Freedom

Responsibility

Diversity

Click E for Ethics

▶ Navigating the values of digital living

Work materials for schools and young people

klicksafe is co-funded by the European Union

klicksafe.de

Media competence
for more internet safety

in partnership with

IDE INSTITUT FÜR DIGITALE ETHIK

HOCHSCHULE DER MEDIEN

Title:
Click E for Ethics
Navigating the values of digital living
Work materials for schools and young people

Authors:
Prof. Dr. Petra Grimm, Karla Neef, Michael Waltinger –
Institute for Digital Ethics (IDE)/Stuttgart Media University (HdM)
Birgit Kimmel und Stefanie Rack – klicksafe

Contributors:
Franziska Hahn – klicksafe
Sandra Lentz – Pädagogisches Landesinstitut RLP
(Rhineland-Palatinate Institute of Education)

Cartoons:
Tim Gaedke

Editing, proofreading and correction:
Dirk Diemer

Responsible:
Birgit Kimmel, Pedagogical Supervisor klicksafe

2nd revised edition May 2015

Cooperation partners:
This guide was produced in partnership with the Institute for Digital Ethics (IDE)/Stuttgart Media University (HdM) and the EU initiative klicksafe.

Publisher:
klicksafe is the German awareness centre in the CEF Telecom Programme of the European Union. klicksafe is run jointly by the State Media Authority of Rhineland-Palatinate (LMK) (Coordination) and the State Media Authority of North Rhine-Westphalia (LfM).

Coordinator klicksafe:
Peter Behrens, LMK

The project is co-funded by the European Union,
http://ec.europa.eu/saferinternet

Berlin liason office:
LMK/Safer Internet DE/klicksafe
c/o die medienanstalten
Gemeinsame Geschäftsstelle der Landesmedienanstalten
Friedrichstraße 60, 10117 Berlin

Contact for enquiries:

klicksafe
c/o Landeszentrale für Medien und Kommunikation
(LMK) Rheinland-Pfalz
Direktorin: Renate Pepper
Turmstraße 10
67059 Ludwigshafen
Tel: 06 21 / 52 02-271
Email: info@klicksafe.de
URL: www.klicksafe.de

While every care has been taken in the production of this module, the publisher cannot guarantee the accuracy of the information it contains. Liability of the authors is excluded.

Note:
Masculine/feminine forms: This module principally uses the masculine form (he, his etc.). This is not intended to exclude female readers, merely to make the text more readable.

Layout and cover design:
Designgruppe Fanz & Neumayer
Schifferstadt

Click E for Ethics

Navigating the values of digital living

Work materials for schools and young people

Authors: Prof. Dr. Petra Grimm, Karla Neef, Michael Waltinger –
Institute for Digital Ethics (IDE)/Stuttgart Media University (HdM)
Birgit Kimmel and Stefanie Rack – klicksafe

Contributors: Franziska Hahn – klicksafe
Sandra Lentz – Pädagogisches Landesinstitut RLP
(Rhineland-Palatinate Institute of Education)

Cartoons: Tim Gaedke

klicksafe.de

IDE
INSTITUT FÜR
DIGITALE ETHIK

HOCHSCHULE DER MEDIEN

Introduction

There are three questions we should all be asking: How should we deal with the new challenges we face when using the Internet? What are the best ways to handle conflict situations? How should we behave in order to be responsible Internet users?

These and similar issues are becoming increasingly important in the process of developing media competence. There are loud calls for greater discussion of values and attitudes on every level of society. Media education and media ethics address these issues from different perspectives. The partners in this co-operation – klicksafe and the Institute for Digital Ethics – have joined forces in order to learn from each other's experiences and insights and formulate a combined approach that finds effective answers to these questions. The objective is not just to engage in a theoretical discussion of ethics and morals but also to consider how we can apply these practically when using media. The Internet is difficult to regulate and almost everyone has access so the effectiveness of moral norms is limited. We have to look more closely at the "new" agreements required among Internet users and, above all, at those required to provide an ethical framework for children and young people. What values should provide the foundation for these "new" rules on the Internet?

Ethical norms and values usually grow out of the interactions between individuals and communities. They are repeatedly revised and updated through negotiation between the various stakeholders. This process of continuous reflection and evaluation can also lead to the development of new perspectives and approaches. Yet negotiations of this kind are also influenced by power structures and special interests. To ensure that they reflect people's differing needs it is essential to be aware of a society's norms and values – as expressed through the behaviour of its citizens. Attitudes can be deep-rooted but also uncertain or ambivalent. The development of an attitude is a social learning process. It takes place through an analysis of the individual's own experiences, discussion with others and guided processes that help us to reflect on our own actions and improve them if necessary. To develop and refine our own attitudes, we need settings that provide a forum for raising awareness of, reflecting on, evaluating and confronting conflicts of values.

The teams from klicksafe and the Institute for Digital Ethics have embarked on a journey that seeks to address these questions. They have developed a process and specific methods, which enable us to promote reflection and the development of a values framework in practical (media) education. The following work materials offer teachers and educators a wide range of practical projects for their work with young people as well as stimulating ideas for taking these processes a step further. We have concentrated on three themes. These focus primarily on the need for an ethical framework, ways we can strengthen our own values and the development of values-based attitudes: protection of privacy, cyberbullying/online violence and gender sensitivity. We hope that these "navigation tools for media ethics" will be a useful guide and help you to enjoy a successful life in digital society.

Renate Pepper
Director
State Media Authority of Rhineland-Palatinate (LMK)
Coordinator, EU initiative klicksafe

Prof. Dr. Petra Grimm
Institute for Digital Ethics/Stuttgart Media University

Module 1

Privacy and big data

1 "How should I behave?"

Ethics

Ethics is the study of moral questions: it is the "philosophical science that deals with the standards and moral framework that govern the actions of human beings"[1]. **Moral** framework is the term used to describe the "overall complex of values, standards, beliefs and rules that define acceptable behaviour in a society or section of society (commandments, taboos)"[2]. The values themselves depend on how a society answers questions about the meaning of life and how to live a good life in a society.

In contrast to the study of morals, ethics examines individual values and attitudes from a critical distance. It has to take into account differences in living conditions and outlooks. It must justify its acceptance of particular values and norms through convincing arguments and reflect their importance for individuals and society as a whole. In summary, the study of ethics provides a foundation for answers to the question "How should I behave?" It formulates criteria, which we can use to establish an agreed framework that guides us on how to live and act. We can thus define ethics as the study of **how to behave well.**[3]

> *"As a scientific or critical discipline that reflects the morals of a society, ethics enables each individual to act with an awareness of his responsibilities. Firstly, it tells him what he can actually do. Secondly, it reveals to him the consequences of his actions and the assumptions on which these actions are based."*
> ***Klaus Wiegerling,*** *1998, p. 4*

A navigator and a helmsman

Media ethics

Media ethics, like medical, environmental or business ethics, is a special area of study and an example of **applied ethics.** Media ethics examines the ethical aspects of human communication via media – such as the Internet, TV, newspapers/magazines, radio, films, books etc. – and their relevance to society. In the wake of digitisation and the penetration of the analogue world by digital media, a new area has evolved in the realm of media ethics: digital media ethics deals with every area of life that is influenced by digital technology or computer-supported media, e.g. by big data or the "Internet of Things". Its task is to reflect on media and digital communication, consider the ethical implications of these technologies and act as a "navigation aid". Media ethics can therefore have three functions:

- descriptive (describe empirical findings and provide an ethical "interpretation" for them)
- normative (question why specific standards and norms should apply)
- motivational (deal with the possibilities, requirements and motivations for ethical behaviour).

This approach to media ethics promotes competence in using and understanding media **– a competence that is based on values.**

Questions of media ethics affect various groups. Firstly, they relate to the **users** who not only consume but also produce and distribute videos, photos and texts using new technologies. Secondly, they have implications for **media companies** and **other corporations** who do not produce media content themselves but profit from it or offer communication services – such as Facebook, WhatsApp, Google or Apple. In addition, media ethics considers the fundamental aspects of the **media system.**

The central questions of media ethics are therefore as follows: "How should I use modern media? How should we behave as producers or consumers of media communication content? And what standards should we apply when designing the structures of regional, national and global media systems?"[4]
We can illustrate these aspects of media ethics using a 3-level model incorporating the macro, meso and micro levels:

Society on the macro level

Fundamental questions regarding the media system

•

e.g. What benefits do media provide for society?
Which structures and regulations are important for a democracy?

Companies on the meso level

Questions affecting the self-perception, structures and actions of companies

•

e.g. What ethical standards should apply to companies?
What are companies responsible for?

Users on the micro level

Questions affecting the use and production of media and communication content as well as the ethos of the user

•

e.g. What are the responsibilities of the user?
What values and norms are desirable?

Fig. 1: Questions in media ethics

Real or media-generated?

Media ethics in the digital environment

Advances in Internet technology ("Web 2.0" or "social web") have opened up many new ways for users to communicate, participate and design their own content. These changes are having a major impact in every sphere of cultural and social life. Today, everyone can both consume and generate information very quickly and easily. We have tools that not only make it simpler to search for information but also to communicate with each other online. Moreover, the widespread use of mobile devices and appliances with Internet capability means that the Internet is almost omnipresent.
Consequently, users are producing and reproducing an ever-greater volume of content with ever-greater speed and adding new communication tools to their repertoire. The boundaries between the real and "media-generated" worlds are becoming less distinct, e.g. due to the intertwining of virtual and real social spaces in online social networks. This leap forward towards greater integration of media in our lives has triggered processes, which have accelerated communication and the fusion of the online and offline worlds. These processes have practical consequences for the ways we find information and communicate with each other, construct our realities and, importantly, for social systems of values and norms.Phenomena such as "shitstorms", "cyberbullying" and, more generally, the opportunities for rapidly disseminating misinformation or rumours are just a few examples that demonstrate the emergence of new ethical battlefields. As a result, there is a growing need for ethical systems that help us to navigate the worlds of society, politics and commerce.

