CHAPTER 2
Responsible research and innovation in ICT: The case of privacy

Walter Peissl

Introduction

The broad use of information and communication technologies (ICTs) in almost every part of daily life produces a huge amount of data. Personal data of the user or of people involved constitute a major part of the data stored and processed. They reveal a lot about the users' behaviour and help creating a picture of people's personal lifestyles. Data stem from economic enterprises as well as from state surveillance systems, and together they manifest a threat to privacy. These new threats can no longer be dealt with by legal means alone; rather, interdisciplinarity is the key word. Since the erosion of privacy is a fundamental problem for liberal democracies, we need combined efforts and a common understanding of the value of privacy among engineers, political and social scientists and decision-makers in private enterprises as well as in the public domain. To take these considerations into account is to be considered part and parcel of responsible research and innovation; therefore, we have to develop new ways to secure privacy in a networked world.

This bookcontribution will present new approaches to incorporate privacy-oriented thinking and PETs[1] principles early into the design-process. The starting point is the idea that even in data protection it is cheaper to decide on the fundamental design earlier in the process rather than applying end-of-pipe solutions to ensure that a product or service complies with legal requirements or to gain acceptance on the market. These approaches will be discussed along with the results from two recent research projects ITA was involved in: PRISE[2] und EuroPriSe[3].

TA and Privacy

According to von Schomberg (in this book), technology assessment is a relevant method in the product dimension of Responsible Research and Innovation (RRI). Presenting two recent research projects of the Institute of Technology Assessment (ITA) of the Austrian Academy of Sciences, this paper shows how technology assessment can feed into RRI processes. Before going into detail I will give a short overview over the Institute and TA in general.

The Institute of Technology Assessment of the Austrian Academy of Sciences (ITA) is an interdisciplinary research institution that investigates the relationship of technology and society and especially is interested in the impacts on society of the widespread use of new technology. The institute's work is devoted to academic analysis as well as to policy advice in technology-related issues. One of the main areas of work is to analyse the impacts of new ICT applications on society. Important areas of work are privacy, e-governance and networked environments. Apart from the focus on the information society, ITA deals with technology and sustainability as well as with the governance of controversial technologies such as biotechnology, nanotechnology and new emerging technologies for human enhancement.

Technology assessment is an interdisciplinary concept, which provides policy advice for technology and research policy. The potential impacts of technology use are analysed in

1 Privacy Enhancing Technologies (PETs)

2 http://prise.oeaw.ac.at

3 https://www.european-privacy-seal.eu/

several dimensions and, if possible, alternatives are described. Technology assessment is always pro-active and constructive in contributing solutions to societal problems. Technology assessment was first established in the USA as an independent and impartial instrument of policy advice for the Senate in the early 70s of the 20th century. Today in Europe, 18 TA institutions work for their respective regional or national parliaments. These parliamentary technology assessment institutions are organised within EPTA[4]. On the European level, the STOA Panel[5] serves the European Parliament. The STOA secretariat is supported by members of the European Technology Assessment Group (ETAG)[6].

In TA we distinguish between different basic approaches: a) technology induced studies analyse potential impacts of the broad implementation of certain technologies and their potential alternatives; b) problem induced approaches focus on societal problems and search for technological or organisational solutions for the problems found; c) project oriented approaches focus on impacts of concrete projects like energy-plants.

With regard to privacy we use a problem-oriented approach based on empirical evidence for the erosion of the fundamental right to privacy due to the widespread use of ICT facilitates (vgl. Tichy/Peissl 2001; Klüver 2006; Peissl 2007; Sterbik-Lamina et al. 2009). Studies in this domain try to find technological, organisational or legal measures to halt the ongoing erosion of privacy. In addition, we investigate how technological and societal developments as described later may change our attitudes towards privacy.

