indicated above it was agreed that ICPP – together with SIRRIX – will develop an overview of the state of the art of technological devices, mostly privacy-enhancing technologies (PET). As discussed in D7.7, contemporary PETs are all focused on personal data, leaving important lacunae in the case that these data are anonymised and having no regard whatsoever for the knowledge that is built and used on the basis of such data (profiles emerging in the process of KDD, using techniques like clustering and association rules).

The legal scholars at ICRI, TILT and VUB will look into the possibility to develop legal transparency tools as regards profiles that may impact our behaviour without our awareness. In terms of access to these profiles, the problem may be (1) that they have not been constructed out of one's personal data (but out of other personal or anonymised data), thus rendering data protection legislation inapplicable and (2) that the profiles are protected by means of intellectual property, e.g., forming part of a database.

TILT and VUB will assess to what extent existing legal and technological tools achieve something like AmL, taking into account the checks and balances warranted in a constitutional democracy that incorporates the rule of law.

5 Annex II: Slides of the presentations

Presentation of Mireille Hildebrandt: Introduction to Ambient Law



AmL: what does it mean 1?

- D7.3:
- legal regulation integrated with computer code for instance on the PDA of a data subject) that regulates the subjects interactions with an AmI environment in accordance with data protection and/or other relevant legal norms

AmL: what does it mean 2?

- 3rd workplan D7.9:
- Ambient Law is the articulation of legal rules in technological infrastructure.

AmL: what does it mean 3?

- draft VUB contribution D14.2:
- a *vision* of AmI requires a *vision* of AmL:
- technological embodiment of legal or of other regulatory (i.e. behaviour influencing) rules and on the regulatory side-effects of technological developments and applications

What is the object of AmL?

- AmI applications may imbed rules that influence people's choices or behaviours and impact their fundamental rights

What is the object of AmL?

- AmI applications may use technologies that countervail the technologies of control, this would fall in the scope of AmL

How to achieve AmL 1?

- technological embodiment of mandatory data protection legislation, effectively ruling out non-compliance by service providers
- brainstorm:
  - assessment of the relevant legal norms
  - technological implementation

How to achieve AmL 2?

- technological transparency tools to detect types of profiles that may be applied (may influence our choices and behaviour)
- brainstorm:
  - assessment of necessary legal norms
  - technological articulation

How to achieve AmL 3?

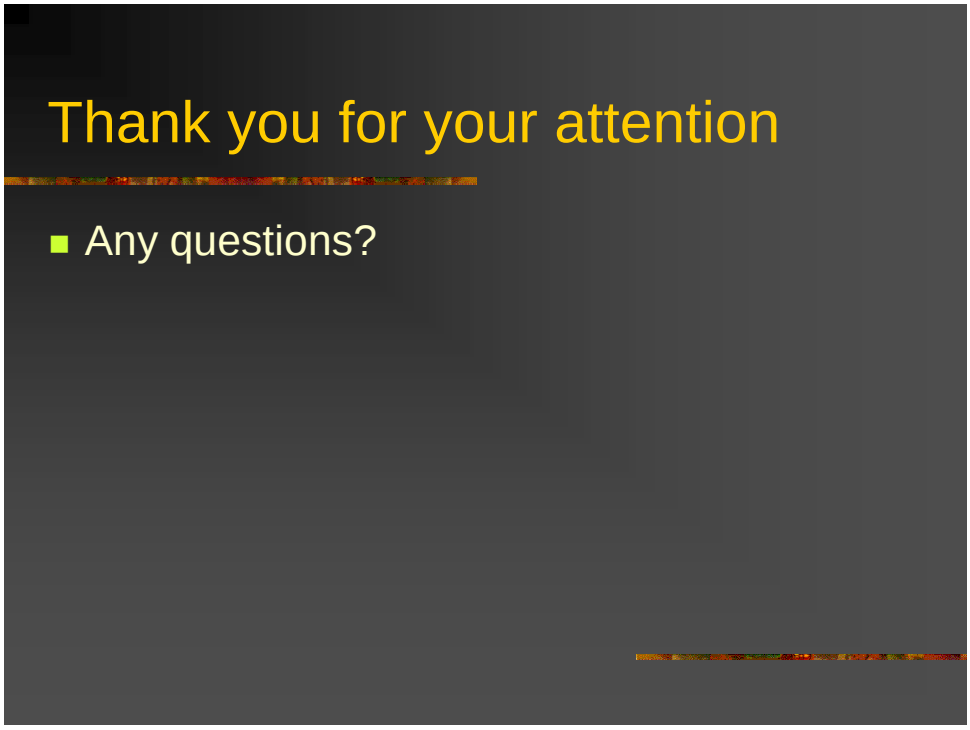
- M2M communication to negotiate with the service provider about the level of anonymity and unlinkability
- brainstorm:
  - assessment of the relevant legal norms
  - technological instrumentation

How to achieve AmL 4?

