> Internet Privacy

Taking opportunities, assessing risks, building trust

acatech (Ed.)

acatech POSITION PAPER

May 2013

acatech
NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

Published by:
acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING, 2013

Munich Office
Residenz München
Hofgartenstraße 2
80539 Munich

T +49 (0) 89 / 5 20 30 90
F +49 (0) 89 / 5 20 30 99

Berlin Office
Unter den Linden 14
10117 Berlin

T +49 (0) 30 / 2 06 30 96 10
F +49 (0) 30 / 2 06 30 96 11

Brussels Office
Rue du Commerce / Handelsstraat 31
1000 Brüssel

T +32 (0) 2 / 5 04 60 60
F +32 (0) 2 / 5 04 60 69

E-Mail: info@acatech.de
Internet: www.acatech.de

Recommended citation:

acatech (Ed.): *Internet Privacy. Taking opportunities, assessing risks, building trust* (acatech POSITION PAPER), Munich 2013.

Coordination: Dr. Karin-Irene Eiermann
Edited by: Dunja Reulein, Linda Treugut
Translation: Joaquin Blasco
Layout concept: acatech
Conversion and typesetting: Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, Sankt Augustin

> THE acatech POSITION PAPER SERIES

This series comprises position papers from the National Academy of Science and Engineering, providing expert evaluations and future-oriented advice on technology policy. The position papers contain concrete recommendations for action and are intended for decision-makers from the worlds of politics, science and industry as well as interested members of the public. The position papers are written by acatech members and other experts and are authorised and published by the acatech Executive Board.

CONTENTS

SUMMARY

Few technologies have changed our lives as rapidly and profoundly as the Internet. There are now more than 1.5 billion Web users around the world, with at least 50 million in Germany. Internet users enjoy easy access to information and are able to shop online and communicate with each other via free video calls. The Internet is spawning new business models, creating new jobs and transforming business processes both within and between companies and public administrations. It also provides the infrastructure for the smart power grids that will be needed to realise the transition to sustainable energy. Cyber-Physical Systems controlled via the Web will facilitate efficient use of manufacturing resources and energy in the factories of the future.

The Internet also has an especially important function in democratic societies, since it facilitates free self-determination, democratic participation and economic well-being. Information and educational content help people to decide for themselves how they wish to live their lives. People who share the same political beliefs can connect with each other through interest groups. Prominent examples include the online petition against data retention and the pro-democracy movements in the Arab world. In recent years, many new jobs have been created thanks to the Internet, while businesses can use it to improve their chances of success by showcasing their products and services to an international audience.

People have grown accustomed to not having to pay for online services. However, these services are not actually free – the currency with which users pay for them is their personal data. In addition to the information that they knowingly provide to the services (e.g. their name, address, etc.), they also leave other traces behind, such as the web sites they visit or what they write in their messages. Virtually every single company that provides free services on the Internet requires users to supply data which they then use to make money, for example through targeted advertising. Personal information is thus a commodity and a currency. This breeds suspicion – many Internet users are sceptical about whether service providers handle their personal data on the Internet with due care and question whether their privacy is always properly protected.

Privacy means that a person has the ability to define and control how much they reveal or hide about themselves and when and to whom they do so. They may wish to hide everything, as in the case of anonymous communication. Equally, they may only wish to hide certain information about themselves, such as their age, gender or address. On the Internet, this privacy is often limited. One risk is *decontextualisation*, where personal data are used in contexts that their owners would not agree to if they knew about it. Another risk is persistence, where data are held for longer than necessary or merely anonymised instead of being deleted. The third way that privacy is curtailed is through *re-identification*, where advanced analysis techniques are used to reassign anonymous records to individuals. People often don't know which of their personal data are known to online services, which rules are used to process them and to whom they are passed on. Although service providers do often include this information in their general terms and conditions, for example, it is not always easily accessible and can be hard to understand.

Netiquette, the Internet's international "moral code", is still not well-developed enough to ensure that Web users can always be confident of each other's trustworthiness. It is possible for users to publish another person's personal data in photo tags, for example. Meanwhile, privacy protection regulation is inconsistent and in some cases ill-equipped to address current challenges. Moreover, there are no widely accepted codes of conduct. Finally, the technical implementation of the relevant regulations is inadequate – data encryption, for example, can slow services down significantly.

If people's privacy is curtailed in these ways, they are no longer in a position to optimally exercise their right to free self-determination, democratic participation and economic wellbeing. If extensive details of someone's personal data and information are known to others, they can no longer freely choose how they go about their lives or how they participate politically. Privacy is essential if these values are to be upheld. Nevertheless, their relationship with privacy is an ambivalent one. This is because online services can actually still support these values, even if they offer little or no privacy. This is the case, for example, when they provide a platform for political debate or sources of information that would otherwise not be available to people. Consequently, it is necessary to implement privacy in an reasonable manner that does not place excessive constraints on the opportunities offered by the Internet.

Three conditions need to be met in order to implement reasonable privacy on the Internet: user competence, freedom of choice and trustworthiness. This can be achieved through a culture of privacy that encompasses education, regulation, business and technology. Education ensures that people know their rights and the opportunities and risks associated with the Internet. This allows them to determine their online privacy preferences and configure them accordingly. Regulation establishes binding rules. To ensure that they can be complied with, these rules need to be technically feasible. The rules are aimed at businesses, public authorities, users, etc. The different actors are able to gain each other's trust by complying with statutory regulations and other rules designed to enable reasonable privacy.

In 2010, the German Parliament set up a Study Commission on the "Internet and Digital Society" to investigate the opportunities and risks associated with the Internet. This topic is also being addressed by the data protection authorities and regional parliaments. The new draft Data Protection Regulation published by the European Commission in 2012 seeks to extend the scope of data protection legislation beyond the boundaries of the EU, thus addressing the transnational dimension of this issue.

In the context of this debate, acatech has formulated the following **recommendations**:

EDUCATION

- Equip everyone with Internet competence
- Ensure that Internet competence forms an integral part of (pre-)school education
- Ensure that privacy protection forms an integral part of professional training and continuing professional development
- Run public information campaigns on privacy protection
- Strengthen research into people's opinions and practices with regard to privacy

REGULATION

- Leave technical implementation up to the service providers
- Apply privacy protection law that users are familiar with
- Regulate how consent is provided
- Create transparency and enable control
- Enable deletion of data
- Support migration
- Comply with data protection principles
- Regulate privacy protection certification
- Investigate incentives to encourage self-regulation

BUSINESS

- Offer more privacy protection options
- Enable use of privacy agents
- Harmonise standards
- Develop privacy seals and certificates

TECHNOLOGY

- Apply the "Privacy by Design" principle to the development and operation of online services
- Support informed and considered consent
- Research the right to be forgotten on the Internet
- Ensure user-friendliness
- Support user competence and freedom of choice
- Support trustworthy auditing
- Investigate data mining processes for big data privacy
- Enable anonymous and pseudonymous use of services
- Continue to develop basic methods and technologies

PROJECT

This position paper was developed on the basis of the acatech STUDIES *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis* (Buchmann 2012) and *Internet Privacy – Options for adequate realisation* (Buchmann 2013).