Technological and societal developments

Over the last decades, three lines of development characterised the technological progress in the domain of ICT. Rendering everything digital resulted in a qualitative change, making many applications possible and revolutionising others. The digitisation of analogue communication systems enabled and accelerated the convergence of information- and communication systems. At the same time, privacy became an important issue. The technological development necessitated the implementation of further measures in order to keep up with legal requirements. For instance in old analogue telephone systems, the connection data disappeared with the end of the communication process. In digital systems, you have to save the addresses of all communication partners as a technical requirement. To comply with data protection rules, you have to design the system to include additional automatic erasure routines.

The second important line of development was *minimisation*. The computing power of 1970s' big machines is nowadays contained in tiny PDAs and smartphones. This is, of course, not the end of minimisation. Thinking of RFID tags[7] and the concept of the Internet of things (Commission of the European Communities 2009; ITU 2005) we see an ongoing development towards smaller or even irrecognisable devices. Minimisation, at the same

4 http://www.eptanetwork.org/EPTA/

5 http://www.europarl.europa.eu/stoa/default_en.htm

6 http://www.itas.fzk.de/etag

7 RFID: Radio Frequency IDentification

time, paved the way for decentralised computational power. Some of the early data protection laws in Europe (e. g. in Austria) are more or less based on the idea of securing data in a centrally locked computer centre. This is why modern data protection laws have to focus much more on the so-called informational self-determination. A centralistic concept of "data protection" no longer matches the conditions of modern decentralised data processing.

This development is accelerated by the third big technological line of development: *networking*. Establishing the universal Internet protocol (IP) actually enabled every user to be connected and to exchange data all over the world within seconds. This raised new challenges to data protection in a globalised world.

Summing up we may say that digitisation, minimisation and networking built a totally new framework for privacy policy.

However, not only technological developments contribute to the erosion of privacy. There are at least two other ambivalent developments in society. On the one hand we can see a higher sensibility for data protection issues, which basically popped up in public debate after huge data losses occurred in several European countries. On the other hand, we face a new trend in communication. In web 2.0 applications or so-called social media platforms millions of users share information rather unscrupulously even on a very private level. Social scientists increasingly become interested in the long-term impacts of such a behaviour (see Sterbik-Lamina et al. 2009; Klüver 2006).

Developments after the terrorist attacks in New York, London and Madrid were even more important. Globally, we recognised a hype of surveillance demands to prevent future terrorist attacks – surveillance mostly served as a synonym for security. As an over-reaction, this entailed new regulation that endangered privacy (see Peissl 2005). Recent studies demonstrated that security and privacy are not necessarily a zero sum game (Raguse et al. 2008).

This short overview on technological and societal developments shows how endangered the fundamental right of privacy is. Are there any ways to cope? Since in the future, technology design will play a more important role, the "Privacy by Design" approach by Cavoukian (2009) as well as the results of the PRISE project[8] can be considered important steps. In addition, it will be necessary to promote research and development and, in particular, to implement so-called Privacy Enhanhcing Technologies (PETs) (Klüver 2006).

The technological and societal developments, of course, need to be mirrored in a modern data protection directive, which is under discussion right now.

Hypotheses and solutions

In order to structure the discussion of possible ways to overcome the challenges to privacy, we present three hypotheses as starting points:

8 http://prise.oeaw.ac.at

Hypothesis 1: Privacy is a fundamental right. Today, it is jeopardised in various ways and can no longer be enforced by legal means alone. Reasons are the very low level of users' awareness of ICT and the lacking resources of data protection authorities (Cas/Peissl 2000; Cas et al. 2002; Klüver 2006; Sterbik-Lamina et al. 2009).

Hypothesis 2: Privacy increasingly is on the political agenda. Indicators may be found, on the one hand, in the media coverage of data-loss scandals around Europe, the low level of acceptance of the data-retention directive and the protests against its implementation in several European countries. On the other hand, the European Commission continues to issue calls for data protection research and to finance pilot projects like the EuroPriSe project. On a global level, there are developments to establish a kind of data-protection standard (Bennett/Raab 2003).

Hypothesis 3: Privacy often is seen as a cost factor only. The main line of argument is that data protection systems cost money and cannot be afforded in a globally competitive market.