- M2M communication to negotiate about the application of profiles predefined by the (potential) client
- brainstorm:
  - assessment of relevant legal norms
  - technological embodiment

D7.9 Division of Tasks

- format:
- VUB & TILT main texts
- ICPP, SIRRIX, ICCS, Reading, ICRI reply


Thank you for your attention
Any questions?

Presentation Bert –Jaap Koops (TILT)

Regulating Technologies

Basic issues for Ambient Law

prof.dr. Bert-Jaap Koops

Tilburg Institute for Law, Technology, and Society (TILT)
Universiteit van Tilburg
e.j.koops@uvt.nl

10 november 2032

Regulation of Technology… (1)

- is harder than you (might) think
  - technology moves faster than the law
    - so: “regulation should be technology-neutral”
    - but can it? too abstract laws don’t provide legal certainty
  - technology is international, the law (still often) isn’t (and often can’t be)
  - so why don’t we stick to self-regulation?
    - tiny problems, e.g., enforcement, protecting the interest of weak parties
  - law on paper ≠ law in practice
    - e.g., data-protection law
  - laws have to be made, but technology is too hard to understand for (many) legislators

26 January 2007 2

Regulation of Technology… (2)

- is, however, not so bad after all
  - contrary to common perception, lawyers do not always create problems, they also solve problems
  - technology has a large impact on society, and can have negative effects if not regulated
  - good laws can stimulate technology
- but what is a good law?
  - basic procedural requirements: well-informed, well-balanced, democratically legitimised, and following common-sense thumb rules for law-making
  - basic substantive requirements: constitutional rights, fundamental principles and values, core cultural values

26 January 2007 3

Regulation by technology…

- is (sneakily) happening more and more
  - from speed bump
  - to DRM, filtering, search engines, GMOs
- put on the agenda by Reidenberg ('Lex informatica') and Lessig ('Code as code', 'code as law'), developed by Brownsword, Asscher (& TILT)
- if technology 'is' law, what about the challenges of:
  - democratic legitimacy
  - transparency of norms ('everyone should know the law')
  - changing, correcting and updating norms
  - fuzzy and open norms
  - allowing exceptions
  - civil disobedience (is there an escape?)

26 January 2007 4

In a world of Ambient Intelligence

- the law as we know it will, in many respects, fail
  - data-protection law based on outdated paradigm
  - privacy, get over it
  - discrimination will become a big issue
  - current legal-protection mechanisms for weak parties (citizens, consumers) become meaningless
- therefore
  - continue making good laws
  - but also develop Ambient Law by building in legal-protection norms in AmI
  - while addressing the challenges of 'code as law'

