SIAM

Security Impact Assessment Measures

SIAM Final Conference Report

Deliverable 13.18

SIAM Final Conference Report

Technical University Berlin

Dr. Leon Hempel

Hans Lammerant

Lars Ostermeier

Tobias Schaaf

Project number
261826

Call (part) identifier
FP7-Security-2010-1

Funding scheme
Collaborative Project

Contents

Final SIAM conference

Aim and setup

On 22nd January 2014 the SIAM project holds its final conference. Aim was to present and disseminate its results to a varied public of stakeholders, like data protection officials, academics, industry professionals, professionals and scholars active in the field of impact assessments etc. Main objective was to present the SIAM Assessment Support Tool, but also some of the research results and methods underlying this tool. The second objective was to open up the discussion on the integration of normative and empirical approaches to impact assessment. This integration has been one of the hurdles with which the SIAM-project was confronted. Discussing the results and experience of the SIAM-project in this regard with other impact assessment scholars deepens the theoretical understanding of impact assessments and can improve the development of impact assessment methodologies.

To attract this varied public the SIAM project opted to look for synergies with other initiatives and to be able to attract a larger public through collaboration. Therefore SIAM integrated its conference into the CPDP conference and collaborated with the EPINET project.

The annual Computers, Privacy and Data Protection (CPDP) conference, now in its 7th edition, offers the cutting edge in legal, regulatory, academic and technological development in privacy and data protection. It gathers key stakeholders from government, academia, industry and civil society to exchange ideas and discuss emerging issues in information technology, privacy and data protection. This unique multidisciplinary formula has served to make CPDP one of the leading data protection and privacy conferences in Europe and around the world. Privacy Impact Assessments have been a point of attention at its earlier editions.

All this made CPDP the ideal platform to present the result of the SIAM-project, while engaging its diverse public in a discussion on impact assessments. CPDP received more than 800 visitors and the SIAM panels attracted around 150 persons.

In order to create an in-depth exchange on impact assessments SIAM collaborated in these panels with the EPINET-project. EPINET stands for the Integrated Assessment of Societal Impacts of Emerging Science and Technology from within *Epi*stemic *Net*works. The EPINET-project explores the plurality of different assessment practices and uses the concept of epistemic networks to do this in a holistic manner. The collaboration with EPINET ensured the participation of a diverse range of impact assessment scholars in the panels. This allowed SIAM to present its results to the wider impact assessment community as well as to use the occasion to confront its methodologies and theoretical assumptions with those of other scholars.

The conference was build up through 3 panels. The first panel was called 'Legal and STS Technology Impact Assessments' presented the theoretical field on impact assessments, and more specifically concerned normative and empirical approaches to impact assessments.

The second panel, called 'Round Table on Normative and Empirical Perspectives on TIA' continued on this subject in a more explorative way through a round table with a range of scholars and practitioners. The third panel, called 'From theory to Practice: Integrated TIAs and their Computational Support', presented the results of the SIAM project and related it to the discussions in the earlier panels.

Panel 1: Legal and STS Technology Impact Assessments

This panel opened the theoretical discussion and delineated the major themes of discussion. It targeted the question of how legal and empirical impact assessments differ and what it means to frame law and social science through the lens of an 'ecology of practices'.

It addressed further questions like:

- What are the gains and the risks of technology impact assessments in the broad sense?
- What is the difference between a PIA and a DPIA and should we applaud the legal obligation to do a DPIA?
- How can we assess the impact on a right, as compared to the impact on the substance of a right?
- Do technologies have normative impact, and what does this mean for courts and legislators?

Serge Gutwirth opened the panel by presenting the concept of an 'Ecology of practices', originating from the work of Bruno Latour and Isabelle Stengers. He presented the scientific, the technical, the political and the legal as distinct regimes of enunciation and of veridiction, or as distinct practices with their own, irreducible properties and characteristics. Every practice has its own constraints and when it gets mobilized by another practice, it is limited by those internal constraints. Each practice can not be reduced to another. With Stengers, Gutwirth promotes to see the collection of distinct practices as an ecology of practices, functioning together without an ultimate arbiter but through relating by each other's practices of composing and articulation.

Niels van Dijk offered a reflection on the 'risk to a right'. This peculiar formulation can be found as trigger for the obligation to perform a data protection impact assessment (DPIA) in the draft General Data Protection Regulation (GDPR). After introducing the DPIA and its legal and historical context, he pointed out that rights and risks belong within different spheres of knowledge and social organization. Rights are defined through legal concepts, while risk is defined based on scientific concepts of probability. Merging risks with rights leads to mutual transformations of both concepts. Van Dijk illustrated this through presenting 4 different relations between risks and rights.