> PROJECT MANAGEMENT

Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/CASED/acatech

> PROJECT GROUP

- Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/CASED/acatech
- Prof. em. Dr. Rafael Capurro, formerly of Stuttgart Media University (HdM)
- Prof. Dr. Martina Löw, Technische Universität Darmstadt
- Prof. Dr. Dr. h.c. Günter Müller, University of Freiburg
- Prof. Dr. Alexander Pretschner, Technische Universität München
- Prof. Dr. Alexander Roßnagel, University of Kassel
- Prof. Dr. Michael Waidner, Technische Universität Darmstadt/Fraunhofer SIT/CASED
- Dr. Wieland Holfelder, Google Germany
- Dr. Göttrik Wewer, Deutsche Post DHL
- Michael Bültmann, Nokia GmbH
- Dirk Wittkopp, IBM Deutschland

> REVIEWERS

- Prof. Dr. Otthein Herzog, Universität Bremen/acatech (chair of the review panel)
- Prof. Dr.-Ing. Dr. h. c. mult. Dr. e. h. José Luis L. Encarnação, Technische Universität Darmstadt/acatech
- Prof. Dr. Roland Gabriel, Lehrstuhl für Wirtschaftsinformatik, Ruhr-Universität Bochum
- Prof. Dr. habil. Claudia Eckert, TU München/Fraunhofer AISEC/acatech

acatech would like to thank all external experts. acatech is solely responsible for the content of this position paper.

> ASSIGNMENTS/STAFF

- Dr. Karin-Irene Eiermann, acatech Office
- Martin Peters, University of Freiburg
- Thomas Heimann, Google Germany
- Carsten Ochs, Technische Universität Darmstadt
- Fatemeh Shirazi, Technische Universität Darmstadt
- Hervais Simo, Technische Universität Darmstadt
- Florian Kelbert, Technische Universität München
- Maxi Nebel, University of Kassel
- Dr. Philipp Richter, University of Kassel
- Daniel Nagel, independent consultant, Stuttgart
- Dr. Michael Eldred, independent consultant, Cologne

> PROJECT COORDINATION

Dr. Karin-Irene Eiermann, acatech Office

> PROJECT PROCESS

Project term: 07/2011 – 06/2013

This acatech POSITION PAPER was syndicated by the acatech Executive Board in March 2013.

> FUNDING

This project was funded by the Federal Ministry of Education and Research (BMBF) (Funding reference: 01.08.2011 – 30.09.2012: 01BY1175, 01.10.2012 – 31.01.2013: 16BY1175).

SPONSORED BY THE

Project Administrators:

01.08.2011 – 30.09.2012: German Aerospace Center's Project Management Agency (PT-DLR), Communication Technologies

01.10.2012 – 31.01.2013: VDI/VDE Innovation + Technik

acatech would also like to thank the following companies for their support:

Google Germany, Deutsche Post AG, Nokia, IBM Deutschland

1 INTRODUCTION

Few technologies have changed the way we live, work and interact as rapidly, dramatically, lastingly and profoundly as the Internet. There are now more than 1.5 billion Internet users around the world, with at least 50 million in Germany. The Internet enables easy access to information and to services such as booking flights, online shopping and communication by e-mail or free video calls. The Internet is demonstrating its innovative potential by spawning new business models and creating new jobs, thus making a huge contribution to value creation across the entire economy. It is fundamentally transforming business processes within and between both companies and public administrations. The Internet also provides the infrastructure for the smart power grids that connect and manage power producers, power storage facilities and energy consumers and will be key to realising the transition to sustainable energy. Moreover, it provides the basis for smart traffic management systems that will make road transport safer and more efficient. Cyber-Physical Systems controlled via the Internet will facilitate efficient use of manufacturing resources and energy in the factories of the future. As this position paper will show, in addition to these benefits for individuals and the economy, the Web also enables participation in social and political movements and contributes to overall social progress and the development of basic values.

It is a feature of Internet culture that many services are "free". Users have grown accustomed to not paying for search engines, encyclopaedias, films, images, music, news, magazines, social networks, message boards, blogs and many other services – indeed, this is something they have come to expect. In actual fact, however, there are various costs associated with providing these services – they require hardware and software, ideas, energy, capital and labour, all of which have to be paid for. The currency with which users pay for these services isn't the dollar or the euro, it is their *personal data*, i.e. login details, search queries, photos, text messages, purchases, addresses, friends and acquaintances, etc. Virtually every single company that provides free services on the Internet requires users to supply this type of data which they then use to make money, for example through targeted advertising. Personal data are thus a commodity and a currency.

Although the Internet is extremely useful for many people, the fact that they have to provide such a large amount of personal information can raise doubts that may eventually grow into suspicion. Even *digital natives* who have grown up with the Internet and feel much safer in the online environment than older generations are often worried that they may be being monitored and identified by other users. *Digital immigrants* who only became familiar with the Internet later in life are often sceptical about whether service providers handle their personal data with due care. Meanwhile, *digital outsiders* who have yet to start using the Internet feel powerless in the face of the dangers that it allegedly poses. And yet, trust between users and service providers is essential in order to maximise the Internet's potential to benefit social wellbeing and progress.[1]

This tension between the desire to use the Internet and concern about the risks of so doing – which might more broadly be described as the Internet's manifold impacts on the individual, society, politics and business – has come to be known as "Internet policy". In recent years, its importance in the socio-political discourse has grown enormously. In 2010, the German Parliament set up a Study Commission on the "Internet and Digital Society" to investigate topics such as data protection, copyright, media competence and consumer protection. Both the experts and the representatives of parties from across the political spectrum are now calling for the Study Commission's work to be progressed in a fully-fledged parliamentary committee on Internet policy. The data protection authorities and regional parliaments also regularly address issues such as the right to use pseudonyms in social networks, the use of user profiles and the retention of telecommunications data in order to fight

[1] Buchmann 2012; DIVSI 2012.

crime. Data protection and privacy questions also play an important role in the debate at European level. The new draft Data Protection Regulation published by the European Commission in 2012 seeks to extend the scope of data protection legislation beyond the boundaries of the EU for the first time, thus addressing the transnational dimension of this issue. Unlike previous directives, if this draft regulation is adopted it will be directly applicable in all the member states – it will not be possible for individual countries to strengthen or water down its provisions. The Commission's proposals task national governments with modernising their data protection legislation and progressing the public debate on the relationship between freedom, responsibility and regulation on the Internet.

This acatech POSITION PAPER and its recommendations are conceived as a contribution to the public debate on Internet privacy and incorporate the outcomes of acatech's "Internet Privacy" project. In view of the huge economic and social significance of this subject, the project initiated an intensive, interdisciplinary academic debate and multidimensional discourse that has not previously been seen on this scale in Germany. It is hoped that the recommendations will contribute to the establishment of a *culture of privacy* on the Internet, thereby relieving the tension between the huge benefits that the Internet offers its users and their concern that it may invade their privacy.