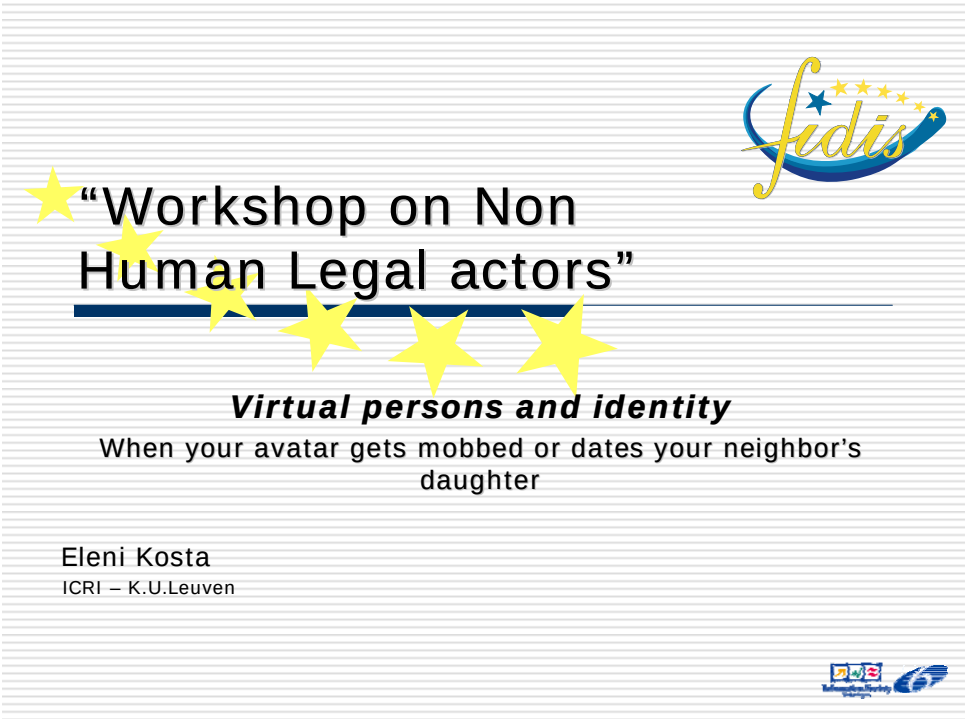
26 January 2007 5

Nice ambition, but how do you plan to do this?

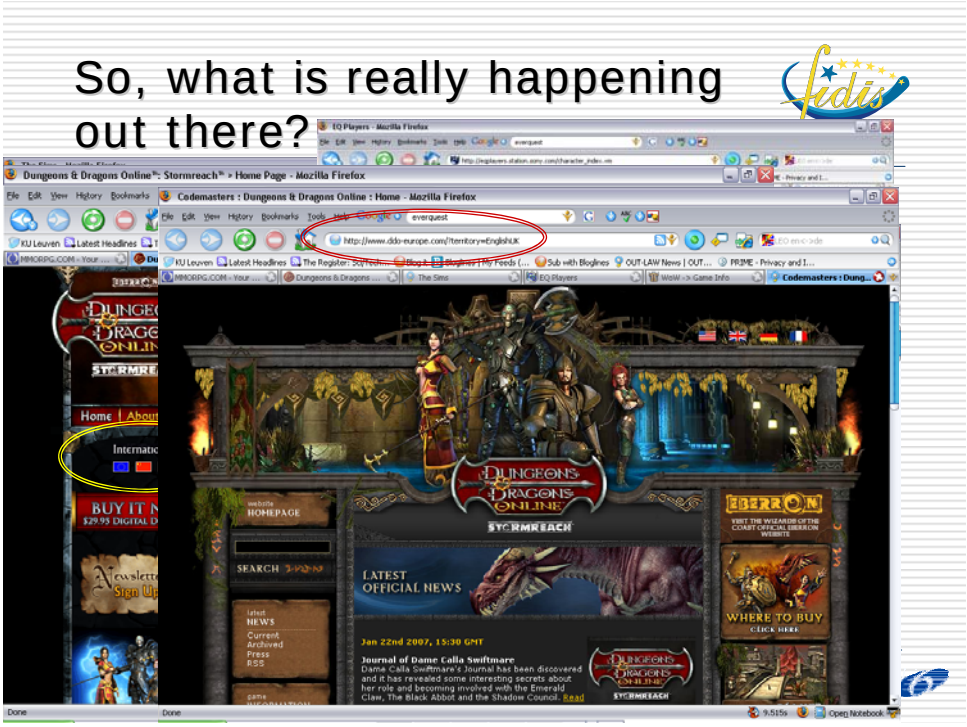
?

26 January 2007 6

Presentation Eleni Kosta (KUL- ICRI): Virtual Persons and Identity




Online games use graphics to create an illusion of a "real world" of tangible objects located in relationship to one another. If we apply the metaphor of "objects" placed in a "space" to the intangible –to the world of ideas- new forms of communication open up.
David Johnson
25.01.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
3


So, what is really happening out there?
fidis
Dungeons & Dragons Online™: Stormreach™ : Home Page - Mozilla Firefox
Codemasters : Dungeons & Dragons Online : Home - Mozilla Firefox
DUNGEONS & DRAGONS ONLINE
STORMREACH
EBERRON
LATEST OFFICIAL NEWS
WHERE TO BUY
Journal of Dame Calla Swiftmare

In the description of the work package…

"We see these virtual persons (characters) as masks used by subjects (human players, computer programs) to act and interact within the game"