'Risks or rights' presents their relation as a trade-off or something to be balanced. This is very present in the post 9/11 counter-terrorism discourse. In organizational risk management the relation can be qualified as 'Rights as risks'. Here negative public perceptions of consumers and media are seen as sources of risk that needs managing. This extends to privacy rights and possible litigation. The current assessment of privacy risks of new technologies fits into this approach. DPIA becomes a probabilistic risk assessment methodology. 'Risks within Rights' points to specific legal ways of dealing with risks to public interest in jurisprudence of the courts. This relation is not characterized as a general choice or a balance, but as a specific composition of rights, risks and public values. The proportionality requirement involves providing a fair mediation between different conflicting interests at stake in a concrete case. What can a 'Risk to a Right' mean? Assessing such risk can involve assessing how a certain technology can pose a risk to a right (of privacy and data protection). It can also imply analyzing how certain assessments can themselves put that right at risk.

Following this exploration Niels Van Dijk considered in a similar way the role of publics and public participation in this risk assessment. From environmental governance we can learn that risks are often framed as an objective issue concealing normative commitments and values. Such risks are assessed by experts through quantitative analysis without participation of the parties affected. But the limits of scientific expertise and the need to draw on a multiplicity of types of expertise, including lay knowledge, leads to institutions and procedures to increase public participation in the risk assessment and management process. The GDPR provides that during the DPIA the controller has to seek the views of the data subjects. On the other hand, the template for the smart grid DPIA seems to consider the public itself as a risk and grants it only a passive role. Looking to 'publics in rights' Van Dijk points to human rights jurisprudence on environmental issues, which delineated procedural rights for the public. The DPIA extends this procedural turn now to data protection.

Based on this analysis Van Dijk poses the question what ecology of practices does a DPIA require and what is the role of law? Aside of the approach which sees data protection as a new source of risk and the one who sees the role of law as providing a forum to judge privacy infringements, he points to the model given by the ECtHR of the interaction between (environmental) risks and the right to privacy in which both concepts undergo a change. This consist in a procedural turn to human rights in the encounter with (environmental) risks, and in a proportional turn to risks as one mode of contestable evidence mediated with individual rights and public values.

Roger Clarke presented the diverse field of impact assessments, ranging in focus from technology, project, social impacts to compliance. In a next step he situated risk assessment in the whole of assessment methods to prepare a business case. Legal compliance is only one and usually minor consideration in risk assessment. Risk assessment is a well-established technique and is the subject of various standards. On the other hand, it is commonly used relatively late in projects, and is mostly undertaken from the perspective of a single organization. Technology Assessment on the other hand is a communicative process, both scientific and participative or interactive, in order to contribute to the formation of opinions on societal aspects of science and technology. TA does not adopt the limited perspective of the project sponsor, but reflects the needs of all parties involved. The same is valid for social impact assessment, which looks into impacts on the social environment.

Seen from this range of impact assessments Roger Clarke made an evaluation of the specification of a DPIA in article 33 of the draft GDPR. He considers the scope of this specification to be highly ambiguous. In some places, the broad expression 'rights and freedoms of data subjects' is used, but in the key locations the very narrow expression 'the protection of personal data' is applied. He concludes that the DPIA notion in the GDPR is not driven by social values, but instead is at most a mere Legal Compliance Assessment. As such it is much more limited than a risk, technology or impact assessment.

Mireille Hildebrandt addressed the relation between law and technology and drew some conclusions concerning DPIA and data protection by design. She introduced the subject by the question Would you rather have food or the right to food? Privacy or the right to privacy? This question is not easy to answer, but the struggle for equal rights highlights that having access to food or privacy is not enough, we want to secure the right to have it, not the privilege, nor a contingent opportunity. Now the DPIA introduces a novel legal obligation to assess the impact on and risk to fundamental rights. Impact assessment relate to the principle of precaution. If the impact is uncertain, ambiguous or the risks are major and/or unfairly distributed this principle requires intervention to mitigate this risks and in the end political decision making.