Privacy

The terms "privacy" and "private sphere" are not synonymous. "Private sphere" evokes a protected place where you can fully conceal yourself from the outside world. However, there is a larger dimension when people communicate and interact with each other on the Internet. In this context, privacy becomes an important aspect of social interaction. Someone having a political discussion with their friends may not wish third parties such as work colleagues to be privy to it. Likewise, if you are shopping online you may not be keen for others to know what you are buying. In interactions like this, people choose to reveal some things about themselves and conceal others. Privacy means the ability for people to choose and control what they disclose and what they hide. They may wish to hide everything, as in the case of anonymous communication. Or they may only wish to hide certain information about themselves, such as their age, gender or address. Another example of this understanding of privacy is that users may choose to appear in different guises, e.g. when participating in professional or private social networks. The details of this definition of privacy depend on our culture. In Germany and the rest of Europe, privacy is closely connected to the basic right to "informational self-determination".

Culture

In the broadest sense, culture refers to everything that human beings create by themselves. It encompasses technology and art, but also the law, our values, business and science. It is a framework built on explicit and implicit rules, regulations and beliefs. Culture creates stability in human actions and interactions. It should be constructed in a way that allows for reasonable privacy. This requires its different aspects to be cross-referenced so that their multiple mutual interdependencies can be taken into account. For example, if the law stipulates the right to be forgotten on the Internet, implementing this right needs to be technically feasible. The EU's draft Data Protection Regulation does in fact provide for this right, however it will be many years, if ever, before it becomes technically possible to implement it. In a culture of Internet privacy, legislation would only require something if it made sense and was technically feasible. Service providers and users would comply with these laws whilst also developing the appropriate voluntary practices and standards to ensure privacy-friendly behaviour by all the stakeholders. Technical experts would work to develop more effective privacy protection methods that did not curtail the benefits provided by the Internet.

Reasonable privacy

It is necessary to create a culture of privacy. To do this, we need to decide what constitutes a reasonable degree of privacy. As yet, no clear answer has been found to this question either in Europe's democracies or elsewhere. For example, while some social network users share their personal information with hundreds of friends, other people would never dream of doing this. In addition, our idea of what constitutes reasonable privacy is closely connected to events in our own history.

In view of this complex and dynamic situation, acatech proposes the use of a fixed reference point that will enable the definition of reasonable privacy to be repeatedly amended as and when necessary. Whether privacy is "reasonable" or not should be judged on how well it promotes the basic European values of (i) free self-determination, (ii) democratic participation and (iii) economic wellbeing that form the basis of our pluralistic western European democracies. In other words, acatech does not regard privacy as a value per se – it is only valuable and worth protecting insofar as it helps to uphold, protect and promote the abovementioned basic values. These basic values form an inalienable part of our universal human rights and are indispensable for people to live in dignity, free from hunger, fear of oppression, violence and injustice. acatech therefore believes that they will also be widely accepted outside of Europe.[2]

The relationship between privacy and these values is ambivalent. If extensive details of someone's personal data and information are known to others, they can no longer freely choose how they go about their lives or how they participate politically. Privacy is therefore essential if these values are to be upheld. On the other hand, online services can actually still support these values, even if they sometimes offer little or no privacy. This is the case, for example, when they provide a platform for political debate, offer sources of information or enable like-minded people to connect with each other when this would otherwise not be possible. Consequently, a culture of Internet privacy must enable reasonable privacy without placing excessive constraints on the opportunities offered by the Internet.

The next section of this position paper will take a closer look at the abovementioned basic values, describe their relationship with privacy and analyse the extent to which the Internet can contribute to upholding them. Section Three outlines the threats to Internet privacy and discusses their impact on the three values. In Section Four, we formulate a number of principles for developing a culture of Internet privacy. Finally, Section Five presents concrete recommendations in the key areas of education for children, young people and adults, regulation, business and technology.

2 UN 2000.

2 BASIC VALUES

The basic values of the European tradition that continue to be upheld to this day and that acatech has chosen as the basis for developing a culture of Internet privacy are as follows: (i) free self-determination, (ii) democratic participation and (iii) economic wellbeing.

Free self-determination

Free self-determination is defined as the ability of the individual to choose freely how they go about living their own life. It relates to choices such as religion, profession, friends and sexual orientation. The many different ends to which the Internet can be used mean that it can contribute to free self-determination. For example, it makes it easy to interact with other people all over the world. This increases a person's chances of coming into contact with like-minded individuals and potentially forming interest groups. Moreover, the availability of high-quality, free information and educational content on the Internet can help people to make their own choices about how to live their lives.

Privacy is also a key requirement for free self-determination. For example, individuals using the Internet to communicate and interact with other people around the world should be in a position to choose which information they reveal about themselves and which information they wish to conceal. Information intended for close friends, for instance, does not belong in a setting such as a business social network where people are showcasing their professional qualifications.

Democratic participation

Democratic participation is more than just the right and opportunity to participate in free and fair elections. It also includes the freedom of the individual to freely express their views on social and political matters, to participate in the formulation of society's goals and to have free access to the information required to make informed political decisions. Democratic participation is an important aspect of free self-determination and cannot exist without it. The Internet can make a very significant contribution to political participation. It is easy for people who share political ideologies or goals to connect with each other online. They can get their messages across in a far more enduring manner than at an individual meeting and they are not forced to rely on conventional media such as newspapers or television. Prominent examples of the Internet's role in political processes include the online petition against data retention, the WikiLeaks platform, which enabled publication of confidential government and corporate documents in the public interest, and the pro-democracy movements in the Arab world. The extremely sensitive reactions of totalitarian regimes to the Internet and their attempts to censor it bear witness to its importance in terms of shaping political opinion and facilitating political and social action.

Notwithstanding the above, democratic participation also requires reasonable privacy. Political groups can only productively develop their opinions if their members are confident that the views they express will not be taken out of context. Moreover, it is important that people engaging in political debates should only be required to disclose those aspects of their personality that are relevant to the debate in question. Exactly which aspects these may be will once again depend on their respective national cultures. For example, in Germany a politician's family life and friends are regarded as their own private affair and are kept out of political debates, whereas in the US they form a key part of a politician's image.

Economic wellbeing

Economic wellbeing, including the guarantee of basic material needs, is a fundamental requirement for people to live in dignity. Economic wellbeing necessitates both the creation of wealth and its widespread and fair distribution. Economic wellbeing also means that those who are able earn enough money to live comfortably whilst at the same time ensuring that the more vulnerable members of society such as children, the elderly and the infirm are supported and provided for. Although economic wellbeing plays an important role in

most societies, opinions differ as to the exact details of what constitutes wellbeing, as witnessed most recently in the debates within the German parliament's Study Commission on "Growth, Wellbeing and Quality of Life".

As a key component of the modern-day economy, the Internet makes a substantial contribution to economic prosperity. As stated in a recent judgement of Germany's Federal Court of Justice[3], Internet access for all is essential in our modern information society. It enables access to education, knowledge and markets, for example. Over the past few years, the Internet has created many new professions and jobs. One study shows that in Europe alone more than 230,000 jobs depend on online social networks.[4] A huge range of products and services can be bought cheaply on the Internet's global marketplace. At the same time, many businesses – especially those providing data-centric services – can use the Web to improve their chances of success by showcasing their products and services to an international audience. Privacy also plays a role in economic wellbeing. Failure to respect people's privacy, for example by using personal data without the user's consent, can damage the extent to which the Internet is trusted, thereby harming the development of Internet-based industries.