25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 5

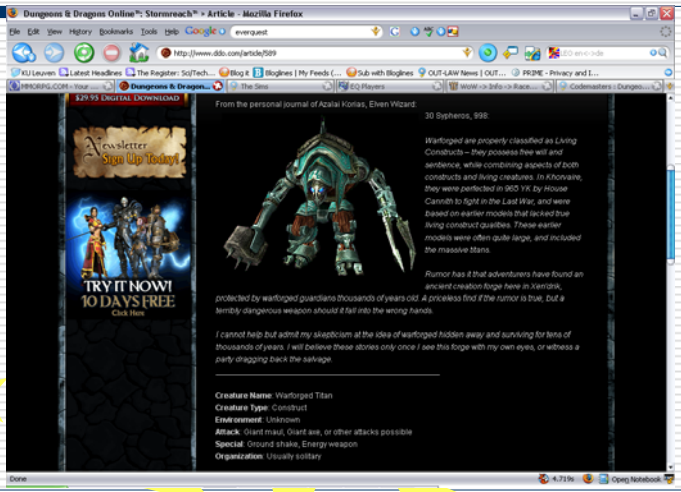
Like…

25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 6

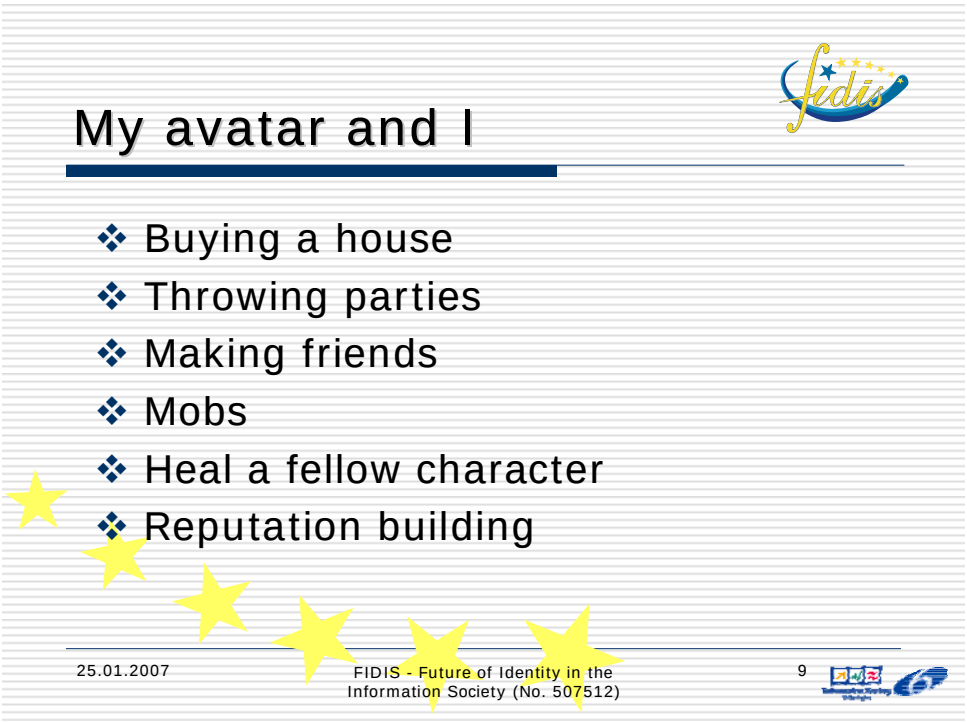
Or like...

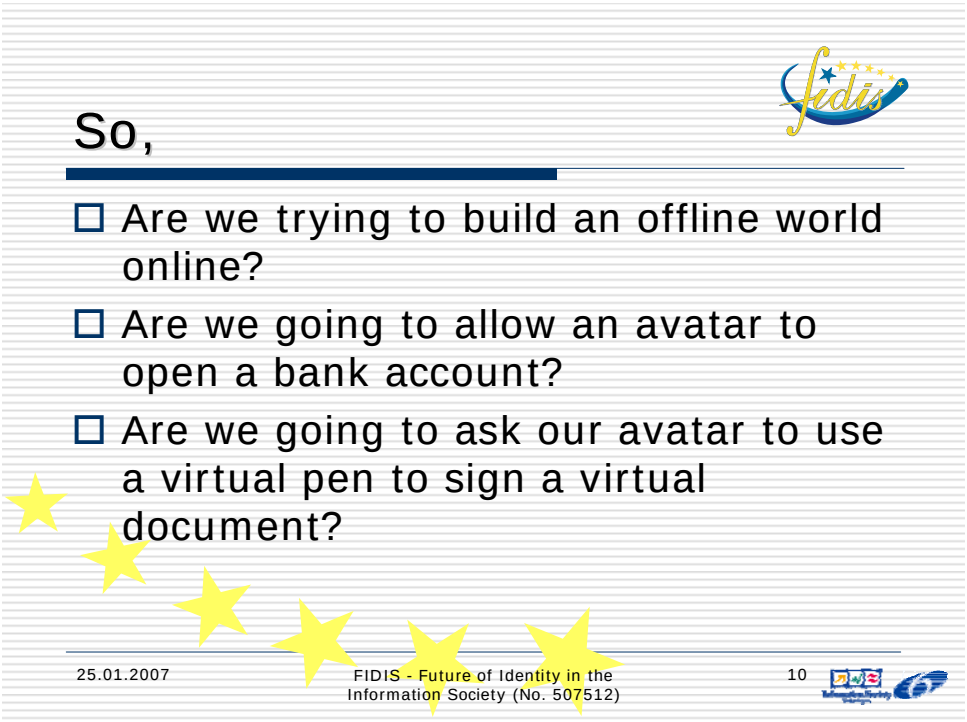
25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 7