> *"We may not know where we are going any more but we are going to get there a whole lot faster."*
> ***Douglas Rushkoff**, 2014*

Who is responsible for what, why, to what extent? These are the central questions of media ethics – especially in this age of digitisation. The public discussion focuses on the following themes in particular:

- the lack of self-determination in the area of information (e.g. data protection and privacy)
- harmful communication behaviours (e.g. trolling, cyberbullying, sexual harassment)
- the potential dangers posed by certain types of media content (e.g. violent videos, hate sites, Internet pornography, violation of human dignity, suicide forums)
- the function of media in providing orientation and role models for children and young people (e.g. sexual identity)
- inequality of access and opportunities for learning (e.g. due to the global digital divide and social disadvantage in media skills).

This handbook addresses three of these aspects. This is because "Internet activities can affect all users of the Web and therefore many more people than most other types of activity"[5]. Users face new challenges in terms of understanding how to behave ethically and their own moral outlook. So ethical questions about dealing with digital media also affect the **values structures** and **orientation of users** and the **motives** that govern their behaviour on the Internet. The **effects** of morally relevant Web content and the **consequences** of media-based activities for the user are also interesting. But first we should perhaps ask the question: what do we actually mean by a "value"?

2 "How can I get my bearings?"

Values

Taking Lautmann's[6] language analysis study of 180 different definitions of "value" found in reference works, we can understand the term as follows:

A "value" is

- a benchmark for what we consider good
- a criterion for deciding what we should strive to achieve
- a normative standard for judging our social environment
- a criterion for norms that are generally approved by a (section of) society.

We can therefore conclude that values are concepts, ideas or ideals. Values tell us what is desirable. They are standards we use to orientate and guide our actions – whether consciously or subconsciously. We can use them to derive specific rules or norms.

What is the function of values?

In sociological and psychological values research, values are assigned defined functions. Values can therefore control actions and behaviours: "A value is a characteristic notion of what is desirable for an individual or a group. It can be explicit or implicit and influences the process of selecting from the various courses, means and objectives of actions that are available to us."[7]
At the same time, values control our perception of the world around us and the judgements we make about it: "A value is understood to be an internal or internalised concept that plays a role in determining how we see the world and how we behave in it."[8]

According to Reichardt, values influence the motives of the individual and contain a high degree of generalisation or abstraction, i.e. they tend to define standards for large population groups.

We understand a value to be a mode of preference or rejection of objects or social statuses in a particular population. This anchors itself in the motivational structure of the individual. It has a high level of generalisation and at least the potential to become accepted by a large population group.[9]

"Absolute ideals of democratic society"	Respect for human dignity, freedom of faith and conscience, free speech, freedom of personal development etc.
"Values that serve as means for achieving the above objectives"	Justice and solidarity
"Values, which are instrumentally focused on the highest and intermediate values"	"Secondary virtues" such as self-control, feelings of responsibility, willingness to help

Fig. 2: Ranking of values (Huber/Funiok 2001, p. 16)

3 "What do I value and why?"

Conflicts of values

A moral dilemma describes a situation in which two or more norms contradict exactly the same system of moral values. It is a conflict that forces the subject to make a choice between two equally important values or principles that, individually, he would not normally wish to break. In other words, he is caught in a moral cleftstick from which there is no entirely satisfactory escape. "Only two options are available to him. Individually, both choices appear morally plausible but they are mutually exclusive. Whichever he chooses, he will break a fundamental moral principle. In other words, a dilemma contains a contradiction that you generally do not want to accept.

To make any kind of decision, you have to weigh up the pros and cons. At the end of this process, one of the possible courses of action will appear more acceptable than the other. Usually, this is the preferred choice."[10] Moral dilemmas are not just thought experiments but problems we encounter repeatedly in everyday life. They put us under immediate pressure when making decisions and have genuine consequences for the decision-maker.[11]

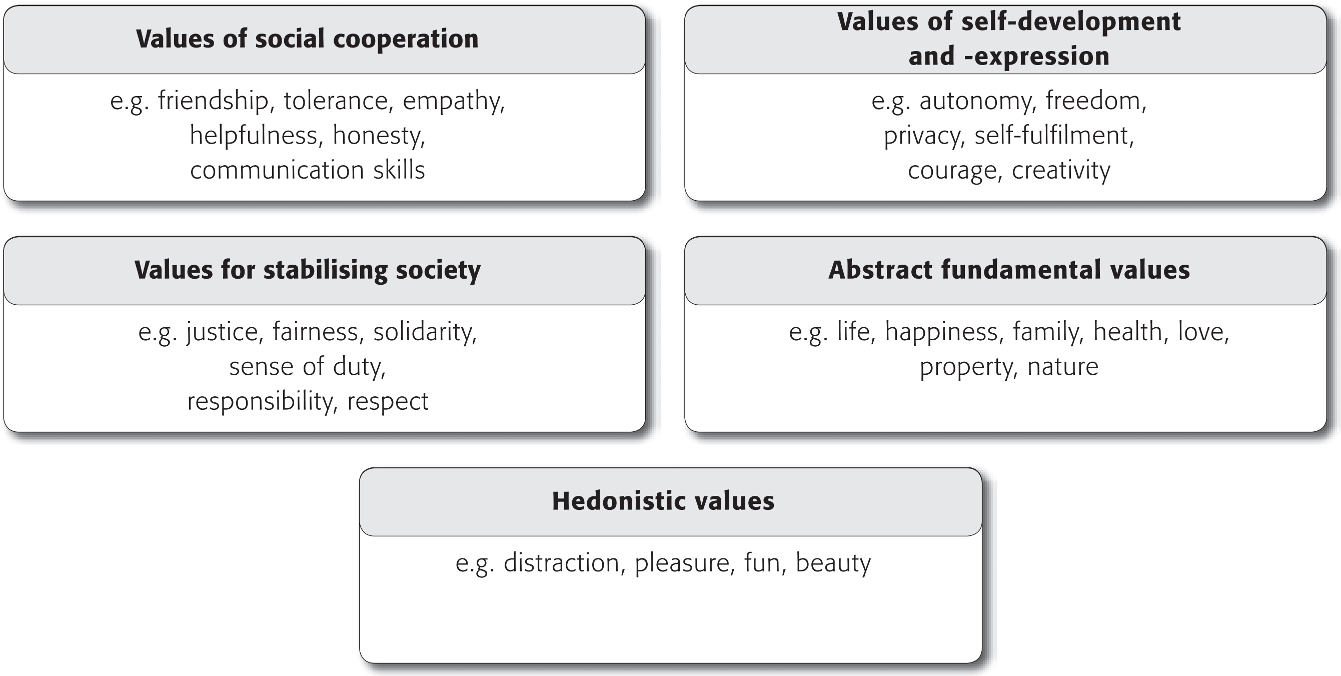
The use of online social networks provides one good example of conflicting values. Social networks offer important types of gratification, which affect the value field of social cooperation (see Fig. 3), especially the formation, care and maintenance of interpersonal relationships and friendships. The social capital generated by these networks generates self-confidence and satisfaction with life. As well as providing an opportunity for presenting yourself and personal development, we can also use social networks to enjoy hedonistic values such as fun, excitement and distraction.

As well as the "experience of community and participation", Funiok adds further values: "the value of being able to express affection (love) towards other people – and have it reciprocated," "the value of freedom/personal development/self-determination", "truth (and authenticity) of communication" and "the value of your own honour and personal reputation".[12]

When using privacy settings – i.e. to protect your own data – the paradigm of convenience also plays an important role. However, according to the definition above, convenience is not a value but a pattern of behaviour. In contrast to the virtues of "engagement" and "willingness to confront important issues", you could describe it as an 'unvirtue'. Regardless, this pattern of behaviour is an understandable reaction to a relatively complicated technology and continuously changing privacy settings, e.g. for Facebook.

Now – when a user of online social networks discovers that his data is being used, disseminated and stored for a long time, he finds himself facing a classic dilemma. The question is this: do the values of social cooperation, self-presentation and the hedonistic values shown in Fig. 3 have a greater controlling function over his behaviour than the value of his own privacy? If the answer is yes, the value of privacy is subordinate to the aforementioned values.

"In situations that can properly be described as moral dilemmas, the role of media ethics is therefore not to provide suggestions and ready-to-use solutions. Media ethics should function as a professional consulting discipline, which reconstructs contradictory positions and can offer transparency through pro and contra arguments"[13].