The Internet thus makes a significant contribution to upholding the basic values of "free self-determination", "democratic participation" and "economic wellbeing", but at the same time this requires users' privacy to be protected. It is therefore necessary to ensure that Internet privacy is protected in a way that does not prevent the Internet from continuing to support these values.

3 BGH 2013.
4 Deloitte 2012.

3 THE CHALLENGE OF INTERNET PRIVACY

Many users of online services have doubts about whether their privacy is always properly protected. Are these doubts justified?

Two conditions need to be met to ensure reasonable privacy on the Internet:

User competence and freedom of choice

The first condition is that users need to be aware of how the Internet can support their personal development, political engagement and economic prosperity, but also understand the risks that could result from infringements of their privacy. They should be in a position to weigh up the pros and cons of these two factors so that they can decide what their preferences are with regard to Internet privacy and ensure that their personal privacy settings are configured in a way that matches these preferences. This implies that the relevant options should be readily available to users in a way that can be easily understood and managed by them.

It is sometimes suggested that it is the sole responsibility of the individual to protect their own privacy. However, given the complexity of the Internet and online services and the diverse nature of the different groups of people who use them, it is impossible for individuals to properly assess and respond to all the potential infringements of their privacy and their possible repercussions. A person's knowledge of and ability to act on privacy issues will always be confined to individual areas and will depend on their skills, interests and desire to engage. Consequently, privacy protection should not be left up to the individual. This is where the second key condition comes in:

Trustworthiness of the Internet and the relevant actors

The Internet and its services and stakeholders must guarantee basic privacy protection that is not tied to individual users' knowledge, personal preferences and actions. On the one hand, this condition applies to online service providers. Internet users want to be sure that there are appropriate (statutory and voluntary) rules governing the operation of online services and that service providers actually comply with these rules. An example of such a rule is data minimisation that requires services to be designed to operate with the minimum necessary amount of personal data. On the other hand, the requirement for trustworthiness also applies to other users, for example a person's friends on a social network. They too should comply with rules that guarantee basic privacy protection, preferably without it being necessary to enforce compliance by technical means.

Potential limitations

In many areas, *user competence*, users' *freedom* of choice and the Internet's *trustworthiness* are not yet sufficient to guarantee reasonable privacy. In this section, acatech provides an overview of the potential limitations on privacy. These are described in more detail in the studies published by the acatech "Internet Privacy" project.[5]

It is currently difficult for users to obtain adequate *information* about which of their personal data are known to online services and which rules are used for processing them and passing them on to third parties. In addition to the information that they knowingly provide to the services (e.g. their name, address, order details, etc.), users also leave many other traces behind which they may not be aware of, for example which web sites they visit, the identity of their friends and the content of the messages they write. Once all of these data have been collected, modern IT techniques can be applied to them to extrapolate additional information. Again, this is something that users are not always conscious of. For example, it may not be clear exactly what information is shared with third parties when a user plays an online game on a social network. This can lead to the danger of *decontextualisation*, where personal data are used in contexts that their owners would not agree to if they knew about it. In addition to decontextualisation, there is also the danger of *persistence*, where personal data are held for longer than

[5] Buchmann 2012; Buchmann 2013.

necessary. Users do not always know what happens to their data once it is no longer needed for a particular service. If a user requests that the data they have provided to a social network should be deleted, does this really happen? The answer is not always "yes". There are cases where the data are either retained or merely anonymised. This is where the third danger of *re-identification* comes in. It is now possible to use advanced analysis techniques to reassign many anonymous records to individuals. Users are not fully aware of what is being done in this regard, despite the fact that service providers do make detailed information available in their general terms and conditions, for example. However, this information is not always easily accessible and can be hard to understand.

Users are also limited in their ability to *freely* choose how their privacy preferences are configured, since online services do not always provide them with the desired options. For example, most e-commerce services on the Internet require users to provide their full personal details (gender, date of birth, address, etc.) even though these are not always necessary to provide the service. Other services, such as social networks, do provide extensive privacy setting options, but these are not always easy to understand and use. For example, it can be hard for social network members to prevent other users from publishing personal information about them in photo tags. Moreover, the freedom to choose one's privacy settings is typically restricted to the data that the service obtains directly from the user and is less likely to cover information extrapolated from these data. Users also tend to have no influence at all over whether the information is shared with third parties.

Netiquette, the Internet's international "moral code", is still not well-developed enough to ensure that Web users can always be confident of each other's trustworthiness. Meanwhile, the statutory regulations intended to contribute to privacy protection are inconsistent and in some cases fail to properly address the challenges posed by the Internet today.

Moreover, there are no widely accepted codes of conduct governing behaviour on the Web. In any case, not all service providers handle users' personal data in accordance with the either the law or the user's stated preferences. Indeed, even if services do try to comply with the relevant regulations, technical reasons can prevent them from doing so, for example if they end up storing unencrypted data in order to avoid slowing the service down too much. If personal data are passed on to third parties, it becomes even more difficult to ensure privacy protection. Advanced IT techniques now enable a lot of information to be extrapolated from the recorded data. For example, it is now possible to reassign anonymised data to individuals.

A lack of user and service provider trustworthiness can result in data being used for purposes for which they were not originally intended, de-contextualisation, unauthorised persistence and the re-identification of personal data. Online service providers are now engaging in auditing processes in a bid to boost their trustworthiness. However, most Internet users are not able to assess how valid these processes really are, meaning that in practice they do little to increase the extent to which users trust a service.

The repercussions of privacy constraints for the basic values

Section 2 showed that privacy is a key requirement for exercising and protecting free self-determination, democratic participation and economic wellbeing. This statement needs to be considered in more detail in view of the potential constraints on Internet privacy that have been described above. There are multiple instances of decontextualisation limiting the right to free self-determination, for example when it leads to Internet users' parents learning of their sexual preferences. Decontextualisation, persistence and re-identification can be associated with significant risks to free self-determination and democratic participation. For example, if people discuss who they have voted for on a private political discussion forum and this information is

subsequently made public, this constitutes an infringement of the basic democratic principle of the right to a secret ballot. In addition to these immediate threats, there are also indirect repercussions. The potential dangers could deter users from using the Internet as a means of supporting their free self-determination and political engagement. Economic wellbeing can also be compromised by a lack of adequate Internet privacy, since it damages people's trust in online services and can therefore prevent their commercial success.

This analysis demonstrates that Internet privacy protection is essential if the basic values described above are to be upheld.

4 PRINCIPLES FOR DEVELOPING A CULTURE OF INTERNET PRIVACY

A number of conclusions can be drawn from the preceding sections, providing a basis for concrete recommendations:

a) The Internet contributes to upholding the basic values of "free self-determination", "democratic participation" and "economic wellbeing".

b) Inadequate privacy limits the extent to which these values can be upheld.

c) Internet privacy should be implemented in a way that enables the basic values to be upheld in optimal fashion.

d) This can be achieved through a culture of privacy that encompasses education, regulation, business and technology.

5 RECOMMENDATIONS

The recommendations presented in this section are geared towards developing education, regulation, business and technology in such a way as to enable Internet privacy whilst at the same time ensuring that the Internet can fulfil its potential for supporting self-determination, democratic participation and economic wellbeing.