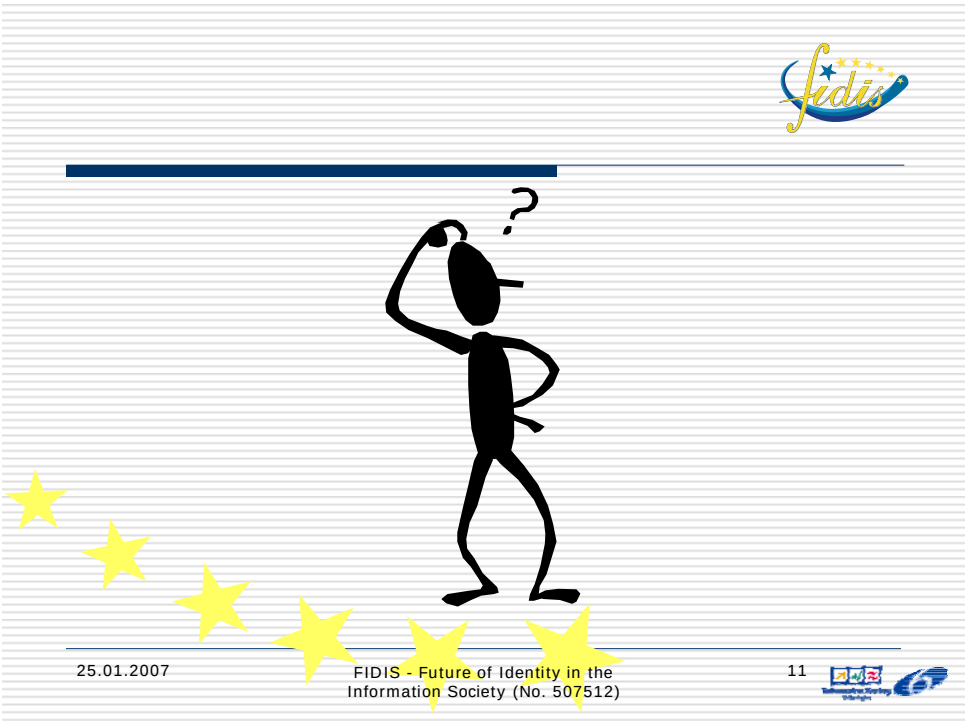
Or even...