Values of social cooperation

e.g. friendship, tolerance, empathy, helpfulness, honesty, communication skills

Values of self-development and -expression

e.g. autonomy, freedom, privacy, self-fulfilment, courage, creativity

Values for stabilising society

e.g. justice, fairness, solidarity, sense of duty, responsibility, respect

Abstract fundamental values

e.g. life, happiness, family, health, love, property, nature

Hedonistic values

e.g. distraction, pleasure, fun, beauty

Fig. 3: Value fields (Grimm/Horstmeyer 2003, p. 24)

4 Thinking aloud rather than doubting in silence

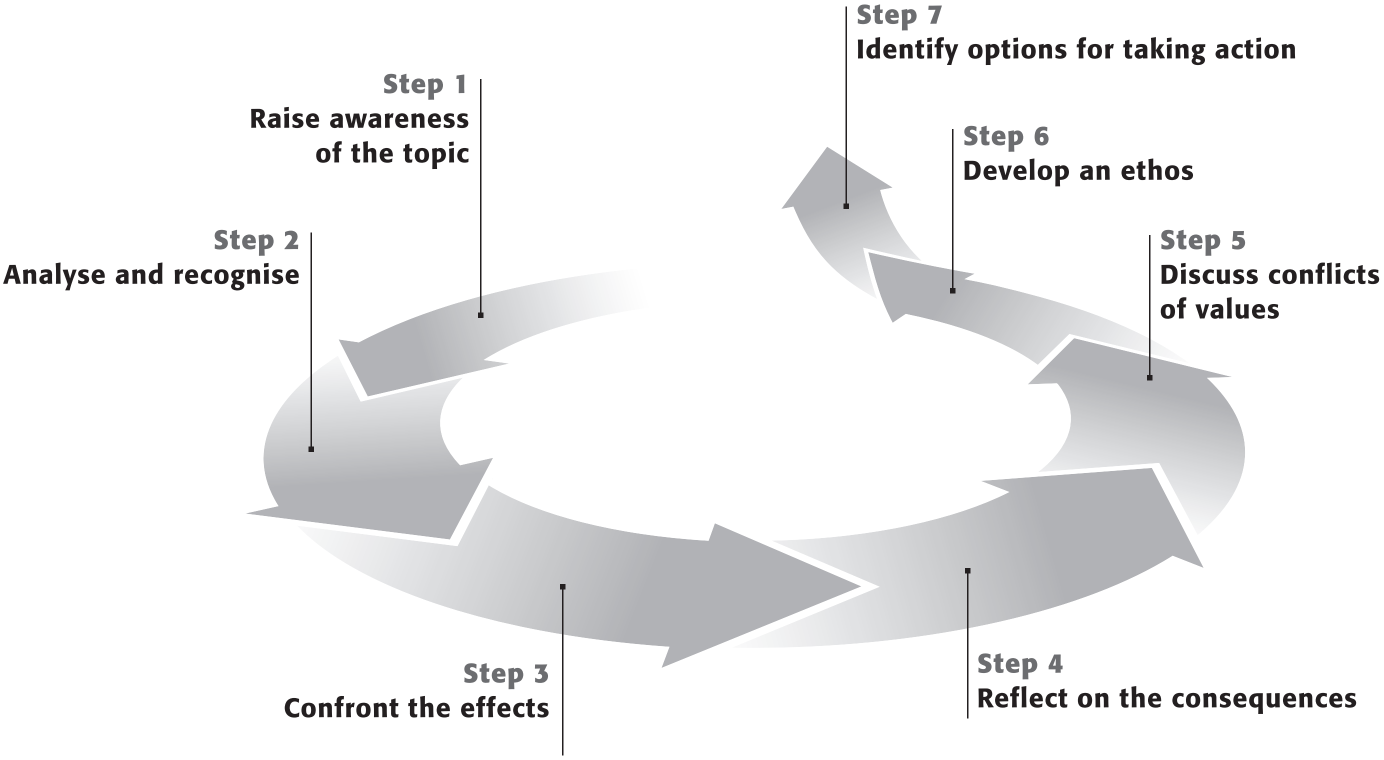
Media ethics roadmap
The aim of this media ethics guide is to stimulate the process of considering moral judgements and actions. It hopes to give pupils and students the skills they require to lead a successful life when using digital media and develop their own opinion – an ethos. To simplify this process, we have structured each module in the same way: each section of the "media ethics roadmap" is divided into seven different steps.

First, we analyse the situation by identifying the participants and scientific insights we have into the topic in question. Who is affected by what? What interactions exist between different interests? (Steps 1 and 2).

Then we analyse and reflect on the possible effects of the action. What would be the consequences? Are alternative courses of action available? (Steps 3 and 4)

In order to develop your own attitude towards a specific situation, it is important to be able to predict the consequences of your action – at least approximately. Above all, you must be able to analyse and reflect on the conflict of values (dilemma). Which values, standards and norms should you apply? Which values are in conflict? Which values should take priority – and why? (Steps 5 and 6). This opportunity to reflect on conflicts of values and consider the reasons underlying different opinions promotes the development of values in young people. By discussing problems that arise in dilemma scenarios, they are encouraged to "think aloud". In doing so, they recognise aspects they were previously unaware of and come to considered opinions.

At the end of each module in our media ethics roadmap, we highlight possible ways that individuals, groups (e.g. school classes) or society as a whole can take action. What can I do or what can be done? (Step 7)


Step 1
Raise awareness of the topic
Step 2
Analyse and recognise
Step 3
Confront the effects
Step 4
Reflect on the consequences
Step 5
Discuss conflicts of values
Step 6
Develop an ethos
Step 7
Identify options for taking action

Endnotes/References

[1] Eisenschmidt, Helge (Hrsg.) (2006): *Werte und Leben. Klassen 9/10.* Leipzig: Militzke Verlag. **p. 221**

[2] ibid. **p. 222**

[3] see Funiok, Rüdiger (2012): *Wertorientierte Strategien zum Schutz der Privatheit in Sozialen Netzwerken*. In: Grimm, Petra/Zöllner, Oliver (Hrsg.): Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffent-lichung des Privaten in Social Media und populären Medienformaten. Stuttgart: Franz Steiner Verlag, **p. 97–118.**

[4] Thies, Christian (2011): *Medienethik*. In: Stoecker, Ralf/Neuhäuser, Christian/Raters, Marie-Luise (Hrsg.): Handbuch Angewandte Ethik. Stuttgart/Weimar: Metzler.

[5] Lenzen, Manuela (2011): *Informationsethik*. In: Stoecker, Ralf/Neuhäuser, Christian/Raters, Marie-Luise (Hrsg.): Handbuch Angewandte Ethik. Stuttgart/Weimar: Metzler.

[6] see Lautmann, Rüdiger (1971): *Soziologie vor den Toren der Jurisprudenz: zur Kooperation der beiden Disziplinen*. Stuttgart: W. Kohlhammer Verlag.

[7] Kluckhohn, 1951, **p. 395**, cited in Scholl-Schaaf, Margret (1975): *Werthaltung und Wertsystem. Ein Plädoyer für die Verwendung des Wertkonzepts in der Sozialpsychologie*. Bonn: Bouvier.

[8] Oerter, Rolf (1970): *Struktur und Wandlungen von Werthaltungen*. München/Basel: Oldenburg.

[9] see Reichardt, Robert (1979): *Wertstrukturen im Gesellschaftssystem – Möglichkeiten makrosoziologischer Analysen und Vergleiche*. In: Klages, Helmut/Kmieciak, Peter (Hrsg.): Wertwandel und gesellschaftlicher Wandel. Frankfurt/New York: Campus Verlag, **p. 23–40.**

[10] Eisenschmidt (see above), 2012, **p. 99**

[11] see Raters, Marie-Luise (2011): *Moralische Dilemmata*. In: Stoecker, Ralf/Neuhäuser, Christian/Dies. (Hrsg.): Handbuch Angewandte Ethik. Stuttgart/Weimar: Metzler.

[12] Funiok (see above), 2012, **p. 98**

[13] Raters (see above), 2011, **p. 102**

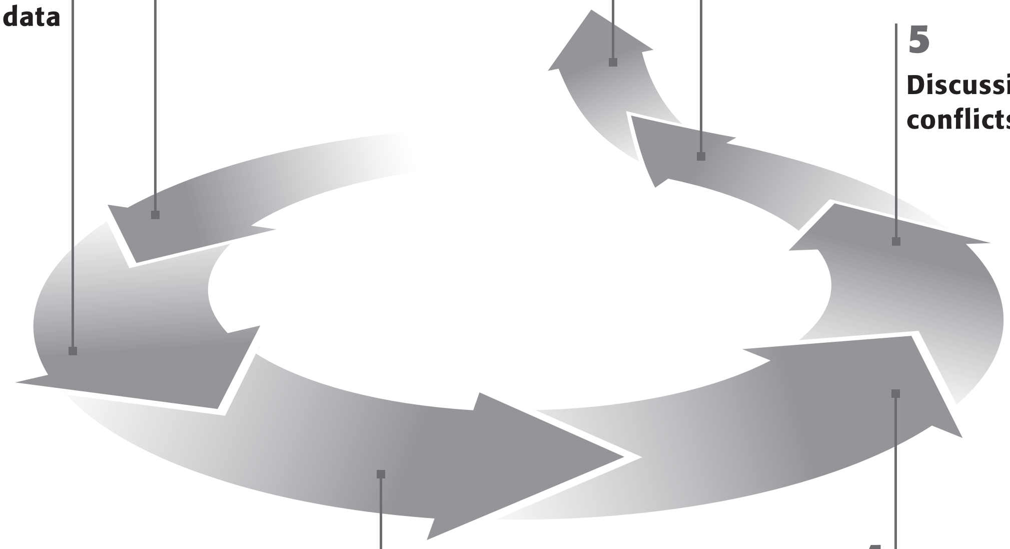
Quotes from the text

Rushkoff, Douglas (2014): *Present Shock. Wenn alles jetzt passiert.* Freiburg: orange-press.
Wiegerling, Klaus (1998): *Medienethik*. Stuttgart/Weimar: Metzler.

1 Privacy and Big Data

Media ethics roadmap for “Privacy and big data”

We can think about issues of privacy and big data and the ways we use media ourselves using the model below. The objective is to acquire competence in digital privacy.



1

Raising awareness of the importance of privacy

2

Recognising the mechanisms used to reveal and collect data

3

Confronting the risks posed by big data

4

Reflecting on the consequences of breaches of privacy

5

Discussing conflicts of values

6

Developing an ethos of privacy

7

Identifying options and tools for taking personal, political and instrumental action

- ***Module 1 | Privacy and big data***

Module 2 | Harmful online behaviour

Module 3 | Images of women and men in the media

Introduction

For many years, society has taken the existence of personal privacy for granted. Yet historically, privacy is a comparatively recent privilege. Protection of privacy only became a priority in the wake of civic emancipation and the creation of modern nation states in the late 18th and 19th centuries.

"The defence of privacy is the first step towards rescuing freedom."
***Wolfgang Sofsky,** 2009, p. 18*

Today, privacy and its values appear to be under threat. The reason: the digitisation of society has produced deep and irreversible changes. The extensive use of digital technologies and their adoption in every more aspects of our lives and living environments also has important consequences for our privacy. Edward Snowden's revelations in June 2013 confirmed what some already suspected: our personal digital data is being stored, traded and evaluated – not just by security services but also by a large number of commercial corporations.