It may be true that the adaptations needed to make an IT system comply with data protection regulation or to gain acceptance on the market are rather costly. However, in contrast to this end-of-pipe approach, we argue that the "privacy by design" approach is more cost-efficient. Early implementing privacy-oriented thinking in the design process does not cost much and "built-in-privacy" is an added quality feature of the respective IT product. As success in global markets is no longer solely dependent on competitive pricing, "privacy" as a new quality feature is a comparative advantage for those who include it at an early stage. The success of the data protection seals in Schleswig-Holstein[9] and the European Privacy Seal may serve as an indication how successful this kind of thinking already is[10].

Summing up, privacy should be seen as a quality feature of IT products and services; and privacy can no longer be guaranteed by legal means alone. Therefore, pro-active and constructive approaches are necessary. Two such approaches will be presented in the following chapters: first, the "engineer-oriented" approach takes up standards and guidelines from IT security and enhances them by catering for the privacy dimension. The aim is to incorporate privacy know-how as early as possible into the design process. Secondly, the "market-oriented" approach stands for self-regulation, audit schemes and quality seals.

The PRISE Approach

The PRISE project aimed at defining criteria for privacy-friendly security technology research funded by the EC in the framework of PASR[11]. The PRISE approach shows how privacy can be designed into security technologies, and how privacy considerations can be operationalised within the research and development process and the deployment phase of a security product.

9 https://www.datenschutzzentrum.de

10 https://www.european-privacy-seal.eu

11 Preparatory Action on Security Research

By applying this evaluation procedure produced for Framework Programme 7, certain generalizations can be made. The method selected was a combination of classic expert Technology Assessments featuring the analysis of literature and documents, together with participative approaches.

The participative approaches had two components: on the one hand, two stakeholder workshops were held with representatives of industry, science, and users of security technologies to discuss the research design and provisional results. The other component comprised so-called "Interview meetings"[12] carried out in six European countries[13]. The main purpose was to stimulate an "informed debate" on the subject with approximately 160 participants and to discover their basic views, in particular lines of argument, and to determine how these might be changed. During the preparation the participants were introduced to several scenarios on the subject. After an introductory talk, the participants were asked to fill in a comprehensive questionnaire. Using a list of questions, the subject was subsequently discussed in small groups.

The results showed a high level of consensus among the non-specialist groups in all countries. Among the key statements made, for example, was that a threat from terrorism does not justify an infringement of privacy, that technologies invading the very private (intimate) sphere are unacceptable, and that the abuse of security technologies ought to be prevented. Of special relevance – as a distinguishing feature between countries – was the degree of trust people had in various institutions. The independent judiciary, in particular, enjoys a high degree of public confidence, which was also reflected in the list of values participants considered to improve acceptance of security technologies. Top of the list was the principle of proportionality, which would only appear to be assured if certain supervisory measures were legally permitted subject to strict checks. The fear of possible abuse was indicated by the demand for strict controls, and by the emphasis people placed on security technologies infringing privacy being implemented as a last resort only. More generally, an informative and open debate on the subject was called for, which should involve as many concerned groups as possible, as well as an obligatory analysis of the implementation effects of such technologies (see Jacobi/Holst 2008).

The key result of PRISE is the so-called PRISE matrix. It is an evaluation instrument for measuring the expected effects of a new security technology in three stages. The three stages investigated are the so-called *baseline of personal life*, which comprises very personal – intimate – data and which, as a matter of principle, should be free from any surveillance. The second area is about *data protection compliance*, i.e. how already existing principles are applied, and the third area deals with *context-sensitive trade-offs*. The latter area examines whether a security technology apparently infringing privacy justifiably promises a sufficient security gain.

There are several evaluation stages in the course of designing a system or evaluating a project. If the initial evaluation of the project idea renders the conclusion that the first or second area is not catered for satisfactorily, there is a package of measures contributing to alleviating a recognised privacy problem, as summarised in the so-called PRISE

12 A short description of interview meetings can be found on the website of the Danish Board of Technology: http://www.tekno.dk/subpage.php3?article=1234&toppic=kategori12&language=uk

13 Denmark, Norway, Germany, Spain, Hungary and Austria

Handbook. Three types of instruments are available – legal, technical and organisational –, which are also described in the report (Raguse et al. 2008).