When technology gets regulated through law, often the plea for technology neutral law is heard. This is based on 3 objectives. First the innovation objective, or avoiding that innovation gets stifled by giving an unfair advantage to particular technologies. Further the sustainability objective, or making sure that legal regulations do not require too regular changes to adapt the law to technological changes. And also the compensation objective, or law compensates for detrimental effects of certain technologies. Protection offered by fundamental rights should not depend on a specific technological infrastructure. However, legal protection can not be understood as independent from the information and communication technologies in use. Technologies induce or enforce and inhibit or overrule our behaviors. They change power relationships and control over things, people and environment. As such they transform expectations and what can be considered as reasonable expectations. This can require technology-specific law, in order to compensate for the loss of protection. And it requires us to investigate how socio-technical systems impact on fundamental rights.

When we look into the DPIA and Privacy by design, we may not confuse privacy with data protection. The right to privacy is a freedom from unreasonable constraints on the construction of one’s identity. The right to data protection entails a set of conditions that must be met to process data that refer to an identified or identifiable person. It aims to contribute to several fundamental rights, like privacy, non-discrimination, due process and the presumption of innocence, but these fundamental rights cannot be replaced by it. Privacy cannot be designed, but we can demand that our environment be designed in a way that enables privacy. Data protection rights and obligations are specifically targeted to enabling and constraining flows of personal data.

These presentations established a broad introduction of the issues under discussion. Where Serge Gutwirth and Roger Clarke offered a reflection on the broad range of practices linked with impact assessments. Mireille Hildebrandt and Niels van Dijk focussed more on the relation between law and impact assessments. The following panel opened up the spectrum of approaches further.

Panel 2: Round Table on Normative and Empirical Perspectives on TIA

The second panel brought a large of experts on technology impact assessment together for an exchange of views. The aim of the round table was to enter into a dialogue of how lawyers, technical experts and social scientists approach the use, purpose and meaning of impact assessments in the field of data protection, privacy and mass surveillance.

Discussion questions were whether impact assessments are sufficient instruments to enforce existing law, data protection, privacy, human rights. How should impact assessments be designed and performed and is there only one way or several of doing impact assessments. How must specificities of contexts be taken into account and what does contextualization means from a normative standpoint. What are the roles of lay and expert actors, stakeholder groups, the industry, NGOs in impact assessments.

The panel opened with a reflection on the reasons for the growing popularity, since their first appearance in the area of environmentalism, of impact assessments. Charles Raab pointed to the tension between a rights-based notion of regulation and a harms-based notion of regulation. He situated impact assessments in the prevailing wind to think more about the harms-based notion of regulation. Data controllers make the impact assessment and offer it for control to the data protection authorities (DPA). This self-regulatory tendency comes down to a decentering of political control. On the question if impact assessments were a sign of crisis of the legal institutions, Paul De Hert made clear that 'Data protection is for adults'. There is an obligation to do an impact assessment but it gives no clearance. Clearance mechanisms would shift responsibility, but here no clearance is given and the uncertainty remains. A red light by the court is at the end still possible.

Sarah Spiekerman responded on the perspective of business organizations, and if impact assessments are the better alternative for companies than a legal regulation? She made clear that for companies impact assessment is a burden with which they do not like to be bothered. Companies lobby to make an impact assessment a quick exercise. From the economical perspective the question is if it pays off and in her opinion it does. A lot of checks are already done and the costs for repair in a later stage is much higher. Roger Clarke responded positively if from his practical experience there were companies which are more open to impact assessments. Namely those that which are already bitten. In his view companies are in general naïve and slow learners. He gave the example of the smart grids in the Netherlands and Australia (Victoria), where delays resulted from not assessing the risks. Companies learn the hard way. Ian Brown added that for effective impact assessments the role of stakeholders to have impact is critical. He also remarked that co-regulation leads to a flow of knowledge from the industry to the regulators. In the example of the smart grids he pointed out that the public inquiry was only done 4 years after the main decisions and the developments of the system architecture was done. Others used this Dutch experience to avoid an expensive roll-out which later meets controversy.

On the question what the role of impacts assessments could be to protect fundamental rights, Julie Cohen pointed to the difference between data protection and privacy. There is a left-over space of privacy not covered by data protection and we do not have a good idea on how to deal with this left-over. She also remarked this is not an isolated problem for PIA/DPIA. Also environmental impact assessments have similar problems, like on how to address the synergistic effects of chemicals. Sarah Spiekerman on the contrary had some doubts on there being a problem. She had mapped the elements of data protection and the conceptual analysis of privacy made by the US scholar Solove and found a strong link between both. For her the main question to answer is 'What is legitimate?'. And such assessment can be done with well-known methods. A focus group of 2 till 5 people can give a representative answer on this question, and these answers can be taken up in the assessment as threats. Brian Wynne strongly disagreed with this vision. In his view we should not look at risk assessment as a model of how things should be done. Risks assessments have their own normativity. He illustrated this with his experience with nuclear power. For nuclear safety the pressure in the nuclear reactor vessel is the key element, which can be easily quantified and modeled. But nuclear power is more than the reactor: uranium mining, transport, waste, proliferation. Where do you end the assessment? Do you limit this to the safety of the reactor or do you consider more? This is normative framing of the assessment. Therefore risk assessment is not a good model for impact assessment, as it is a one-stop event. We should of impact assessment as a process, while now operational monitoring is very weak. And we should include reflexive questions: what are we assessing?