Section three establishes that two things are required to enable Internet privacy. Firstly, users must possess the relevant knowledge and be aware of the possibilities that the Internet can offer them. And secondly, they need to be confident that online services and other users will respect their privacy. The recommendations outlined below will help to meet these requirements. They are aimed at the areas of education, regulation, economic actors (service providers) and technology. It is the interplay between these areas that will create a culture of Internet privacy. Education ensures that users know both their rights and the opportunities and risks of the Internet and are able to configure their own personal privacy settings. Regulation establishes binding rules that must, however, be technically feasible if they are to be complied with. These rules are targeted at businesses, public authorities, users, etc., all of whom need to comply with both statutory regulations and other rules in order to enable reasonable privacy.

Every single one of the recommendations needs to strike a balance between strengthening privacy and avoiding placing excessive limitations on online services and their ability to support the basic values. Finding the right balance is by no means easy and was the subject of much debate during acatech's "Internet Privacy" project. Many aspects still require further research and debate and the recommendations should therefore not be regarded as definitive but should instead be seen as a basis for further discussion.

5.1 EDUCATION

Education has a key role to play in the development of a culture of privacy. The Internet and information technology in general are among the most important technologies of our contemporary culture. The extensive knowledge and skills required to use the Internet are known as *Internet competence*. The goal of education should be to develop these competencies.

In the context of this position paper, Internet competence refers to the ability to evaluate the usefulness of the Internet for one's own life and use it, in particular in order to enable free self-determination, democratic participation and economic wellbeing. This includes ensuring that users understand the Internet's main business models ("I pay for services with my personal data, service providers are commercial enterprises", etc.) and the relevant risks to their privacy ("data may be shared with potentially untrustworthy third parties", "once something is on the Net it stays there – information that may seem harmless now could cause trouble in the future").

Once they have this knowledge, users are in a position to modify their privacy preferences whenever they wish to (for example, a user might decide that they don't care whether a particular service provider knows what they are buying). Moreover, they know how to use the available options (monitoring tools, privacy settings, etc.) in order to configure their privacy preferences.

Users also know their duties (e.g. "defamation is also illegal on the Internet, the laws of the analogue world also apply to the digital world") and their responsibilities towards themselves and others. They understand that privacy is not an individual issue but that we are all responsible for guaranteeing one another's privacy.

Consequently, developing Internet competence enables users to manage Internet privacy issues in an informed manner, provides them with a variety of options and ensures that they are mutually trustworthy.

> Equip everyone with Internet competence

It is important that everyone should possess Internet competence. The appropriate educational provision should therefore be available for a variety of target groups. These include children and young people, students and trainees – particularly those who are training for professions where they will be dealing with privacy issues – and adults of all ages and educational levels, irrespective of whether they are frequent or infrequent Internet users. In addition, special continuing professional development measures will be required for professions that work closely with the topic of privacy. These include multipliers such as educators and teachers, as well as IT specialists, etc.

> Ensure that Internet competence forms an integral part of (pre-) school education

acatech recommends that, as a component of media competence, Internet competence should form an integral part of pre-school and school education. This is essential to ensure that children and young people acquire the relevant competencies. Internet and media competence should receive the same attention in schools as more traditional subjects. It can either be taught as a separate subject or be integrated as a cross-cutting component of existing subjects. Whichever approach is taken, it will be necessary to develop and implement innovative teaching methods and content. One idea might be a media workshop incorporating a variety of different formats. These could include students teaching teachers, e.g. how does self-organisation operate in online social networks? Students could also teach other students, e.g. how do service providers' privacy rules work, how do I use privacy settings properly, how do I find out whether a service is trustworthy? Discussions where everybody teaches everybody might also be valuable, e.g. what level of privacy do I actually want (my preferences) and why? Which rules are appropriate for the digitally networked world? Another format might involve students presenting the results of the media workshop to their parents, accompanied by presentations from external experts. These novel formats could be complemented by the traditional approach where the teacher teaches the students, e.g. "what business models are used on the Internet, what does its legal framework look like, what technical methods are employed to collect and exploit data (what is a cookie, what does "inference" mean)? acatech also recommends appropriate adult education provision for parents, e.g. at adult education centres.

> Ensure that privacy protection forms an integral part of professional training and continuing professional development

Many professions come into direct or indirect contact with privacy issues, for example doctors and other medical professions or IT specialists. acatech recommends that privacy protection should be a compulsory part of the training for these professions and should be incorporated into the relevant study and training courses. This also applies to economics and business studies courses whose students will become tomorrow's managers. As decision makers, they will be responsible for making the necessary resources available for privacy protection and will therefore need a sound grasp of the issues. The rapid rate at which Internet technology is developing means that appropriate continuing professional development (CPD) measures will be needed for people in work. These measures could potentially cover a wide range of topics. Parents, teachers and educators need to gain an understanding of how children and young people behave online and the specific group dynamics that arise in this environment. They also need to learn the importance of guaranteeing young people's privacy on the Internet and not "spying" on them. CPD courses teaching the ethical, legal and technical aspects of privacy protection can help teachers become experts on privacy and the Internet.

> Run public information campaigns on privacy protection

Recent years have seen public information campaigns on a variety of different topics. For example, the Federal Ministry of the Interior ran a campaign on the new electronic ID card. Meanwhile, "Safer Internet Day" is a day of action organised by the European Union to promote safety on the Web. This is also the aim of the initiative "*Deutschland sicher im Netz*" (A Safe Online Germany) being promoted by Internet industry businesses and associations under the auspices of the Federal Ministry of the Interior. acatech recommends that similar campaigns should be developed for the area of Internet privacy ("the Internet is very useful, but make sure you protect your privacy"). Campaigns could be run in the media (radio, TV, press, cinema), on billboards and on the Web itself, for example on social networks (viral marketing). acatech also proposes holding regular awards for the best and worst practices in the realm of privacy.

>Strengthen research into people's opinions and practices with regard to privacy

The widespread use of the Internet in everyday life is resulting in huge pressure to change our traditional understanding of what constitutes privacy. However, we still have very little idea about exactly where these changes are likely to occur and what they will involve. We are currently unable to gauge the extent to which the ideas and practices of the first generation of "digital natives" differ from traditional attitudes towards privacy or whether they will be perpetuated as a lasting trend in the future. acatech therefore recommends strengthening both diachronic research (focused on social history) and synchronic research (focused on the present). It has become particularly evident in recent years that quantitative studies based on user surveys can only serve as a first step in researching the current transformations. On the other hand, it would be desirable to encourage more research into the everyday privacy practices of Internet users in order to allow more concrete predictions to be made about how privacy might be handled in the future and the potential problems that could arise. Research into these issues in Germany is still in its infancy compared to the English-speaking world, for example.

Furthermore, it is inevitable that privacy practices which have emerged hand in hand with the Internet and are specifically related to it should have a large technical component. This has two consequences. Firstly, the rapid pace of innovation on the Net is matched by an almost equally rapid rate of change in terms of online practices (there are some applications that have only achieved widespread popularity in the last couple of years but are nonetheless already triggering extremely far-reaching transformations). It is therefore necessary to ensure that these practices are researched on an ongoing basis. Secondly, it is now almost impossible to conduct meaningful contemporary social research without considering the technological aspects. Consequently, research is now addressing processes whose nature and consequences cannot be properly analysed without a well-established culture of interdisciplinary research. Whilst the social sciences have a lot to learn from the technological sciences in this regard, the reverse is also true. Cooperation between the two is essential if we are to gain an in-depth understanding of the relationship and possible discrepancies between widely accepted ideas about privacy, what users actually do in practice and the technical aspects of how the Internet operates. Among other things, this approach would enable specific problems associated with the use of particular tools (privacy settings, PETs) to be identified (usability research).