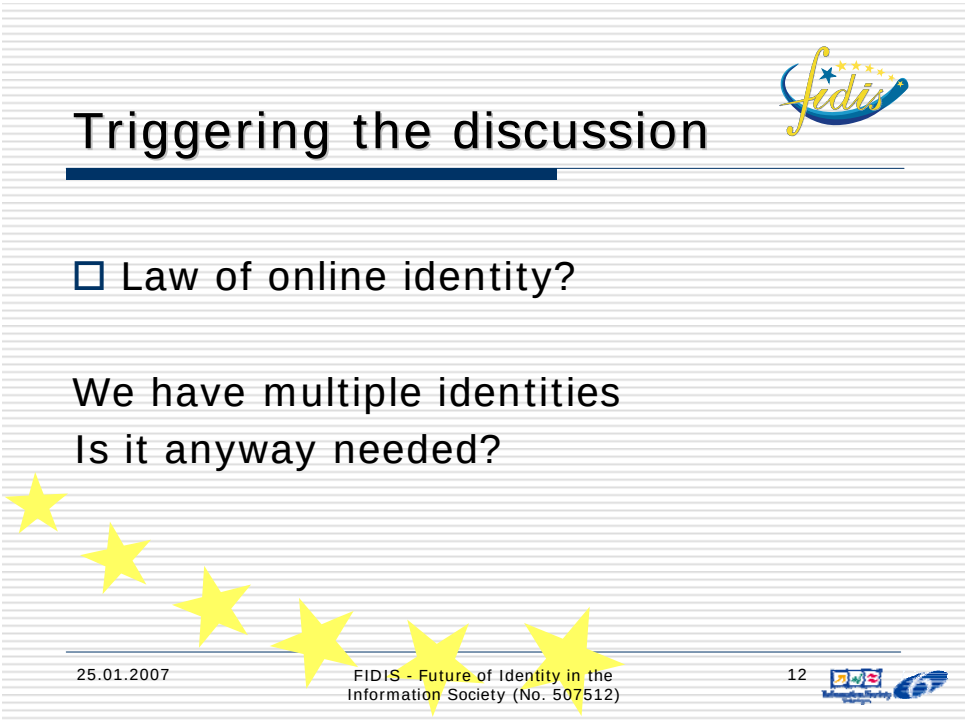


25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 8


My avatar and I
Buying a house
Throwing parties
Making friends
Mobs
Heal a fellow character
Reputation building
25.01.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
9


So,
Are we trying to build an offline world online?
Are we going to allow an avatar to open a bank account?
Are we going to ask our avatar to use a virtual pen to sign a virtual document?
25.01.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
10


25.01.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
11


Triggering the discussion
Law of online identity?
We have multiple identities
Is it anyway needed?
25.01.2007
FIDIS - Future of Identity in the Information Society (No. 507512)
12

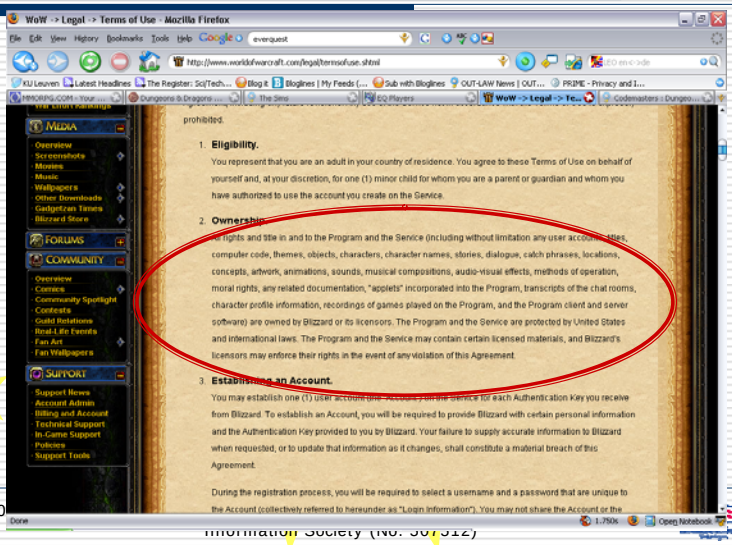
Triggering the discussion

- Who owns my avatar (or else: hands off my avatar!)
- Who owns my reputation

Online intermediaries have "ownership of online identities and reputations" being able to remove identities they don't like, according to their EULAs.

25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 13

From the EULA of "World of Warcraft"



25.01.20 Information Society (No. 507512)

Triggering the discussion

Codes of conduct

Removal with the agreement of the online community

U.S. approach*

- Avatar could be protected under the right of publicity
  - The right of publicity enables the individual to control the commercial use of their identity
    - ? Can an avatar be seen as part of an individual's persona?
    - ? Is an individual in a virtual community seen to hold rights in their personality?

* Some scholars at least!

Other issues...

- ***Virtual property rights***
  - *Norrath*, the virtual kingdom of *Everquest*, had, as of 2002, a greater net worth than Bulgaria and a higher GNP per capita than India or China
  - In *Project Entropia*, a virtual island was bought for $26.500, a space station for $100.000).

25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 17

Questions and Answers

Thank you for your attention!
Any questions?

eleni.kosta@law.kuleuven.be

25.01.2007 FIDIS - Future of Identity in the Information Society (No. 507512) 18

6 Annex III: Discussion Paper: 'A Vision of Ambient Law'

(Disseminated amongst contributors 14th December 2006)

6.1 Introduction

Deliverable 7.9, 'A Vision of Ambient Law', aims to refine the conceptualisation of the vision of ambient law that should act as a counterpoint to the vision of ambient intelligence. In section 1.2 we present the references to the term ambient law within FIDIS documents. In section 1.3 we present a selection of relevant literature on the relationship between law and technology. In section 1.4 we suggest a framework for discussion and reporting within the workshop of 26th January and D7.9.