The next issue was the role of public participation. Dariusz Kloza pointed out that the practice of environmental impact assessment rarely directly involves the public, and then it are often tickbox-exercises. He referred to a paper he wrote on what PIA can learn from environmental law. Important in environmental law is the Aarhus Convention, which contains 3 pillars: access to information, impact assessment (including the obligation for public participation) and access to justice. He made the plea to adapt this broader framework to privacy. Stefan Verschuere reflected on public participation from the viewpoint of data protection authorities. He highlighted the problematic gap between the technical reality and the law. They evaluate legal provisions in a pragmatic way and use the law as a framework. They take into account what are the 'reasonable expectations' of the data subject. Kristrun Gunnarsdottir was asked about her view of impact assessments as learning environments and what sort of knowledge we are talking about in that. She remarked that impact assessments are often formalistic exercises. Referring to the presentation by Roger Clarke, she stated that these methods work to some degree but have their limitations. The GDPR framework identifies several potential risks to assess. As limitations she saw issues as who will be required to participate, who will be capable, costs, etc. These procedures have a limited scope and the question is how we can build venues where wider issues can be explored. To close the debate Paul De Hert was asked to relate this to the role of law. He pointed to the limited role of law and of a judge. Judges can only play their role in the legal framework and give unsatisfactory, legal answers. When you want to raise wider questions, you have to ask them to who can answer them.

This round table made clear that wide differences in opinion and approach exist concerning how to do an impact assessment, as became very obvious in the discussion between Sarah Spiekerman and Brian Wynne. A large tension exist between the limits of procedures and instruments and the range of issues to raise, while on the other hand the rationale for impact assessments was made clear. Law plays an important role in this framing, but legal actors are only one of the players in the field.

Panel 3: From Theory to Practice: Integrated TIAs and their Computational Support

The third panel turned the perspective from theory to practice, and presented results of the SIAM-project. It related the earlier discussions on the wide range of approaches to impact assessments and the integration of disciplinary perspectives to reflections on this issue based on the experiences within the SIAM-project. A method for the concretization of legal requirements as an instrument to design and evaluate security technologies and measures was demonstrated. Also the participatory assessment toolkit, developed as part of the SIAM FP7 project, was presented. This was also related to some of the first findings of the integrated technology assessments developed within the EPINET FP7 project.

Leon Hempel and Hans Lammerant picked in on the earlier discussion with presenting impact assessments as political tools and by highlighting how the role and purpose given to impact assessments determined the roles of knowledge and public participation.

First they situated impact assessments as regulatory technique in the account of Ulrich Beck on the Risk Society, as an example of the decentralization of politics and an attempt to democratize the resulting sub-politics. Through this they characterized impact assessments as predominantly political tools in which knowledge is inextricably mixed with power or interests, contrary to the assumption present in a lot of PIA literature that it is possible to split off knowledge production from value discussions. They illustrated this by presenting a typology of impact assessments, developed by Cashmore, through which they showed how different assumptions on the role and purpose of impact assessments determined the role given to knowledge and to public participation. This varies from impact assessments as forms of scientific research to inform political decision making, over models where public participation has a growing role in providing information and where the active framing of the research agenda by the public in order to influence the decision making is accepted, to models where impact assessment is a tool for co-decision making and where knowledge which is relevant and useful is negotiated between the stakeholders. This perspective of negotiated knowledge was also used for the integration of different disciplines. Having one of the disciplines in a dominant role transforms the impact assessment in a legal or a scientific exercise, while the perspective of impact assessments as a political tool implies that the role of distinct disciplines is open for negotiation. This analysis was related to findings made in the empirical research, the STEFi (security, trust, efficiency, freedom infringement)-approach and the openness of the AST.