In technology circles, some people are even suggesting that privacy may be a thing of the past. The post-privacy movement is convinced that privacy is outdated. They are calling for complete transparency and suggest that data protection is impossible to implement due to the global structure of the Internet, the notorious difficulty of applying national regulations and the "communication needs, curiosity and appetite for convenience (...) among users"[1].

Ask young people and young adults what they understand by "privacy" and they often struggle to define precisely what they think it should mean. "Young people and young adults associate the word "privacy" on the Internet above all with the privacy settings used by online communities – especially the settings for Facebook. In other words, they think primarily in terms of technological features that they can activate or deactivate. Consequently, you can even 'switch off your privacy'."[2]

Clearly, we must scrutinise the value of privacy once again. What is it precisely and what is it good for? Privacy is not an abstract concept but an important element of our lives yet very few of us are conscious of what it would mean to give up our privacy. To some extent, privacy is comparable with health: you only truly value it when you no longer have it. To protect your data – and therefore your own privacy – you must first be aware of the value of privacy to our own humanity and identity. This is the aim of Module 1 "Privacy and big data".

1 Trust is good, privacy is better

Raising awareness of the importance of privacy

There is no generally valid definition of “private”. It is more useful to think of privacy as an idea that can change due to historical and cultural factors as well as specific situations.

1.1 What is private?

Questions for reflection: *Questions for reflection: What do I understand by “private/public”? What would I describe as being “private” and “public”?*

Definition
The word “private” is derived from the Latin “privatus” meaning “stolen (from rulers), separate, standing for itself”. It signifies a separation from the public sphere – and especially from the state. In common usage, we normally use “private” as the opposite of “public”. This separation of the public and private spheres is not as clear-cut as it appears. When applied to personal privacy, it can refer not only to rooms or places but also to “actions, situations, (mental) states (…) and objects.”[3]. In the **spatial** sense, it is possible to imagine the uses of “public” and “private” as being like the layers of an onion. At the very core is the area of personal intimacy and confidentiality, e.g. a diary. The second layer comprises the areas that are traditional bedrocks of “private life”: family and other intimate relationships. Private life is usually represented by private spaces such as your own apartment or home (see Fig. 4). In contrast, public life comprises the outside worlds of society and the state.

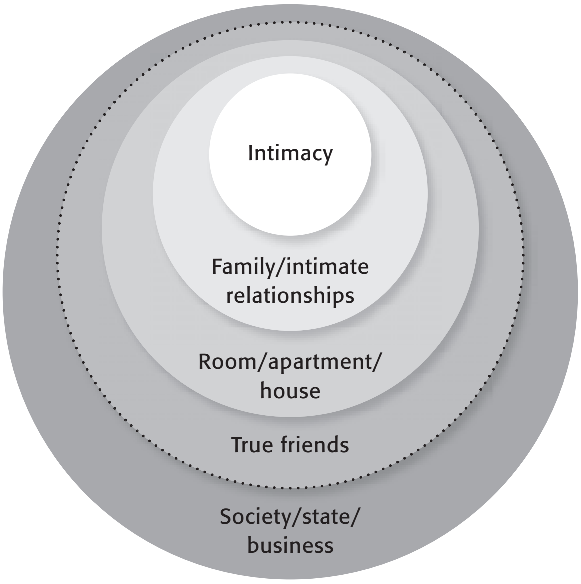


Fig. 4: “Spatial” privacy

However, it is also possible to describe **actions or decisions** as “private” even in public life. Going to a demonstration or to church is as much my own private business as talking with a friend in a café or the choice of clothes I wear in a public space. I could also describe my political outlook, opinions about people, information concerning my health or even who I live with as **private**.

We use “private” to describe rooms, actions, behaviours and specific types of information.

We should not confuse “private” with “secret”. Private matters can be secret but need not be so – as the example of clothing in a public space clearly shows. Conversely, secret information – such as state secrets – need not be private. Moreover, “private” does not have the same meaning as “intimate”: intimacy is a core area of private life but it is not identical to “privacy”. Privacy encompasses a much wider range of areas.

1.2 Here I can just be myself

Forms and functions of privacy

***Question for reflection:** What are the forms and functions of privacy?*

The political scientist and lawyer Alan F. Westin (1967) described four forms of privacy:

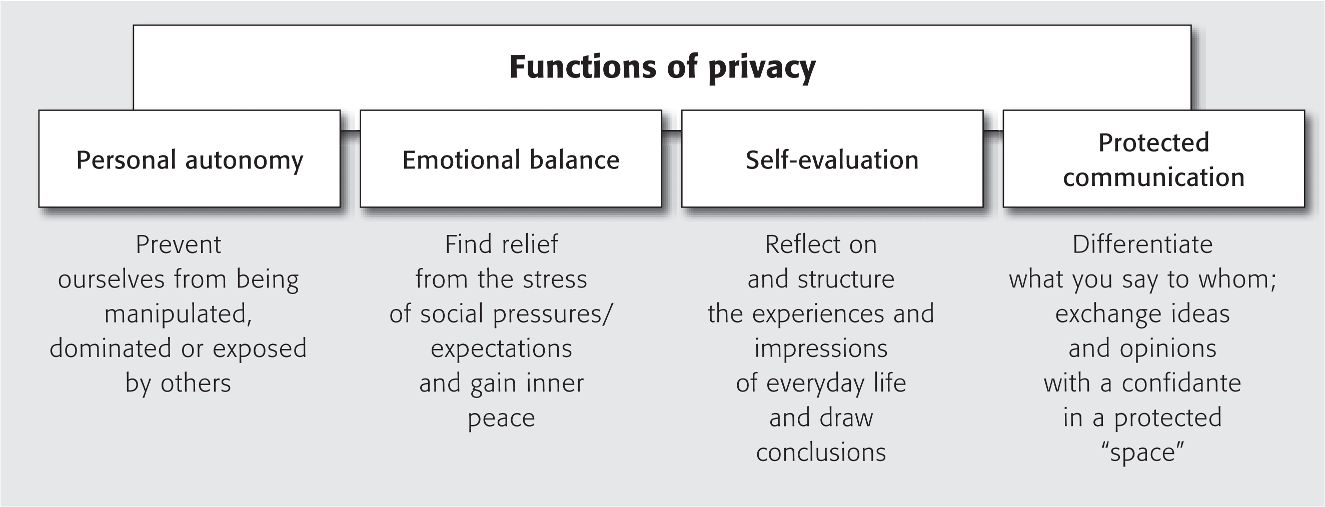
- Solitude: the situation of the individual in which he is alone and therefore unable to see or be seen by other people.
- Intimacy: the situation in a loving relationship or a small group of friends or family. The participants can speak freely to each other in an atmosphere of mutual trust.
- Anonymity: the freedom to go unidentified in public and therefore not be observed or controlled.
- Reserve: the most subliminal form of privacy. Describes a spiritual and physical detachment from others. Expressed, e.g. as forms of propriety when people share a confined space (such as a lift).

Through living together, humans have developed a range of different mechanisms for regulating privacy. These include cultural norms (e.g. standards of decency), the spatial design of living spaces (e.g. architecture), non-verbal (e.g. clothing) and verbal behaviours. The individual regulating mechanisms can vary from culture to culture.

The optimum level of privacy is not achieved by maximising the distance between members of a community (solitude or isolation). It is a dynamic process that varies according to the specific constitution and situation. Each individual has to find the ideal balance between two poles – the need for social interaction on the one hand and privacy on the other.

For Westin, privacy has another four central functions, which remain true today (see Fig. 5).

Privacy offers a protected space in which we can act independently of external influences – and can therefore authentically be who we want to be and act as we wish to act. Here we can think freely without restrictions, test ourselves and form our own opinions.



Functions of privacy

Personal autonomy	Emotional balance	Self-evaluation	Protected communication
Prevent ourselves from being manipulated, dominated or exposed by others	Find relief from the stress of social pressures/ expectations and gain inner peace	Reflect on and structure the experiences and impressions of everyday life and draw conclusions	Differentiate what you say to whom; exchange ideas and opinions with a confidante in a protected "space"

Fig. 5 The functions of privacy

1.3 Are we agreeing voluntarily to mass surveillance?

Privacy in the digital age

***Question for reflection:** How has privacy changed since the advent of the social web? What disadvantages could handing over private information have for me?*

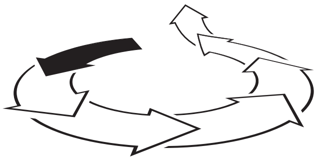
The protection of personal information has not just been a matter of public debate since the advent of Web 2.0 (social web). However, the potential availability of private information has never been greater because the essential requirement for participating in the social web is that you hand over personal data. Access to a broader public audience used to be impossible without the assistance of media institutions such as publishers, TV and radio broadcasters. Now everyone can participate and reach an audience of millions using Web 2.0. The fundamental conditions governing privacy have undergone a dramatic transformation.

Unlike verbal face-to-face communication, the information you provide on the Internet is published in a digital format. It is no longer fleeting and ephemeral but **enduring** and **available for a long time**. Users can **seek out** and **collate** this private information using search engines; it can be **reproduced**, copied and **removed from its original context** and applied to a different one.[4]

The **lack of social, spatial and temporal barriers** in the social web makes it difficult to maintain the integrity of social contexts. It is virtually impossible for the user to know how many people are able to view his personal data or who these people are – friends and family, acquaintances or complete strangers. Even if you rigorously apply the privacy settings for online networks or set up different groups of recipients in WhatsApp, it is still possible for data to be duplicated and passed on to other users against your wishes/ intentions. This unwanted audience can become a major problem. After all, there are often things we would tell a friend that we would not tell our parents – or say to our families that we would not say to our employer. We are different people in different contexts. We need these different social roles.