6.2 Provisional definition and elaboration in FIDIS documents

6.2.1 Provisional definition in D7.3

Ambient law is legal regulation integrated with computer code (for instance on the PDA of a data subject), that regulates the subjects interactions with an AmI environment in accordance with data protection and/or other relevant legal norms.

6.2.2 Provisional definition 3rd workplan D7.9

Ambient Law is the articulation of legal rules in technological infrastructure. This will be the working definition for D7.9, which may be refined at the end.

6.2.3 Provisional elaboration in draft for VUB contribution D14.2

In the course of the FIDIS cooperation within the workpackage on profiling we have come to the conclusion that to achieve an effective legal regulation of the access to and use of profiles (including the possibility to contest these), this regulation must be articulated in the technological design of AmI devices. The *vision* of AmI thus requires a *vision* of Ambient Law. At present, workpackage 7 on profiling is preparing the ground for a report on such 'Ambient Law', to be finalised in the middle of 2007. A vision of Ambient Law should reflect on the technological embodiment of legal or of other regulatory (i.e., behaviour-influencing) rules and on the regulatory side-effects of technological developments and applications. On the one hand, in AmI applications, rules may be embedded that influence people's behaviours or choices and thus impact their fundamental rights. AmI could for example embed privacy-threatening or transparency-threatening technologies. On the other hand, AmI can also use technologies that countervail the 'technologies of control' used in an AmI world. For example, such ambient law could require:

- technological embodiment of mandatory data-protection legislation, effectively ruling out non-compliance by service providers;
- technological embodiment of transparency, for instance requiring a user's proxy that is able to detect the types of profiles that may be applied and that warns the user if this may be disadvantagous;
- technological embodiment of machine to machine (M2M) communication to negotiate with the service provider about the level of anonymity and unlinkability
- technological embodiment of machine to machine (M2M) communication to negotiate about the application of profiles predefined by the (potential) client; such negotiations could concern the terms of the contracts made between service provider and client, for instance the price, the exchange of data etc.

Having access to the types of profiles that may be applied should reduce the risk of falling victim to illegitimate price (or other) discrimination and should counter attempts to manipulate behaviour without awareness of the client.

6.3 Relevant literature on Code as Law

Since Lawrence Lessig's Code and other laws of cyberspace many lawyers, computer scientists and policy makers have embraced the idea that the architecture of ICT have a major impact as regulators of human and non-human interaction. Recognising that computer code both enables and restricts our actions, many have come to believe that code can be equated

with law. Such an equation would ignore major difference and has been critised from the perspective of democracy and rule of law, as we don't want to live under the rule of technology. However, we think it a mistake to ignore the regulatory impact of technological infrastructures and consider a reconceptualisation of the relationship between different types of regulation of foremost importance.

Clarke, R. (1994). "The Digital Persona and its Application to Data Surveillance." *The Information Society* **10** (2)

Roger Clarke may be the first to have detected the importance of a digital proxy to enable M2M communication with service providers in an online environment. In an AmI environment such a proxy would be something like a PDA, which would likewise serve as a proxy for an individual person, for a category of persons or for different 'identities' or roles of one person (depending on the different contexts in which this person moves around).

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, Basic Books

Reidenberg, J. R. (1998). "Lex Informatica: The Formulation of Information Policy Rules Through Technology." *Texas Law Review* **76** (3): 553-585

Lessig detects four regulatory mechanism: law, market, code and social norms. Though one can argue that in the end law, market and code depend on social norms to be interpreted and applied, his book provides a refreshing approach to regulation. Technologies constrain our actions by both inducing or enforcing specific behaviours and inhibiting or ruling out specific behaviours. General statements about the rule of technological devices or infrastructure therefor make no sense: each infrastructure much be assessed for its potential impact. In the case of AmI such impacts are mostly discussed in terms of privacy or data protection, but this seems to restrict the scope of the debate. Based on FIDIS findings one could argue that the relevant consequences of pervasive profiling will be segmentation and discrimination on the one hand and what Zarsky calls 'the autonomy trap' on the other hand. To counter undesirable effects the technologies that produce such consequences should be used to empower citizens.

Reidenberg takes a more direct approach to the implementation of policy rules by means of technologies; his understanding of law seems very instrumental, implying that legal tools can be replaced by technological tools on the sole basis of their comparative efficiency and effectiveness. His view of both law and technology seems to take for granted that these are just neutral tools, a vision to which we cannot agree and that he subsequently, in ‘States and Internet Enforcement’, seems to have abandoned by acknowledging the controlling power of technologies that enforce rules. Still, Lessig seems more aware of the normative impact of both technological and legal tools.