There is also an urgent need for reliable data regarding the impact of educational measures on how privacy is dealt with. Close coordination of media education and privacy research in the social sciences would be desirable in this regard. As described above, there are a number of arguments in favour of systematically integrating the teaching of Internet competence into school education. It would be desirable for the introduction of these educational measures to be accompanied by pedagogical and social science

research in order to establish how successful different teaching methods are and the extent to which they influence users' privacy practices.

5.2 REGULATION

The following propositions are designed to increase people's confidence in the Internet by making them more aware of what is going on when they are on the Web and increasing its trustworthiness. Since the Internet is a global phenomenon, it should ideally be subject to international regulations. The recommendations outlined below suggest some fundamental principles that might serve as a basis for international regulation. Although they draw on the European Union's Data Protection Regulation, they also include a number of proposed amendments to this document.

> Leave technical implementation up to the service providers

Laws and regulations should confine themselves to formulating goals (e.g. "users should have the option of deleting their personal data"). The technical implementation of these goals should be left up to the individual services so that unnecessary restrictions on the service can be kept to a minimum. Auditing processes can be used to check whether the goals have actually been met.

> Apply privacy protection law that users are familiar with

acatech recommends that service providers should be required to comply with the privacy protection law in the place where the people using the service are located. This would mean, for example, that European privacy protection standards would be guaranteed within Europe even if the service provider is based in a country with lower privacy protection standards. In this way, users can be confident that the local legislation which they are familiar with will always apply and they will not have to acquire a knowledge of several different legal systems if they wish to enforce their privacy protection rights. In order to make this approach feasible for service providers, privacy protection legislation should be harmonised over as wide a geographical area as possible and this area should be governed by a single privacy protection authority like the one being planned for Europe.

> Regulate how consent is provided

As a rule, the acquisition and use of personal data requires the informed and voluntary consent of the person in question. This is particularly true when it comes to creating user profiles. Consent should be obtained in such a way as to ensure that users know exactly what they are consenting to. Parents or legal guardians should have the sole right of consent to the use of their children's personal data in order to increase their trust in the services being provided to them. Since it can be hard to determine whether consent was granted voluntarily in individual cases, standard case scenarios should be developed in order to help establish this. Use of personal data without prior consent should only be permitted if appropriate security measures such as encryption are taken in order to guard against the relevant risks.

> Create transparency and enable control

Service providers should provide their customers with up-to-date and easily understood information about which personal data they are storing, how these data are being used, who they are being shared with (particularly if they are being shared with parties in other countries with weaker data protection standards), how long they will be retained for, etc. Users should have the option of amending and deleting these data.

> Enable deletion of data

In addition to enabling active personal data deletion, service providers should also offer users the option of setting dates after which their personal data – or at the very least any data generated by the users themselves – will be automatically deleted. The universal right to be forgotten on the

Internet is not yet a realistic proposition with the technology that is currently available.

> Support migration

Today, long-time users of online services such as particular social networks or e-commerce platforms are very tied to using these services, since they have personalised the way they use them over a long period of time. Social network users have built up groups of friends, stored photos, posted information, etc. E-commerce services know their customers' preferences and can use this information to optimise the products and services that they offer them. Customers should have the option of taking all this personal information with them if they choose to switch to another service provider. Supporting migration in this way is important not only for users but also for competition between service providers. Offering better privacy protection might be one way for providers to convince customers to switch to them.

The recommendations presented up to this point in this section are geared towards establishing a regulatory framework that enables users to obtain adequate information about the repercussions that using an online service may have for their privacy and provides them with the option of configuring their own preferences for how they wish to use the service. The recommendations outlined below focus on how the Internet can be made trustworthy, which is the second key requirement for reasonable privacy protection.

> Comply with data protection principles

Online services should comply with the basic data protection principles of restriction to a specific purpose, data minimisation, data security and data privacy friendly default settings. Restriction to a specific purpose means that personal data (irrespective of whether they have been obtained directly or through data processing techniques) may only be used for purposes to which the user has consented or which are permitted by the relevant legislation. Data minimisation requires services to be designed to operate with the minimum necessary amount of personal data. For example, this may mean allowing users to use services anonymously or under a pseudonym. Data security should be implemented using modern technologies such as encryption. Data privacy friendly default settings should serve to ensure that services meet users' expectations regarding their personal data privacy even if the users do not modify the default privacy protection settings.

> Regulate privacy protection certification

acatech recommends the introduction of privacy certificates and seals that are globally or at least widely regulated and recognised. This would make it possible for privacy protection to confer a competitive advantage. Furthermore, privacy certificates and seals would allow service providers to delegate the task of checking whether their suppliers have adequate privacy protection guarantees in place. Regulation should only provide a framework for guaranteeing quality and consistency. The actual design of privacy certificates and seals should be left up to businesses themselves.

> Investigate incentives to encourage self-regulation

The main need for research concerns how the law – which focuses on decreeing what people should and shouldn't do and official enforcement thereof – might be replaced or complemented by other mechanisms to create suitable incentives for encouraging privacy protection. First of all, it is necessary to investigate how competition can be harnessed to promote privacy protection. How can privacy protection be made into a selling point and competitive advantage? How can the reliable market information needed to do this be generated and disseminated? Secondly, privacy protection in the context of online services is highly dependent on regulation and technology working together. It is important to ensure that users can protect their own privacy (individual data protection) whilst also being protected by the online service (system data protection). Thirdly, research is needed into which matters can be self-regulated by service providers. What framework and incentives are required to

ensure that self-regulation is delivered in a timely manner and fulfils the desired goals?

Furthermore, acatech recommends investigating whether and how the introduction of no-fault liability for online services might help to increase people's trust in the Internet. No-fault liability would guarantee that online service providers would be liable for any damage caused by their service, irrespective of whether or not they were at fault for the damage in question. Accordingly, acatech also recommends studying whether and how privacy protection laws should be extended to cover the processing of data intended for private and personal use, since powerful data processing tools are now readily available to all Internet users.

5.3 BUSINESS

As described in the previous section, all providers of online services, whether commercial or otherwise, should contribute to a culture of Internet privacy by creating transparency, enabling control and migration and complying with the principles of data protection. They should do so irrespective of whether it is legally required of them or not. This will increase the extent to which their service is trusted and improve their commercial prospects. It will also increase the overall level of trust in the Internet and thereby support its development for the benefit of society and the economy. acatech's recommendation is that regulation should be confined to establishing goals, incentives, controls and penalties, allowing service providers to choose the best way of implementing the relevant rules. In addition, acatech has also formulated the following recommendations:

> Offer more privacy protection options

Currently, many online services (e.g. search engines and social networks) are "paid for" with users' personal data. This means that users only have limited control over their own data. acatech recommends the introduction of chargeable premium services that have tighter restrictions on how personal data may be used. For example, they might undertake not to use personal data for targeted advertising or they may allow pseudonyms or even anonymous use. This recommendation is not only aimed at existing service providers – start-ups offering this type of service should also receive the appropriate support. The higher the number of users wishing to protect their privacy, the more attractive this business model will become for service providers, especially if credible privacy seals and certificates are introduced.