Using the matrix together with two checklists, which enable a quick evaluation to be made, an attempt was made to develop guidelines and support for product proposing enterprises, for evaluators, and for research and development teams in general. The PRISE matrix and the PRISE Handbook can, however, also provide users of security technologies with valuable information on an ICT use that complies with basic law and enhances privacy.

Taken together, it was possible to show that security and privacy do not necessarily exclude each other and that it is possible to endorse both at the same time, provided design principles are appropriately complied with..

The PRISE results were presented at an international conference, where representatives of the security technology industry, users, NGOs and representatives from the scientific community discussed them. The conference concluded with the presentation of a Statement Paper[14], summarising the project team's and its international advisory committee's main results in terms of recommendations for action and policy options.

The Statement Paper contains the following conclusions and recommendations: i) An inviolable *baseline of privacy* needs to be established. ii) There is no linear, interchangeable relationship between privacy and security, and the relationship between them is *not a zero-sum game*. iii) Minimising the processing of personal data is an important principle of data protection. iv) *The consolidation of databases* in order to analyse the behaviour of the entire population breaches the principle of the presumption of innocence and the principle of proportionality. v) The protection of privacy is the shared responsibility of all involved, and observance of *privacy should be a key non-functional requirement* of security technologies. vi) In addition, the *criteria* for evaluating security technologies must be *continuously developed* and regulations should be introduced for a limited time and continuously reassessed (see as 2008).

The European Privacy Seal

After the description of the "engineer-oriented" approach we now present a brief description of the "market-oriented" approach, based on the example of the EuroPriSe project[15], which focuses on conditions for introducing a European Privacy Seal. Such a privacy quality seal is intended to certify "that an IT product or IT based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the pilot countries." (Bock 2009)

The project had several aims. Firstly, it was concerned with a market analysis, which was intended to assess the extent to which a European privacy seal might be viable on its own without subsidies from certification fees, and whether it would be able to succeed in the market. The second aim was to promote awareness of data protection issues

14 http://prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf

15 https://www.european-privacy-seal.eu

among manufacturers. The most challenging theoretical task was to develop criteria for evaluating data protection friendliness at a European level. EU Directive 95/46 already provides a standard framework for data protection legislation, but member states vary widely in interpreting it. The project succeeded in establishing a common set of criteria based on the European framework (Bock et al. 2009). It also undertook to collect existing experience regarding the European certification of products and services and European admission criteria for the relevant experts.

The specific aims of the seal are to promote data protection per se, to improve consumer trust in IT products and services, to contribute to greater transparency in data processing and to demonstrate theoretically and empirically a possible competitive advantage for products complying with data protection, carried out using the ROSI model – Return on Security Investment (Borking 2009). In addition, EuroPriSe aimed to simplify the certification procedure for businesses interested in data protection, since a certification recognised throughout Europe would abolish multiple certification requirements, rendering immediate effects.

The certification procedure is largely based on the privacy seal the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP/ULD) established in 2002. The procedure comprises two stages, which are voluntary in principle but regulated by law. In each case the manufacturer or vendor of a product and/or service to be certified selects a legal and a technical expert from a register of accredited experts. Together they agree the "Target of Evaluation" (ToE). At this stage, initial contact is made with the certification body to clarify the ToE. Subsequently, the two experts begin their independent evaluation of the product or service. Once the evaluation has been concluded the manufacturer submits the report to the certifying body, which carries out its own examination of the report. If the result of the examination is positive, the seal is awarded and a short report is published on the Seal Homepage. It is important that the entire procedure remains confidential, that no business secrets are contained in the published short report, and that any negative examination results are not made public.

The only costs incurred by the business enterprise are the fees for the two experts and the fee charged by the certifying body.