The privacy paradox
For several years, various programmes have aimed to raise awareness among young people, in particular, of the need for caution when handing over personal information. Moreover, the NSA affair has catapulted the topic of data protection into the public spotlight.[5] Yet the "privacy paradox"[6] is still very much in existence. In other words, users generally believe that it is important to protect their privacy but do not necessarily transfer this conviction to their actions. For example, a recent study of data protection behaviour when using apps concluded that "despite being clearly aware of the importance of security, there is still an obvious contradiction in user behaviours with popular social apps such as Facebook or WhatsApp. Over half of those surveyed (51%) were not willing to do without these apps despite their concerns about data protection".[7] Nor are the vast majority prepared to change their habits when using search engines. More than 90 % of users in Germany use Google despite all the well-documented criticisms of the company's data protection practices. Indeed, few were able to name any alternative search engines.

There are a number of possible explanations for this paradoxical behaviour. For example, there could be a lack of understanding about the protection technologies available or problems in using them. Or it could be the polar opposite: a digitally socialised generation believes that "it has got digital self-presentation under control. That it is possible to control the complex, digitally assembled mosaic image of ourselves that we generate."[8] Another significant motive could be a strong dependency on – even addiction to – the comfort and convenience provided by digital services and devices. But perhaps there is also a lack of awareness about the consequences of handing over data because the problems are too complex for the wider public to understand?[9]



"But I haven't got anything to hide."
"I have nothing to hide and therefore nothing to fear." This is a very popular argument – but it is wrong. Anyone can suffer if certain types of private information – e.g. about a serious illness – become public. It is easy to overlook or forget "that data does not communicate a fixed, objective and infallible picture. It is processed, linked and evaluated to produce a constant flow of new information. The picture that one person sees can look very different from the picture that the person in question himself believes to be correct. Furthermore, many people are insufficiently aware that they could attract the attention of the security services despite being innocent. They believe that surveillance only affects other people, such as terrorists."[10]

My identity belongs to me:
Control over your own identity
In order to protect your privacy in a digital, networked world, you must retain control over your private data. Beate Rössler's definition describes this very succinctly: "(…) a thing is private if you control access to it yourself."[11]

Privacy means "that I have control over who has access to knowledge about me, i.e. who has what relevant data about me. It also means that I can control, which people are authorised to contribute to or take action in the decision-making process for decisions that affect me." ***Beate Rössler,*** *2001, p. 24*

This form of control applies not only in a spatial sense but also metaphorically. I decide who knows what about me, when and in what context. Or as Steffan Heuer and Pernille Tranberg put it:

"If you want to protect your privacy, you must assert control over as many aspects of your identity as possible. We are the sum of the things that describe us – our qualities, our preferences and dislikes, our passions, genes, facial profiles, retina scans, speech patterns, circles of friends, Internet surfing behaviours and even the way we walk (...)." ***Steffan Heuer & Pernille Tranberg,*** *2013, p. 23*

2 Nothing to look for but plenty to find

Recognising the mechanisms used to reveal and collect data

Question for reflection:
Who gathers, processes and, potentially, distributes private data?

2.1 Hunters and gatherers

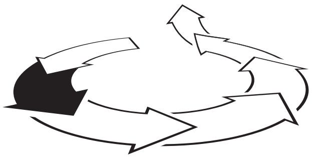
Data trails on the Internet
The data we freely provide in social media are just one element of the data trail we leave behind us wherever we go. These data trails are recorded, evaluated, used and/or distributed by – primarily commercial – data collectors. "In the context of data protection, this type of data collection (...) poses a much more profound problem. In combination with the distribution of (more or less consciously) freely volunteered (profile) information, it potentially has a wider dimension in questions of identity, complex aggregated information about a person, movement profiles etc."[12] If our Internet activities are subject to continuous monitoring, recording and evaluation, the World Wide Web – purportedly an instrument for promoting freedom, participation and transparency – is actually the exact opposite: an instrument of mass surveillance.

A recent study by the German Institute for Trust and Security on the Internet (DIVSI) also confirms that users still underestimate the extent and scope of data collection. "When they hear the word 'public', young people and young adults think primarily in terms of their peer group and their reputation with their network. They do not consider the possibility that their activities may be monitored by states, their data collected and read by corporations or stored by other institutionalised processes."[13] However, they are usually aware that their online activities are being tracked and the information used for personalised advertising. They have no objections to this. On the contrary, they see practical benefits.[14]

Users must be aware of the situations and circumstances in which they leave data trails and how data can be gathered. This is an essential step in helping them to assess the resulting risks to their own privacy. The following table provides an overview of data collectors in digital, analogue and networked environments (the Internet of Things; see Fig. 6).

Digital environments	Analogue environments	Networked environment / Internet of Things
• Social media • Search engines • Surfing (cookies) • Online shopping • Apps • Cloud computing • Smartphone/tablet • E-readers • ...	• State authorities (Police, financial authorities, security services) • Communication data (telephone, SMS) • ID papers • Customer loyalty cards • Credit cards • Health insurance cards • Video monitoring • Sat-nav devices • Toll booths • Flight data • ...	• Smart home • Self-tracking devices (e.g. fitness wristbands) • Smart cars • Smart clothing • ...

Fig. 6: Data collectors



More data is being gathered and stored about each and every one of us than ever before. One reason for this is that we and our digital surroundings are leaving an increasingly bountiful crop of data to harvest. Most importantly, the Internet has made it much simpler, cheaper and more useful to collect personal data. This information can be used to identify our hobbies, who we will fall in love with, our political opinions, whether we are likely to get divorced soon, have children or become ill. And it is derived from apparently harmless statements using algorithms. It is a threat to our privacy.

Video from the TV show Quarks & Co: "The daily data trail: how my digital self is created": ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-digitalesich100.html***

We are now being monitored continuously – even when we are not on the Internet. Every credit card payment, flight reservation you make at the travel agent and mobile phone you carry leaves a data trail. You may not be a member of Facebook but Facebook knows something about you from its members' address books. This allows the company to use its social network to create profiles about people who do not even have Facebook accounts. Moreover, as user devices become ever more intelligent, they can export data from our analogue to our digital lives, e.g. through video surveillance with integrated facial, speech and behavioural recognition technologies or RFID chips (Internet of Things).

The "Internet of Things" *is the term used to describe the networking of everyday objects and appliances via the Internet. This enables them to communicate with each other independently. To do this, they require a unique IP address for identification purposes. These objects collect, store and process information, e.g. about a person or an environment. Their programming, ability to store information, sensors and communication technology enable them to exchange information online and autonomously. They perform a variety of tasks for the user and can therefore optimise many areas of human life.*

2.2 A fatal attraction?

Today, we understand "big data" to mean primarily "data analysis that aims to gain new insights based on enormous data storage and evaluation capacity."
Thilo Weichert, *2013*

Big Data

Big Data is a collective term for the vast volumes of data produced everywhere – quantities far too large to be processed using standard storage and evaluation tools. It was the reason that companies such as Google and Yahoo developed tools like Google MapReduce or Hadoop, which are capable of processing huge amounts of data. The data does not even have to be organised in a database. It can be unstructured. These technologies consequently have the capacity to evaluate texts, photos and videos from social media. Internet companies have developed these programs because they themselves have the most data and a financial interest in exploiting it commercially.[15] In 2011, experts at the World Economic Forum in Davos described personal data as "the oil of today".[16] In the digital age "**all** data is considered valuable (...), and moreover as a commodity in itself"[17]. Personal data has now become the core business of many companies.

Video on "big data" by the State Media Authority of North Rhine-Westphalia (LfM): ***http://www.youtube.com/watch?v=otWN5o1C2Bc***

The intelligent evaluation of gigantic quantities of data derived from a variety of sources allows companies to gain many insights into users' interests and lives. They are able to spot statistical trends or patterns, rules or correlations between individual attributes. For example, they can predict future behaviours by correlating and evaluating past and present patterns of activity. Companies, organisations and states are extremely interested in these forecasts for many reasons: they can use them to provide early warning of potential dangers, minimise risks, save time and make profits. However, they can use them to exercise control and power.

In short, it is possible to extract value from information that may have been collected for entirely different purposes. This material was worthless until analysis, cross-referencing and reorganisation transmuted it into precious data.[18] Of course, processing destroys none of the data's value. It can be re-used any number of times for other purposes.

Video (Quarks & Co): "Partner search 2.0: How big data is becoming big business" ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-partnersuche100.html***

3 The end of privacy?

Confronting the risks posed by big data

Question for reflection: *What can happen to the private information you reveal – voluntarily or involuntarily?*

Tracking and **scoring** are the most important methods used to collect and evaluate personal data. Both are used to predict future behaviour by creating a profile for a person or a group. This lists their interests, consumption patterns, whereabouts, social contacts, credit ratings, credit worthiness, behaviour or health.

3.1 "Show me where you click and I will tell you who you are."

Tracking

Tracking follows the behaviour of a person using a specific attribute. For example, when a mobile phone is switched on – it need not be a smartphone – it creates metadata. This information such as the numbers you call, the number and duration of your phone calls and your whereabouts, is sufficient to generate a detailed profile and hence insights into your private life. It is not even necessary to evaluate the content of the communication.

On the Internet, tracking means that our surfing, use and consumer behaviours are being observed. Companies use cookies to collect information on websites. These little files follow us wherever we go in the Web and are mostly used for advertising and marketing purposes. The website gives each user an ID number, which identifies him whenever he visits the site. On average, visiting a website triggers 56 tracking processes, of which 40 percent are from major advertising networks. The aim is to be able to show the user tailor-made adverts from the moment he opens a website. This advertising is sold in milliseconds through online auctions powered by automated systems that run in the background.[19]

Now you could say, "Isn't it great that I am shown advertising that is specially designed to reflect my interests" or "I don't take any notice of the adverts. It doesn't make any difference to me." But that ignores some of the key issues because our surfing patterns say a lot about us and our lives – about our interests, worries, preferences or thoughts. “Show me where you click and I will tell you who you are.”[20] One French study[21] analysed the surfing patterns of nearly 370,000 Internet users. It showed that special software was possible to identify many users after they had visited as few as four websites. This is because 69 percent of us have an unmistakeable surfing history that is as unique as a fingerprint. If you are not protected against tracking, it is impossible to remain anonymous – and therefore protect your privacy – when surfing the Web.