Christian Geminn presented a method for the concretization of legal requirements as an instrument to design and evaluate security technologies and measures. It is based on the KORA-method, which is not a compliance check, but a method to concretize legal requirements in several steps into technical design proposals which are legally compatible with the fundamental legal norms. The use of KORA is composed of four steps. Starting point of its use are the relevant constitutional norms, which have to be identified and selected in a preliminary stage. What follows is a step by step concretization of the fundamental legal provisions identified in the preliminary stage, at first into legal requirements, then in a second step into legal criteria, in the third step into technical objectives and finally into technical design proposals. The abstract legal requirements become more concrete with every step. Between the legal criteria and the technical objectives, there is a shift from the terminology of the law to the terminology of technology. In the SIAM-project this method has been adapted for the legal evaluation and comparison of security measure technologies. The last step consists of evaluating the security technologies with the technical objectives.

The use of this method requires an interdisciplinary discourse between legal researchers and technicians: a dialogue of disciplines. This is one of the core elements of the method to ensure that the expertise of both sides is channeled into the evaluation process.

Ronald Grau presented the SIAM assessment support tool (AST). The talk demonstrated how specially designed assessment support software can be useful to support and provide insight into the distributed work flow of activities in technology impact assessment processes.

The SIAM AST was presented as an example which illustrated the utility of such a system in the domain of mass transportation, and specifically with respect to the assessment of the impacts associated to security measures and technologies in this domain.

The software was shown to be capable of eliciting and processing information provided by different actors and stakeholders, whilst considering the related perspectives, tasks, responsibilities, and interests that exist in such a multi-user assessment. This included a spectrum of economical, organizational, technical, ethical, or societal impacts and the related questions about various topics in the context of security, efficiency, trust, or freedom infringement, for example.

Kjetil Rommetveit presented some early feedback from the EPINET-project. This project loops back in the opposite direction from practice to theory. It makes case studies of some emerging technologies (wearable sensors, social robotics, in vitro meat and smart grids) and their assessment and looks at data protection and privacy impact assessments as a cross-cutting issue. Kjetil Rommetveit gave some insights based on the smart grid case. The EPINET workshop on smart grids revealed poor understandings across national, professional and interest boundaries: little agreement exist on what the smart grid is. Some advocated abandoning the term altogether. It also revealed poor knowledge about the needs and preferences of consumers and citizens in main smart grids initiatives. The EPINET knowledge assessment revealed that the EC smart grid strategy is opaque, self-referential and defined mainly by industry and EU policy elites. The workshop on DPIA learned that most experts were positive towards DPIAs, while some argued the need to expand the scope (PIAs and surveillance impact assessments). It also showed there is conceptual confusion at work: the relationship with risks are not seriously considered; the relationship with (human) rights is not taken into account.

The smart grid template for DPIA reflects these problems. It is based on a 'rights as risk'-logic and considers risks to rights and freedoms mainly from the point of view of an organization or corporation. It extrapolates the discourse of risk management and assessment and feels 'alien' to legal thinking and practice (i.e. attempts to quantify risks to rights). The views and interests of 'the data subject' remains largely unknown (e.g. smart grids omission of 'the consumer'). A problem to be addressed by courts and human rights advocates is how to conceive rights at risk.

All this shows a need to assess the involved knowledges and world views, including fundamental rights, as well as the uncertain and ambiguous character of the technologies involved and of the scientific risk discourse. In practice, this entails continuous and reiterative assessments of the concerted ecologies of practices within which smart grids emerge and are assessed. Aim is to develop public meanings that may serve as reference points for wider segments of implicated groups. These assessments should include the voices of citizens (consumers, data subjects, publics), the different scales of technological, legal and regulatory interventions and the huge diversity among European countries regulatory and technological cultures.

Conclusions

The conference offered a broad view on impact assessments, on the underlying views and approaches and the practical difficulties and methodologies. This presented an opportunity to situate the SIAM approach and results in this broader discussion and to introduce it to the wider community of scholars and practitioners involved with impact assessments. As such this conference was not just presenting the SIAM results as a product or selling it as a business case, but it contributed to the further development of impact assessments as a practice and in involving the wider impact assessment community in it.

The presentations and discussions showed the tension between impact assessment as part of a well-defined risk management methodology and impact assessment as a political tool, including public participation into decision making processes. Also the danger of reductionist views based on one disciplinary approach was clearly put on the table and a lot of attention went into how to establish the dialogue and understanding between disciplines. These discussions enabled the SIAM-project to highlight how it had addressed these issues and the SIAM-results could be very well situated in it.