A key factor in this process is the criteria used in certification. The fundamental question is: can the product or service be designed so that its use will comply with data protection? This refers in particular to settings, configurations and also to the pertaining documentation. The European Privacy Seal particularly emphasises the combination of law and technology. The certification criteria have been worked out in great detail and are also published in a comprehensive catalogue (Bock et al. 2009). They basically follow the standard principles of data protection such as the legitimacy of data processing, purpose limitation, data subjects' rights, transparency and auditability, data minimisation and avoidance, as well as data security.

Ever since it was launched the project proved surprisingly popular with experts as well as with manufacturers. No fewer than 110 experts from ten countries attended the training seminars to be trained, examined and accredited. Austria currently has twelve experts. A total of 19 pilot certification processes had been initiated, which in the meantime have resulted in the award of 15 seals.

Conclusion

The starting point for this article was the question of how to manage responsible research and innovation with regard to ICT development and privacy. Based on the evidence that privacy protection can no longer be assured by legal means, attempts have been made to find alternative solutions. These have shown that (new) instruments for ensuring privacy protection do already exist. On the one hand, design-oriented assistance supports early compliance with data protection aspects in the design phase, involving only minimal additional costs. Fitting an IT system with PETs can qualify as a quality feature providing the product a competitive advantage, which is reflected in a positive Return-on-Investment (ROI). On the other hand, market-oriented mechanisms of self-regulation such as the Quality Seal can contribute to greater transparency on the market.

Particular responsibility falls to the policy-makers and those areas of public procurement that purchase large IT systems or are responsible for providing widely used IT applications. There is a particular potential in so-called "sensitive" areas such as, for example, security applications in the fight against crime, in e-government and, above all, in e-health.

Finally, the arguments and results discussed above are summarised in four messages:

1) Security and privacy do not not necessarily exclude each other; security technologies can often be designed in such a way that they fulfil their function and enhance security without, at the same time, infringing the fundamental right of privacy.
2) The debate about data protection and privacy thus far has been concerned with legalities almost exclusively. It now needs to be widened to include technical and social scientific aspects. This broader perspective has become necessary because of both, technological developments and changes in society. It would therefore appear helpful if, in future, we were to speak about privacy protection rather than "just" data protection.
3) The well trained and powerful statutory regulations in Europe are needed as a "support", but it would be insufficient to rely on them exclusively. We need to remember that statutory regulation only makes sense if it can be enforced. This means that data protection authorities need to be equipped with the technology and the legal resources required being able to adequately meet new challenges.
4) Additional instruments and incentives need to be used. These include the promotion of the "privacy by design" approach and the use of the PRISE matrix tools, of Privacy Impact Assessments (PIA) etc. This represents a key task for public procurement and funding agencies. Also, from today's perspective it is clear that there is a great potential for the implementation of self-regulation instruments such as, for example, data protection audits and quality seals. An additional and still too little funded public task is raising relevant awareness – including a debate of privacy issues and of the inalienable right to privacy at an early stage in schools –, which will play an important part in future privacy protection activities.

With a package of measures, an interdisciplinary approach and the appropriate political will at European as well as nation state level, it should be possible, in the future, to preserve the fundamental right of privacy so important for our democracies.

References

Bennett, C. J. und Raab, C. D., 2003, *The Governance of Privacy*, Aldershot, Hampshire GB: Ashgate.

Bock, K., 2009, *European privacy Seal – Final report*, im Auftrag von: European Commission – eTEN, Kiel: Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD, Independent Centre of Privacy Protection) <https://www.european-privacy-seal.eu/results/deliverables/Final%20Report>.

Bock, K., Meissner, S. und Storf, K., 2009, *Description of EuroPriSe Criteria and Procedures (updated Version 1.1)*, im Auftrag von: European Commission – eTEN, Kiel: Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD, Independent Centre of Privacy Protection) <https://www.european-privacy-seal.eu/results/deliverables/procedures>.

Borking, J. J., 2009, *The Business Case for PET and the EuroPrise Seal*: unveröff. Manuskript.

Čas, J., 2008, Privatsphäre und Sicherheit Ergebnisse aus dem europäischen TA-Projekt PRISE, *TECHNIKFOLGENABSCHÄTZUNG – Theorie und Praxis 17(3)*, 79-82 <http://www.itas.fzk.de/tatup/083/jcas08a.pdf>.