When tracking data from the online world is also combined with tracking data from the “real” world (e.g. via credit cards, loyalty cards or bonus programmes), the knowledge of the subject becomes even more detailed and the opportunities for manipulation even greater. The quality of the analysis and the predictions depend entirely on the quantity and quality of the raw data that can be assigned to an individual – and the algorithms that evaluate this data.

Well sir, I could give you 10,000 contacts next week. Their “scores” have gone down really badly
What have you got for me?

▷ *Video: Quarks & Co shows the story of the pregnancy forecasts from TARGET researched by Charles Duhigg: “Till receipts as pregnancy tests”,* ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdatatalk-kassenbon100.html***

3.2 Big Brother is scoring you

Scoring
Scoring generates a numerical score for a person based on a mathematical-statistical analysis of past empirical data. This score is used to predict his future behaviour. It means that a person is assigned an individual score that expresses a predicted future behaviour.
It applies specifically to him. Scoring assumes that **people with comparable attributes** will behave in similar ways. For example, possessing even a small amount of data about a person – such as his address – allows a company to make a risk assessment.
This can relate to many different areas of human behaviour: workplace performance, predicting criminal behaviour or forecasting a person’s future state of health. The most common and best-known type of score is used to estimate the probability that a person will pay a bill or repay a loan, e.g. performed by credit rating agencies.

Today, credit agencies are just one of many sources of information used to generate risk profiles and individual prices for customers. For example, the insurance company Axa Global Direct has said that it uses around 50 variables to calculate individual premiums – including browser cookies, shopping patterns or party entries on Facebook.[22]

3.3 The measurement of mankind

Profiling and classification

Companies use our data to measure, evaluate and classify us or even to generate comprehensive profiles. They can divide us into good and bad customers, set individual prices or premiums, judge our creditworthiness, forecast our needs and patterns of behaviour, deny us an insurance product or offer it to us at less advantageous conditions. Our data can also be used to determine our political and religious dispositions, health, sexual preferences and even emotions and moods. As a result, companies and organisations that possess this data have a wide range of options for **manipulation, discrimination, social control** and **surveillance**. However, while their options expand ours diminish as we face greater **restrictions on our freedom to make our own decisions and act accordingly**.

What happens when a potential employer no longer takes the trouble to meet a job applicant in person because he feels he has already found out all the relevant details via Facebook? It is well-known that many employers use applicants' Facebook profiles to help them select the most suitable candidates. One study[23] has now shown that information taken from Facebook profiles can predict the performance of job applicants more accurately than traditional aptitude tests. Likewise, tweets could give a Head of Human Resources further insights into a candidate's personality – analysis of factors such as style, form of address and topics of interest could reveal whether he is unstable, extrovert, open to new ideas, agreeable or conscientious. With all this information available, does a personal impression really count for anything?

Many of us make our own contributions to perfecting this profiling and classification process. We freely hand over valuable and very personal data: about our fitness and health, the number of steps or distances we have walked, our speed, heart rate, body temperature, calorie consumption, rest phases etc. Wristbands or shoes fitted with sensors – so-called fitness trackers and the corresponding smartphone apps have become part of daily life for many amateur sportsmen and women. Many people enjoy comparing their performance with that of others and getting feedback about their own activities from competitors or friends. They see nothing strange about sharing their sporting achievements with the rest of the world. However, this recorded data could also change our entire health system – if continuous recording of health information were to become the norm in order to save money for health insurers.

... the vision is forming. I can see that the groom will give the bride a pale blue convertible as a wedding gift, both will go to Bermuda for their honeymoon and in 9 months they will have their first child because they have stopped using birth control ...

3.4 We know who you are! The "big four" Apple, Google, Facebook and Amazon

Four giant American corporations dominate the Internet business: Apple, Google, Facebook and Amazon. Although they offer products and services around the world, all four see themselves as American companies. One reason for this is that consumer and data protection are more relaxed in the USA. This makes it very difficult to enforce the more stringent consumer and data protection laws that apply in Europe.

More than 800 million people regularly use Facebook. The company now also owns further services such as WhatsApp or Instagram. Facebook's success is based on the "social graph", which shows who your friends are, what music you like, which articles you have read, where you are right now, where you like to go on holiday or your latest "Likes!" – what you currently find interesting on the Internet. Advertising campaigns on Facebook run by third parties use this information to tailor their adverts to the individual user. It is unclear in what other ways the company uses its user data. However, Amazon recently agreed a contract with Facebook, which will enable it to optimise its recommended purchase system with the help of the social graph.[24]

"We know where you are. We know where you've been. We can more or less know what you are thinking about right now." This is not the statement of a chief of intelligence or a dictator but of Eric Schmidt, CEO of Google.[25] Google knows a great deal about its users and not just because of its quasi-monopoly position in the search engine market (70% of global market share). Google is also the owner of YouTube, the world's largest video sharing platform; Android, the world's most important operating system for mobile devices (and soon in gaming consoles, TVs, cars and cameras); Chrome, which is now the world's most popular browser: and Gmail, the world's most widely used email service in which all emails can be automatically searched by Google. Market leadership in all these areas has led to an unbelievable concentration of power as Eric Schmidt confirms in his book "The New Digital Age"[26]:

"We believe that modern technology platforms, such as Google, Facebook, Amazon and Apple, are even more powerful than most people realize (...), and what gives them power is their ability to grow – specifically, their speed to scale. Almost nothing, short of a biological virus, can scale as quickly, efficiently or aggressively as these technology platforms and this makes the people who build, control, and use them powerful too."
***Eric Schmidt,** 2013*

Since making changes to its data protection provisions in March 2012, Google has been able to evaluate the data it collects about its users across all its services and thus build up a comprehensive picture of every area of their lives. Data protection campaigners are taking action against these provisions. Google argues that it only does this with the agreement of its users. The problem is that most users do not (or cannot) know what information they are handing over and what will happen to it in future. But even if they do not use Google products, Google can still collect information and data about them – via third parties who use Gmail, a Google contact list or Google Calendar. This undermines the fundamental right to self-determination in the area of information.

▷ *Video: LfM Digitalkompakt "Apple. Google. Facebook. Amazon."* 🖱 ***https://www.youtube.com/watch?v=h2hiuzTjegg***

4 My life belongs to me!

Reflecting on the consequences of breaches of privacy

Question for reflection: *What are the possible consequences of revealing personal data – voluntarily or involuntarily?*

The risks posed to our private lives by digitisation fall into two categories:

❶ Risk of breaches resulting from information published by me or by others about me on the Internet – usually direct communication partners or people whom I expect to have access to this data (see 4.1).
❷ Risk of breaches resulting from uncontrolled use of private data by commercial data collectors (see 4.2).

4.1 No right to be forgotten?

Damage due to the revealing of private information
The risks of individual breaches of privacy in social media are principally due to the distortion and uncontrolled distribution of information by or about us. The abuse of this data can lead to bullying, stalking, identity theft, insults, humiliation or serious damage to your reputation (which could, e.g. hinder your career), minimise your opportunities (e.g. of getting a job) or result in discrimination (e.g. due to looks or appearance).

Your privacy is compromised if people gain insights into your private thoughts and actions against your wishes. Other people can use this information to observe us, make judgements about us and spread this information whether they know us personally or not. This makes it virtually impossible to manage and control your own image – i.e. to decide for yourself how you want to define and present yourself to the world

Yet every individual should have sovereignty over his own life. Protection against the uncontrolled use of private information – protection of privacy – is essential to the formation and development of an identity and hence to living responsible and independent lives.

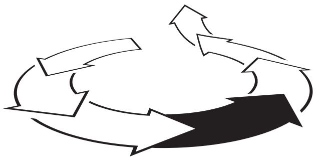
This includes the right to decide, which life events we want to share with other people who may make moral judgements about us – in other words, the right to decide freely, which life plans, roles and values are recognised as “the right ones” for us. This could be described as the right to “experiment in life”[27]. However, the typical attributes of data – its persistence and the ease with which it can be searched, copied and classified – make it possible to match data from the past and the present. As we develop as people, we inevitably make mistakes. We should have the right to decide whether we want these mistakes to be kept secret or revealed to and judged by others. Adolescents, in particular, need to have the opportunity to test boundaries, find their own way and experiment with roles. The opinions they express in this phase – and post on their profile pages – may very quickly cease to reflect their systems of values and approaches to life. Removing the individual’s right to decide for himself what should be remembered and forgotten hinders him in creating his identity.

4.2 Think big: Big Data, Big Power, Big Business

Breaches of privacy by big data
The consequences of intrusions on our privacy by big data can be characterised and summarised in three concepts: **big data, big business, big power** or **classification, commercialisation** and **surveillance**.

Replaced by a digital doppelgänger

Classification
Classification by big data divides people into groups and assigns them scores – e.g. for credit agencies or insurance companies. This process de-personalises the individual and forces him to conform to defined criteria. Above all, in order to evaluate a person’s behaviour it is vital to know the behaviour of many, many other people who act in similar or identical ways according to specific characteristics. Even so, their personalities could still have very little in common.

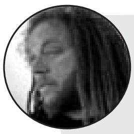


Big data judges people based on their predicted preferences – and not on their actual behaviour. This restricts our opportunities to behave in unexpected ways and shape our own futures. Our previous actions are never forgotten because they are used to make predictions: so we can never escape our own past. Most importantly, the predictive analytics used by big data actually endanger our freedom to act independently and make our own decisions.