Annex 1: Abbreviations

EPINET: EPIstemic NETworks

SIAM: Security Impact Assessment Measures

STS: Science and Technology Studies

TIA: Technology Impact Assessment

PIA: Privacy Impact Assessment

DPIA: Data Protection Impact Assessment

GDPR: General Data Protection Regulation

ECtHR: European Court of Human Rights

AST: assessment support tool

KORA: Konkretisierung rechtlicher Anforderungen (German) – Concretisation of legal requirements

STEFi: security, trust, efficiency, freedom infringement

Annex 2: programme SIAM conference

10.00 - START SESSION ON IMPACT ASSESSMENTS: welcome address

organized by TUBerlin, SIAM project and EPINET project

This full day session focuses on the need for, and the practice of, Technology Impact Assessments (TIAs) with regard to novel technologies such as those used in security measures and grid applications. An increasing demand to include perspectives on the wider changes of the socio-political fabric of our societies creates a particular tension between normative and empirical approaches.

10.15 LEGAL AND STS TECHNOLOGY IMPACT ASSESSMENTS

Chair Mireille Hildebrandt, Erasmus University Rotterdam/Radboud University Nijmegen/Vrije Universiteit Brussel (NL/BE)

Moderator David Wright, Trilateral Research and Consulting (UK)

Panel Serge Gutwirth, Vrije Universiteit Brussel (BE), Niels van Dijk, Vrije Universiteit Brussel, (BE), Roger Clarke, Australian National University (AU), Mireille Hildebrandt, Erasmus University Rotterdam/University of Nijmegen/Vrije Universiteit Brussel, (NL/BE)

This panel focuses on presentation rather than discussion. It targets the question of how legal and empirical impact assessments differ and what it means to frame law and social science through the lens of an ecology of practices. Further questions addressed will be:

- What are the gains and the risks of technology impact assessments in the broad sense?
- What is the difference between a PIA and a DPIA and should we applaud the legal obligation to do a DPIA?
- How can we assess the impact on a right, as compared to the impact on the substance of a right?
- Do technologies have normative impact, and what does this mean for courts and legislators?

11.45 - ROUND TABLE ON NORMATIVE AND EMPIRICAL PERSPECTIVES ON TIA

Chair Mireille Hildebrandt, Erasmus University Rotterdam/Radboud University Nijmegen/Vrije Universiteit Brussel (NL/BE)

Moderator Leon Hempel, Technische Universität Berlin (DE)

Panel Ian Brown, Oxford Internet Institute (UK), Julie Cohen, Georgetown University (US), Roger

Clarke, Australian National University (AU), Paul de Hert, Vrije Universiteit Brussel/Tilburg University (BE/NL), Kristrun Gunnarsdottir, Lancaster University (UK), Dariusz Kloza, Vrije Universiteit Brussel (BE), Charles Raab, University of Edinburgh (UK), Sarah Spiekerman, Vienna University of Economics and Business (AT), Stefan Verschuere, Belgian Privacy Commission (BE), Brian Wynne, Lancaster University (UK)

This panel aims to focus on discussion rather than presentation; the questions raised here shall have an "explorative" character rather than pursuing a well-established academic debate. The panel will confront the issues of legal and technological normativity, participatory social research and ethical standards. The question to be addressed is:

- How can TIA approaches on the legal, technical as well as on the socio-organisational level go hand in hand to address common regulative paradoxes between legal norms and socio-technical practices?

13.00 - Lunch break

14.00 - From theory to Practice: Integrated TIAs and their Computational Support

Chair Mireille Hildebrandt, Erasmus University Rotterdam/University of Nijmegen/Vrije Universiteit Brussel (NL/BE)

Moderator Rasmus Nielsen, Danish Board of Technology (DK)

Panel Leon Hempel/ Hans Lammerant, Technische Universität Berlin/Vrije Universiteit Brussel (DE/BE), Christian Geminn, Universität Kassel (DE), Ronald Grau/ Graeme Jones, Kingston University London (UK), Kjetil Rommetveit, University of Bergen (NO)

This session will turn the perspective from theory to practice. We will demonstrate a method for the concretization of legal requirements as an instrument to design and evaluate security technologies and measures. The focus is on a participatory assessment toolkit developed within the SIAM FP7 project, which will be related to some of the first findings of the integrated technology assessments developed within the EPINET FP7 project.

- This session will engage with the issues discussed during the previous sessions and show how assessment criteria can be interfaced with an ICT Assessment System, and how legal conditions can be interfaced with engineering requirements.

- Finally, the attempt to provide computational support will be discussed from the perspective of an integrated TIA to detect added value, missing links and to other issues of future research.