Brownsword, R. (2005). "Code, control, and choice: why East is East and West is West." *Legal Studies* **25** (1): 1-22

Tien, L. (2004). "Architectural Regulation and the Evolution of Social Norms." *International Journal of Communications Law & Policy* (9)

The criticism in the field of lawyers, legal theorists and legal philosophers seems directed to Reidenberg's instrumentalism, but they do attack Lessig for his attempt to use code as law. The problem with this type of criticism is that it builds on inadequate ideas about the normative impact of technology (taking for granted a kind of technological determinism) and aims to rule out any attempt to articulate legal norms in technological devices. One of the arguments is the fact that technologies are constructed outside the domain of democratic decision making, while one could easily turn this argument around to insist on new political practices to facilitate democratic decision-making regarding devices that have a major impact on our choices of action.

Koops, B.-J. and R. Leenes (2005). "'Code' and the Slow Erosian of Privacy." *Michigan Telecommunications and Technology Law Review* **12** (1): 115-189

Leenes, R. and B.-J. Koops (2005). "'Code': Privacy's Death or Saviour?" *International Review of Law Computers & Technology* **19** (3): 329-340

FIDIS researchers Koops and Leenes take a more nuanced view. In the first article they discuss software code as a tool for law enforcement (embedding interceptibility and/or privacy protection), while indicating that many of the consequences of software code are unintentional but rather serious side-effects. They argue that PETs may be an adequate answer, rather than the commodification of data. In the second article they discuss why PETs are not widely used. They explain that data protection, based on the idea of data minimisation is not in the ruling paradigm of those in charge of profiling; they plead a paradigm shift from data maximisation to privacy by design.

Hildebrandt, M. (2007). Technology and the End of Law. *The Limits of (the Rule of) Law*. E. Claes and B. Keirsbilck

FIDIS researcher Hildebrandt discusses three perspectives on technology: (1) technological determinism, (2) the neutrality thesis and (3) technological pluralism, in counterpoint with (1) legal substantivism, (2) legal instrumentalism and (3) a relational conception of law. Connecting technological pluralism with a relational conception of law she argues (1) that democratic participation is required for the introduction of profiling technologies, and (2) that effective legal regulation of the impact of profiling technologies on human freedom and

identity building warrants the technological embodiment of legal norms. This could mean that: (a) mandatory legal norms should be inscribed into the technologies to preclude violation as much as possible and (b) exchange of data and transparency of profiles should be facilitated by personal digital agents.

6.4 From data minimisation to minimisation of knowledge asymmetry

AmI depends on data maximisation and according to some authors urgently calls for a paradigm shift from the protection of data to the transparency of knowledge (Zarsky 2002-2003). Instead of focusing on the collection and storage of personal data we need to concentrate on the application of profiles. Minimising data will render an environment less intelligent, thus obstructing the objectives of AmI. If we are confronted with the realisation of AmI, we need an ambient law that directs it attention to transparency of profiles, which function like knowledge claims. Instead of spending all energy on PETs we should start investing in tools to establish minimisation of knowledge asymmetry (Jiang 2002).

These are central findings within workpacakge 7.

6.5 Further Issues

6.5.1 Which mandatory legal rules are missing?

Before moving into the issue of technological embodiment of legal norms, we will need to articulate the legal status of profiles, entailing a paradigm shift from personal data to profiles. Which mandatory legal rules are needed to provide adequate transparancy about the profiles that impact our lives?

6.5.2 Which type of negotiations must be supported?

Ambient law should not only embody mandatory legal rules, but also enable negotiations between consumers and service providers. In view of the principle of minimum knowledge asymmetry the power balance between parties and the long-term effects of such negotiations need to be taken into account when designing the technological tools to enable fair transactions.

6.5.3 M2M communication and HMI (TETs)

After assessing the mandatory legal rules and the types of negotiations that need technological embodiment the technological possibilities need to be assessed, taking into account that legally protected trade secrets and intellectual property may preclude adequate access to profiles.

6.6 Bibliography

Jiang, X. (2002). *Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social*. *Privacy Workshop September 29, 2002, University of California, Berkeley*. Berkeley, available at: http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf

Zarsky, T. Z. (2002-2003). ""Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion." *Yale Journal of Law & Technology* **5** (4): 17-47