There is a further problem. Our data trails and inputs are used to form digital versions of ourselves, which we can never get to know. These "digital doppelgängers" are not exact copies of us – but they do represent what commercial companies and security agencies know about us. "For the original human being, there is something deeply disturbing about this 'personal' data twin. Not just because he is invisible but also because he is a chimera of original and alien information. His 'body of data' is born from the living person and his search patterns; but his 'character' and 'soul' are defined by the Internet industry – by external views, external interests, external profilers."[28] What remains of the man if he is judged by data alone? Digital data collection cannot authentically record the complexity of moral outlooks, human activities and the myriad other factors that truly define a person.[29]

When we also remember that the basic data may be incorrect or of poor quality, analysed incorrectly or used misleadingly – and that we have no way of correcting this – the implications become horrific.

"You are the product!"



"You are not the customer of the Internet companies. You are their product."
***Jaron Lanier,** 2014*

Commercialisation
All our data is evaluated on behalf of advertising customers. In reality, we pay for products and services by offering a detailed view of our behaviours, preferences and interests. Ultimately, we pay with our identity. It is a high price for the supposed "free-of-charge" culture of the Internet.

Many aspects of our lives play out in the social web. We should therefore be concerned that private activities and statements should be continuously subject to commercial interests and that Internet companies now have such a major role in our lives. As Evgeny Morozov emphasises, we should not be discussing the merits of the technology but the practices of Internet companies.[30]

"I am not a critic of technology. I criticise the monopolisation of power by technology – and our naive approach to it."
***Evgeny Morozov,** 2014*

The dilemma is highlighted by the fact that we legally consent to our data being used in this way when we agree to the company's terms and conditions. After all: if we do not agree, we cannot use the service. Yet it is extremely rare for the user to have any idea what the consequences of his consent may be – even if he is not fundamentally against the commercial use of his data. In many cases, the purposes for which the data will be used have not been determined at the time of collection. Or the data may be re-used later for new purposes. Moreover, the terms and conditions may change – thereby fundamentally altering the rules that govern the ways it may be used. And when this happens, what happens to the data that was previously collected under the old terms and conditions?

The dictatorship of algorithms

Surveillance

Very few people know how much data about us is circulating in the Internet nor the conclusions that companies draw from it. Big data is capable of continuously monitoring, documenting and evaluating every aspect of our online behaviour – and can therefore restrict the freedom of every individual. We must always view the argument that we have nothing to fear if we have nothing to hide with general suspicion. After all, "the nature of freedom is precisely that I am not obliged to reveal everything about myself but have a right to discretion and even secrets – that I myself can decide what I want to reveal. These rights are essential to democracy. Only dictatorships want (…) mass surveillance."[31]

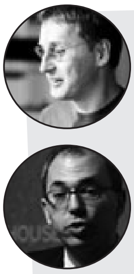
The fact that data is being gathered continuously can lead people to restrict on their own behaviour to prevent themselves being noticed. The German census verdict has already acknowledged this fact: "If citizens are unsure whether deviant behaviour is being monitored and recorded in a persistent form as information that is used and passed on to third parties, they will try to conceal or suppress this behaviour in order to avoid attracting attention." Always behaving as one of the crowd, suppressing your own opinion or even refusing to make contact with people who express critical political opinions would have fatal consequences for a democracy founded on freedom of speech and autonomy. It would trigger a spiral of silence and self-censorship in the digital age.

Even making data **anonymous** no longer offers adequate protection because big data increasingly has the capability to re-identify the person associated with the anonymous data by using more and more diverse data. Even the most harmless piece of information can reveal the identity of a person if the analysing system has gathered enough data.[32]

4.3 The return to autonomy

A new paradigm?

Correlations are the new paradigm for generating knowledge in the digital age. They are the key for making evaluations and predictions. For Alexander Filipovic, this creates an ethical problem. "To me, it seems clear that as we put more trust in the power of big data, we also put more trust in correlations rather than theories, socially negotiated and agreed interests, insights and demonstrable facts. Correlations are not bad in themselves. For example, translation programs based on correlations are much better than those that stick to grammatical rules. But if the goal is to predict phenomena through human behaviour – a suitable target for big data analyses – we will systematically compute freedom of action and autonomy out of human behaviour."[33]



"These approaches are just the beginning. They must be resisted because they lead directly (...) to a world in which freedom of will and the freedom to make our own choices no longer exist; in which our moral compass has been replaced by predictive algorithms; and in which the individual is exposed to and unprotected against the will of the collective. If used in this way, big data literally threatens to make us prisoners of probability."
Viktor Mayer-Schönberger & Kenneth Cukier,
2013, p. 206

5 What is more important to me?

Discussing conflicts of values

***Question for reflection:** What conflicts of values can you see in protecting your own privacy?*

So far, it has already become clear that privacy is an essential factor in developing our own identity, protecting the autonomy of the individual and ensuring personal integrity in modern western culture. The expression of liberty – a mature and independent lifestyle – is therefore only possible under conditions in which privacy is protected. We need private spaces in both the literal and metaphorical senses because they are the only places where we can shape and assert our autonomy.[34]

In summary, when we protect our personal data we protect our own privacy – one of the foundations of our freedom to act and make our own decisions. However, these important and necessary steps for self-protection can compete with other wishes and lead to conflicts of values:

Conflicts of values

1. **Self-protection vs. self-expression**
   Self-protection can conflict with our desire to express ourselves and experiment (different roles).

2. **Self-protection vs. social recognition**
   Self-protection can conflict with our desire for social recognition, participation and connectedness (integration).

3. **Self-protection vs. incentives**
   Self-protection can conflict with our desire to use free services, bonuses and discounts.

4. **Self-protection vs. utility and convenience**
   Self-protection can conflict with our desire to be in touch with everyone at all times, stay informed (while travelling) or use other forms of "digital support".

5. **Self-protection vs. entertainment**
   Self-protection can conflict with our desire to be entertained (e.g. YouTube, music streaming services).

6. **Self-protection vs. sharing**
   Self-protection can conflict with our need to share apartments, cars, parking spaces, services etc. with other people.

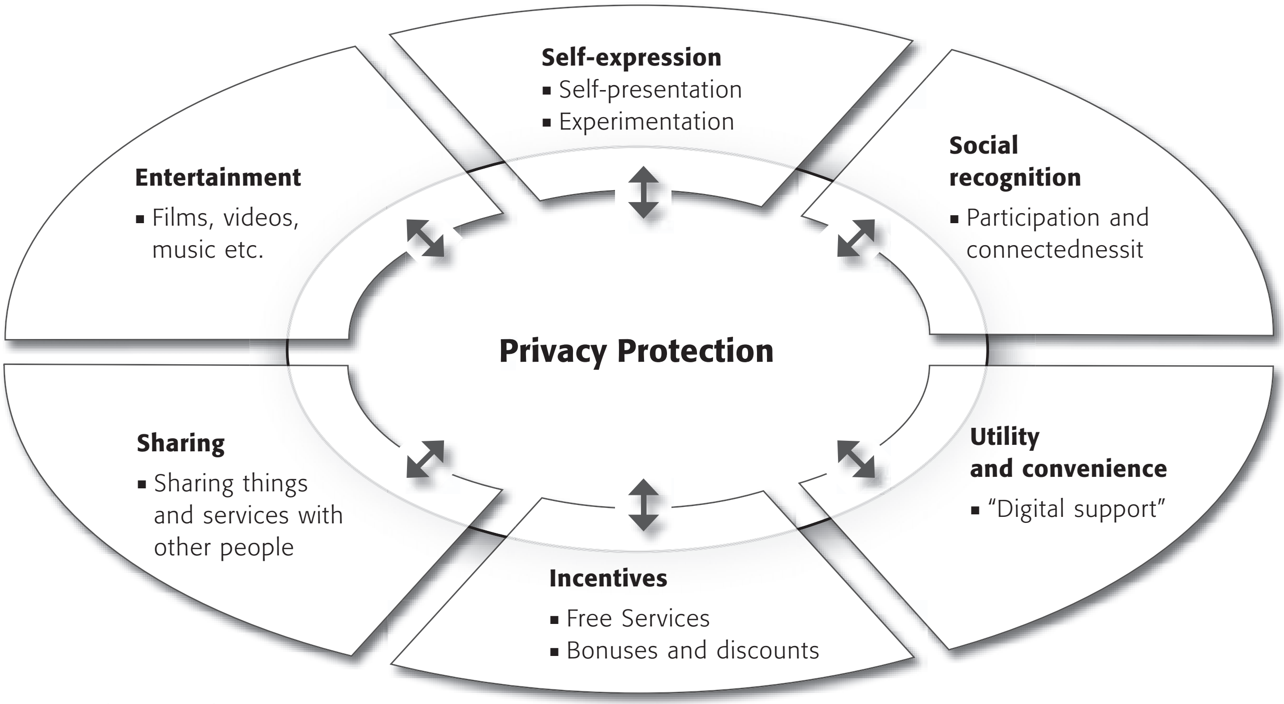
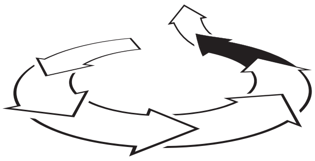


Fig. 7: Conflicts of values



6 Privacy as a human right

Developing an ethos of privacy

Question for reflection: *Why is privacy good, desirable or worth protecting? What has it got to do with the development of an autonomous and free citizen?*

There are many indications that privacy is in crisis. Yet there is still a consensus that privacy is an instrumental value and cultural achievement because it is closely linked to the image of modern humans as autonomous, free and equal citizens. For example, the information ethicist Rainer Kuhlen believes that privacy is still very highly valued despite the tendencies towards relativism that clearly exist: he even states it as a human right.