Čas, J. und Peissl, W. (Institut für Technikfolgen-Abschätzung und Österreichische Akademie der Wissenschaften), 2000, *Beeinträchtigung der Privatsphäre in Österreich – Datensammlungen über ÖsterreicherInnnen*, im Auftrag von: Bundeskammer für Arbeiter und Angestellte, Oktober 2000, Wien: Institut für Technikfolgen-Abschätzung, <http://www.oeaw.ac.at/ita/ebene5/d2-2a24a.pdf>.

Čas, J., Peissl, W. und Strohmaier, T., 2002, *Datenvermeidung in der Praxis – Individuelle und gesellschaftliche Verantwortung*, im Auftrag von: Bundeskammer für Arbeiter und Angestellte, Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften <http://www.oeaw.ac.at/ita/ebene5/d2-2a29.pdf>.

Cavoukian, A., 2009, *Privacy by Design ....take the challenge*, Toronto: Information and Privacy Commisioner of Ontario, Canada <http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook.pdf>.

Commission of the European Communities, 2009, *COM(2009) 278 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Internet of Things — An action plan for Europe*; Letzte Aktualisierung: Brussels, 18.6.2009 [Aufgerufen am: 2009-09-07 2009] Commission of the Euroepan Communities, <http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf>.

ITU, 2005, *IITU Internet Reports 2005: The Internet of Things - Executive Summary*; [Aufgerufen am: 2009-09-07 2009] International Telecommunications Union (ITU) <www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf>.

Jacobi, A. und Holst, M., 2008, *PRISE D5.8 Synthesis Report - Interview Meetings on Security Technology and Privacy*, im Auftrag von: European Commission PASR, Vienna: Institute of Technology Assessment Austrian Academy of Sciences, <http://prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf>.

Klüver, L., Peissl, W., Tennøe, T., Bütschi, D., Cas, J., Deboelpaep, R., Hafskjold, Ch., Leisner, I., Nath, Ch., J., Steyaert, St., Vouilloz, N.„ 2006, *ICT and Privacy in Europe – A report on different aspects of privacy based on studies made by EPTA members in 7 European countries*, 16 October 2006: EPTA <http://epub.oeaw.ac.at/ita/ita-projektberichte/e2-2a44.pdf>.

Peissl, W., 2005, Überwachung und Sicherheit – eine fragwürdige Beziehung, in: Nentwich, M. und Peissl, W. (Hg.): *Technikfolgenabschätzung in der österreichischen Praxis Festschrift für Gunther Tichy*, Wien: Verlag der Österreichischen Akademie der Wissenschaften, 73-90.

Peissl, W., 2007, Die Bedrohung von Privacy – ein grenzüberschreitendes Phänomen und seine Behandlung im Kontext internationaler Technikfolgenabschätzung, in: Bora, A., Bröchler, S. und Decker, M. (Hg.): *Technology Assessment in der Weltgesellschaft*, Berlin: Edition Sigma, 277-288.

Raguse, M., Meints, M., Langfeldt, O. und Walter Peissl, 2008, *D6.2 – Criteria for privacy enhancing security technologies, Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies* im Auftrag von: European Commission PASR, Vienna: Institute of Technology Assessment Austrian Academy of Sciences, <http://prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf>.

Sterbik-Lamina, J., Peissl, W. und Čas, J., 2009, *Privatsphäre 2.0 (Beeinträchtigung der Privatsphäre in Österreich; Neue Herausforderungen für den Datenschutz),*, im Auftrag von: Bundesarbeitskammer, Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften <http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf>.

Tichy, G. und Peissl, W., 2001, Beeinträchtigung der Privatsphäre in der Informationsgesellschaft, in: Österreichische Juristenkommisssion (ÖJK) (Hg.): *Grundrechte in der Informationsgesellschaft – 24.-26. Mai Weißenbach am Attersee*, Wien: Neuer wissenschaftlicher Verlag, 22-48 <http://www.oeaw.ac.at/ita/ebene5/GTWPweissenbach.pdf>.