> Enable use of privacy agents

acatech recommends that online services should offer users the option of using privacy agents. Privacy agents are programs where users only have to input their preferences once (e.g. "when I use an app, never disclose my address"). The program subsequently applies these preferences automatically, only requiring further personal input from the user for important or critical issues. This approach requires the relevant information to be provided in a format that can be interpreted by privacy agents.

> Harmonise standards

Irrespective of any regulations that may be introduced, service providers should agree among themselves on voluntary standards that allow privacy agents to help users configure their privacy preferences and enable them to migrate their key data from one service provider to another. These standards should include privacy agent user interfaces to ensure that it is simple for users to configure their privacy preferences.

> Develop privacy seals and certificates

Online service providers should jointly develop independent, quality-assured privacy seals and certificates and undertake to use them on a widespread basis. Regular quality testing by independent institutions would help these privacy seals to gain acceptance and contribute to building trust in general.

5.4 TECHNOLOGY

None of the above recommendations can be implemented without being supported by the relevant technologies. However, the necessary technologies, if they exist at all, are often still in their infancy. In many cases, a substantial research effort will be required to develop the relevant technologies.

> Apply the "Privacy by Design" principle to the development and operation of online services

Traditionally, the primary consideration when developing a service is its functionality. Measures to guarantee the security and privacy of the service are only taken at a later stage. This approach adds to the cost of protection measures and its results are often unsatisfactory. Consequently, it would be desirable for the "Privacy by Design" principle to be applied to the development and subsequent operation of online services.

"Privacy by Design" begins with an analysis and public discussion of the impact that a service has on its users' privacy. This analysis requires the service's security, trustworthiness and privacy to be defined, quantitatively assessed and analysed as automatically as possible, particularly with regard to aggregated and derived data. acatech recommends strengthening research into the technical support tools (checklists, development tool upgrades, automated tests, etc.) and reference architectures (best practices for particular use cases) that developers and administrators will need to enable successful and cost-effective implementation of "Privacy by Design".

> Support informed and considered consent

As described in Section 5.2, the acquisition and use of users' data by service providers generally requires the user's consent. Even today, this principle poses numerous technical challenges most of which have yet to be properly investigated and still lack adequate solutions. acatech recommends that particular attention should be paid to solving the following research and development questions: how can we design consent mechanisms that ensure users are fully aware that they are giving their consent rather than blindly agreeing to everything so that they can obtain the desired service more quickly, or giving up in frustration on a transaction that they actually want to carry out? How can we ensure that children's consent, for example, may only be granted with their parents' approval so that children cannot use services that are deemed unsuitable for them? How can consent be granted (or refused) for the use of derived data, i.e. data that have been acquired without direct involvement of the person they relate to?

> Research the right to be forgotten on the Internet

A comprehensive "right to be forgotten on the Internet" would constitute a significant step forwards. This would involve going beyond simply deleting the primary data collected directly from users by service providers. However, we currently lack both a precise understanding of what is meant by the "right to be forgotten" and the means to ensure its widespread implementation. acatech recommends carrying out research and development into methods to enable deletion of data that have been shared with third parties and information obtained using analysis techniques, for example through cross-provider data and security models (e.g. sticky policies where the data "know" when they should be deleted). It is likely that these methods will involve a lot of effort and expense. It will therefore also be necessary to develop practical evaluation methods that allow the consequences of not deleting data to be assessed. For example, while there is no good reason to delete properly anonymised data, apparently anonymised data can often be subsequently reassigned to individuals.

> Ensure user-friendliness

Privacy protection technologies, where they exist at all, are often not implemented in a way that allows them to be used to their full effect. One reason for this is that they

are often complicated to use and thus fail to meet the requirement for services to be as simple to use as possible. acatech recommends research into the usability of these technologies. This would include investigation of Internet users' preferences, i.e. the mental models which describe people's reactions to using services.

> Support user competence and freedom of choice

For user competence to be possible, users need to know which of their personal data are being held, where they are being held and what the consequences for their privacy are. Once they know this, they are in a position to determine and configure their privacy preferences. acatech recommends the continued development of tools (privacy agents) that show users which of their personal data are known to a particular service or group of services (e.g. all the social networks that they are active members of) and what the implications are in terms of their privacy preferences. This will not only involve major analytical and technical challenges – the tools will also need a user-friendly design employing non-verbal information such as traffic lights or signposts, for example. The tools should also provide users with support when taking decisions about their privacy, for instance if a service wishes to use their address details.

acatech recommends the development of standards in a variety of areas. The policies used by service providers for processing personal data should be standardised. Standardised policies can be written in a way that is easier for users to understand and also enable automatic evaluation. It is particularly important for this automatic evaluation to be performed before a service accesses other services. By the same token, standardised user privacy profiles should be developed and made available. This would increase the options available to users and remove the need for them to create their own profiles, since they could be confident that the standard profiles would achieve their desired goals. Standardised user profiles should be supported by technologies that enable previously formulated preferences (e.g. "please do not share this information with third parties") to be converted into automatically executable policies. acatech also recommends the development of standard formats to support the migration of user profiles from one service to another. This would allow users to choose the service that most closely matches their privacy preferences.

> Support trustworthy auditing

It is not easy for users to know whether a service is really respecting their privacy. Auditing and certification schemes can provide a solution to this issue. acatech recommends the development of standardised audit evaluation criteria and processes that encompass not only a given online service but also any third parties that may be involved, for example app developers, advertisers, enhanced service providers such as recommenders or third-party vendors in the sphere of e-commerce. This would help enhance the comparability and validity of audits and certificates. IT baseline protection and common criteria protection profiles could serve as a model in this regard. Continued development of software systems for automatic evaluation is particularly important in this area. The certificates awarded by independent auditors should be complemented by the development of recommendation systems such as those already in use in the area of e-commerce. These would provide an additional means of rating the privacy-friendliness of online services. Finally, acatech also recommends the development of certification technologies to provide users with verification of whether their privacy agents work correctly.

> Investigate data mining processes for big data privacy

Vast quantities of data are stored on the Internet (big data) and are analysed using advanced IT techniques (data mining), especially for business purposes (business intelligence). This ability to analyse big data has repercussions for privacy. acatech recommends the use and continued development of methods for informing users of potential threats to their privacy.

> Enable anonymous and pseudonymous use of services

It is undoubtedly important for many online services to be able to repeatedly identify users so that they can build stable customer relationships. On the other hand, there are many services that could be used anonymously or at least using a freely chosen pseudonym. All they need to do is reliably confirm certain customer attributes such as their age group, current address or membership of a particular group – they do not need any further information about their identity. acatech therefore recommends that businesses should allow services to be used anonymously or with pseudonyms. Specific technological solutions will be required to implement this recommendation. Systems should be developed to help users manage their own identities, pseudonyms and attributes and monitor how they are used by online services (personal identity management). By the same token, systems should also be developed to enable online services to confirm certain attributes without needing to obtain any further information about the user's identity. Specific R&D challenges in this area include user-friendliness and the use of mobile and embedded (cyber-physical) end devices and the associated attributes.

> Continue to develop basic methods and technologies

In order to ensure effective privacy protection, the basic technologies employed need to be sufficiently secure. However, this is not something that can be taken for granted. Processes that are secure today may no longer be so in the future. Furthermore, future IT scenarios will require new basic protection technologies. acatech therefore recommends that research and development of basic technologies should be significantly strengthened. One key area is the development of encryption techniques capable of countering new threats such as quantum computers and tolerating the resource constraints of many modern IT components. A further example is the development of practical encryption protocols that support privacy, such as "fully homomorphic encryption" and "secure multiparty computation". These processes enable computations to be performed using encrypted data without actually disclosing the data themselves. One final example is the development of methods that support privacy whilst at the same time allowing illegal activity to be attributed to the people responsible for it.

acatech also recommends investigating how pairs of opposites such as privacy-friendly/privacy-unfriendly or secure/insecure can be differentiated in a more sophisticated manner to enable rating as "adequate for a particular context". Differentiating them in this way will allow acceptable solutions to be found that are also affordable.

6 THE NEXT STEPS

Working in an interdisciplinary project group proved to be a very productive approach. Following intensive research and discussion, the representatives of the different scientific disciplines and commercial enterprises involved in the project were able to formulate joint recommendations for the establishment of a culture of Internet privacy. These recommendations are based on our current understanding of Internet privacy today and our expectations for the foreseeable future. However, research efforts also need to address challenges and opportunities that lie beyond the foreseeable horizon.

acatech therefore recommends the formulation and investigation of scenarios to examine how information technology, its social and economic importance and its impact on privacy and the basic values may develop in the future. Additional disciplines such as psychology and other social groups could be invited to participate in this process.

Mention has already been made of the unmistakable trends towards cloud and mobile computing and embedded IT and cyber-physical systems, all of which are primarily driven by information technology. These technological developments are accelerating key economic and social trends such as the transformation of consumers into producers of information and services, the globalisation of work and the increased prevalence of flexible and dynamic employment relationships, dispersed energy generation and urban manufacturing and personalised medicine involving extensive use of information technology. Common to all of these trends is the fact that IT is quite literally becoming ever more closely involved in people's lives, making privacy protection even more important.

Will current trends continue apace, with more and more private information entering the public domain, or will a counter-movement emerge and if so what impact will this have on the fundamental technological trends?

Many of the technologically most effective privacy protection measures will require huge, non-evolutionary changes to existing IT infrastructure. For example, end-to-end encryption on the global Internet will require a globally trustworthy infrastructure (known as a PKI). Whilst technical solutions do exist, organisational issues mean that implementation does not currently appear to be feasible. How could and should current trends such as the transformation of manufacturing industry into "*Industrie 4.0*" (the third industrial revolution) be managed in such a way as to provide people with more options for choosing how they wish to protect their privacy?

There is an even more fundamental question in this regard: is it even possible to find trustworthy solutions for the Internet as it exists today? If the answer to this question is no, what would an Internet where trustworthiness is possible look like and how could this information be used to influence current developments?

LITERATURE

BGH 2013
Bundesgerichtshof (BGH): *Judgement of 24.1.2013* (Az. III ZR 98/12), Karlsruhe 2013.

Buchmann 2012
Buchmann, J. (Ed.): *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Buchmann 2013
Buchmann, J. (Ed.): *Internet Privacy – Options for adequate realisation* (acatech STUDY), Heidelberg et al.: Springer Verlag 2013.

Deloitte 2012
Deloitte: *Measuring Facebook's Impact in Europe. Executive Summary*, London 2012. URL: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/uk-tmt-media-facebook-europe-economic-impact-exec-summary.pdf [Accessed: 04.02.2013].

DIVSI 2012
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*, Hamburg 2012.

UN 2000
United Nations (UN): *United Nations Millennium Declaration*, September 2000. URL: http://www.un.org/millennium/declaration/ares552e.htm [Accessed: 04.02.2013].

> THE FOLLOWING ENGLISH VOLUMES HAVE BEEN PUBLISHED TO DATE IN THE "acatech POSITION PAPER" SERIES AND ITS PREDECESSOR "acatech TAKES A POSITION":

acatech (Ed.): *Perspectives on Biotechnology Communication. Controversies - Contexts – Formats* (acatech POSITION PAPER), Munich 2012.

acatech (Ed.): *Towards a Financially Viable Transition to Sustainable Energy. Efficient regulation for tomorrow's energy system* (acatech POSITION PAPER), Munich 2012.

acatech (Ed.): *Georesource Water –The Challenge of Global Change Approaches and requirements for an integrated management of water resources in Germany* (acatech POSITION PAPER), Munich 2012.

acatech (Ed.): *Future Energy Grid. Information and communication technology for the way towards a sustainable and economical energy system* (acatech POSITION PAPER), Munich 2012.

acatech (Ed.): *Driving German Innovation. The role of incubator organisations in the promotion of high-tech academic spin-offs* (acatech POSITION PAPER), Munich 2012.

acatech (Ed.): *Cyber-Physical Systems. Driving force for innovation in mobility, health, energy and production* (acatech POSITION PAPER), Heidelberg et al.: Springer Verlag 2011. Available at www.acatech.de and www.springer.com

acatech (Ed.): *Phasing Out Nuclear Power Safely. Why Germany needs nuclear expertise for decommissioning, reactor safety, ultimate disposal and radiation protection* (acatech POSITION PAPER), Munich 2011.

acatech (Ed.): *Smart Cities. German High Technology for the Cities of the Future. Tasks and Opportunities* (acatech TAKES A POSITION, No. 10), Munich 2011.

acatech (Ed.): *Strategy for Promoting Interest in Science And Engineering. Recommendations for the present, research needs for the future* (acatech TAKES A POSITION, No. 4), Munich 2009.

acatech (Ed.): *Materials Science And Engineering in Germany. Recommendations on image building, teaching and research* (acatech TAKES A POSITION, No. 3), Munich 2008.

> acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

acatech represents the German scientific and technological communities, at home and abroad. It is autonomous, independent and a non-profit organisation. As a working academic institution, acatech supports politics and society, providing qualified technical evaluations and forward-looking recommendations. Moreover, acatech resolves to facilitate knowledge transfer between science and industry, and to encourage the next generation of engineers. The Academy counts a number of eminent scientists from universities, research institutes and companies among its Members. acatech receives institutional funding from the national and state governments along with third-party donations and funding for specific projects. It organises symposiums, forums, panel discussions and workshops to promote new technologies in Germany and to demonstrate their potential for industry and society. acatech publishes studies, recommendations and statements for the general public. The Academy is composed of three bodies, the Members, organised in the General Assembly, the Senate, whose well-known figures from the worlds of science, industry and politics advise acatech on strategic issues and ensure dialogue with industry and other scientific organisations in Germany, and the Executive Board, which is appointed by the Members of the Academy and the Senate, and which guides the work of the Academy. acatech's head office is located in Munich while offices are also maintained in the capital, Berlin, and in Brussels.

For more information, please see www.acatech.de