> *"Privacy is undoubtedly a human right, one of the codified collection of basic rights and freedoms for all people. Even if privacy is unimaginable without its connection to western systems of values, commerce and democracy, privacy is now a universal aspiration. Against the backdrop of a radically changing media landscape, it is being defended primarily through the principle of the individual's right to determine the way that his personal information is used. This is legally implemented as a right to data protection. (...) However, for many reasons, we can also see an unmistakeable tendency to relativize the high status that privacy enjoys, e.g. anticipated economic advantages, acceptance of supposed improvements in security or simply ambivalence or ignorance"*
> ***Rainer Kuhlen,*** *2004, p. 193 f*

For Rössler (2001) and many others[35], privacy is an instrumental value, which is a necessary requirement for and expression **of autonomy**. According to Rössler, adopting a relativistic attitude towards privacy would strike at the foundations of our democracy. "It would not only affect the idea of a successful – self-determined – life but also the idea of a liberal democracy, which depends on citizens who are autonomous, aware of their own autonomy and know its value."[36]

In a liberal democratic society such as Germany, the importance of privacy is also enshrined in its laws. These laws are based on the individual's right to determine the way that his personal information is used. Modern data processing puts our **freedom of self-determination and self-expression** at risk. If citizens do not know or cannot influence how information about their behaviour is saved and archived for future reference, they will become cautious and adapt their behaviour. This phenomenon is known as "chilling effects": pre-emptive, self-restricting action due to the fear of possible consequences. This does not merely harm **the individual's freedom to act** but also the **general well-being** of the population. A liberal, democratic community depends on the participation of its citizens. They must not live in fear of surveillance or being disadvantaged because of their involvement. Lawmakers also see a close connection between the protection of data, protection of privacy and healthy democracy.

Data collection classifies each person based on correlations to create a "digital doppelgänger". This provides a basis for making – or even withholding – special offers and options. It does not record users as individuals but as data puzzles. These can be quantified and capitalised. Moreover, there is an **information asymmetry** between the users and the data collectors. Users do not know the context in which the data was gathered or context in which it is used. Nor do they know the algorithm used to classify them (**lack of transparency**). The private data often voluntarily supplied by users (or required by providers) is correlated to create a digital doppelgänger and "interpreted" using formulae that are completely lacking in transparency.

From an ethical viewpoint, we should also ask whether the objectification and capitalisation of people as digital doppelgängers is reconcilable with the notion of human dignity. According to Kant, "**dignity**" and "price" are opposites: while objects have a price and can be exchanged, human beings have a dignity that cannot be purchased at any price.[37]

"In the realm of ends, everything has a price or it has dignity. Whatever has a price can be replaced by an equivalent while whatever is above price has dignity."
***Immanuel Kant,** 1786/1999, p. 61*

7 What can we do?

Identifying options and tools for taking personal, political and instrumental action

***Question for reflection:** What can people do to protect their privacy? What should government, politicians and companies do?*

We would like to propose a four-point programme of ethical recommendations in order to create a balance between the achievements of digitisation and the protection of privacy (see 7.1–7.4).

7.1 Digital self-defence

We must anchor an understanding of the importance of privacy in the education system and public debate. We must teach people its value. We must also expose the high risks associated with the frequently used argument "I have nothing to hide". The following skills could be used to assess **competence in the area of digital privacy**:

- The ability to reflect on why private data should be considered worth protecting (**ethical competence**)
- The knowledge of who collects, processes and passes on private data and for what purposes (**structural competence**)
- The ability to estimate the potential consequences of publishing private data (**risk competence**)
- The knowledge or data protection guidelines and possible means of protection (**legal and technical competence**).

The first steps towards digital self-defence: always use the correct privacy settings in networks; delete your browser history and cookies permanently; use StartPage or lxquick – one of the search engines based in the Netherlands – instead of Google; use an encrypted email services instead of Gmail (e.g. from Telekom or United Internet); use the messenger Threema instead of WhatsApp and deny free apps access to your data.

Quarks & Co-Video: "Secure data: Tips for data protection on the Internet" ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-tippszumdatenschutz100.html***

7.2 Political activism

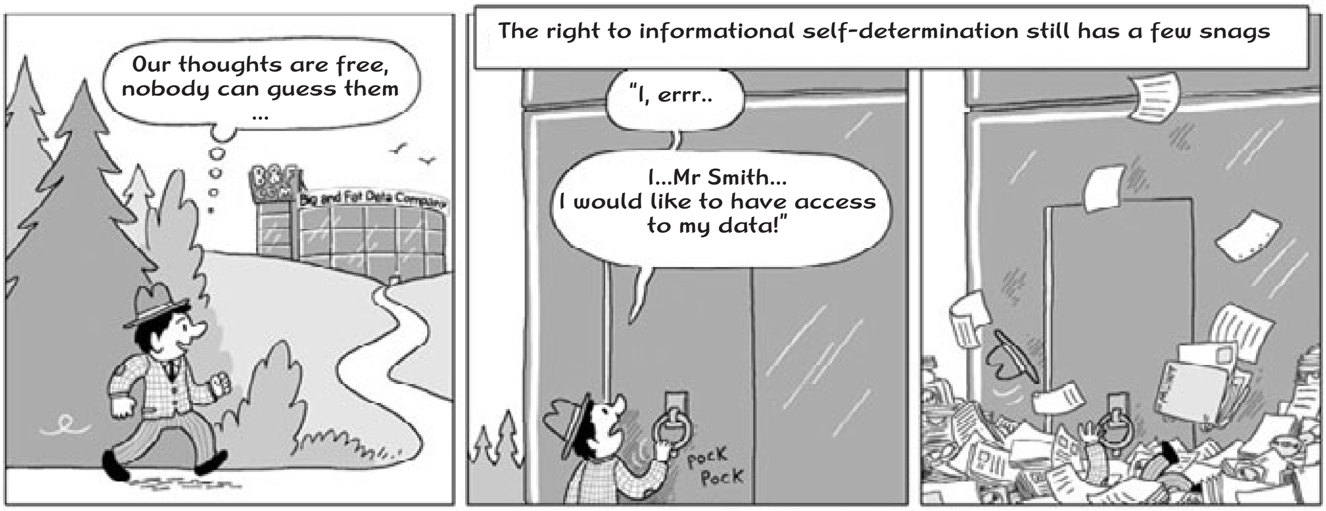
Digital self-defence is just the first step in the battle against the big data collectors. The ethical questions arising from the misuse of private data and blind trust in algorithms clearly show that this is not a discussion about technology. It is a social debate. Citizens must decide whether they wish to subordinate their entire lives to efficiency criteria, constant surveillance, second-by-second analysis and determination of their behaviour by software programs. They can do this through participating in politics and becoming political activists (demonstrations, petitions, civil rights movements). For example, citizens could campaign for the new EU data protection regulations, which were announced in January 2012 but have not yet been passed. This data protection law would also put limits on the activities of US companies such as Google or Facebook because it would give all EU residents the right to see the data that has been collected about them and delete it permanently if they wish. This is known as the "right to be forgotten". The new law would also introduce greater accountability for all processors of personal data.[38]

7.3 Big-Data-Kodex

In principle, data sets are neither good nor bad. However, current developments in digital networking, security and surveillance technologies make it clear that **big data**, above all, translates into **big power** and **big business**. Wherever possible, companies, governments and public organisations should therefore undertake to act in accordance with the principles of **proportionality** (earmarking), **information equality** and **fair access**. They should also make it clear which algorithms they are using and "continuously check and validate the selection and quality of input data"[39].

7.4 Privacy by Design

One of the key requirements during the design phase of new technologies, products and networking systems should be to minimise the amount of data they use that is worth protecting (data efficiency). They should also provide transparency about how they intend to use the data and the third parties to whom they plan to send it. They should also offer users easy-to-use default settings that enable them to protect their data effectively even if they have no specialist IT knowledge (**privacy by default**). To achieve these aims, we must raise awareness of ethical considerations among developers from the earliest stages of their education and training. The three-I's concept –fairness of access to information, information equality and information autonomy – should be established as the categorical imperative of privacy for companies and state institutions.


Our thoughts are free, nobody can guess them ...
B&F
Big and Fat Data Company
The right to informational self-determination still has a few snags
"I, errr..
I...Mr Smith... I would like to have access to my data!"
POCK POCK

Links and further information

Further reading

Rössler, Beate (2001): *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp Verlag.
Heuer, Steffan/Tranberg, Pernille (2015): *Mich kriegt ihr nicht! Die wichtigsten Schritte zur digitalen Selbstverteidigung.* 3. Aufl. Hamburg: Murmann. – Twitterfeed zum Buch: @MeinDatenschutz
Grimm, Petra/Zöllner, Oliver (Hrsg.) (2012): *Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten.* Schriftenreihe Medienethik, Bd. 11. Stuttgart: Franz Steiner Verlag.
Mayer-Schönberger, Viktor/Cukier, Kenneth (2013): *Big Data. Die Revolution, die unser Leben verändern wird.* München: Redline.
Broschüre *"Kleine Daten, große Wirkung"* aus der Reihe Digital Kompakt der LfM www.lfm-nrw.de/nrwdigital/digitalkompakt.html

Novels on this subject

Eggers, Dave (2014): *Der Circle.* Köln: Kiepenheuer & Witsch.
Elsberg, Marc (2014): *Zero.* München: Blanvalet.

Studies and reports

Christl, Wolfie/Winter, Renée/Schweinzer, Barbara (2013): *Collecting, Collating, and Selling Personal Data: Background Information and Research.* Online: http://datadealer.com/datadealer_backgrounds_research.pdf

Websites and articles

Artikel "Das Ende der Geheimnisse": http://www.zeit.de/2007/11/Geheimnis
Artikel "Für Algorithmen ist jeder verdächtig": http://www.zeit.de/digital/datenschutz/2013-06/mustererkennung-algorithmen-terror
Online-Animation zum Thema Überwachung: http://panopti.com.onreact.com/swf/
Selbstdatenschutz und digitale Selbstverteidigung. Datensparsamkeit, Datenschutz und Verschlüsseln in Eigenregie: http://www.selbstdatenschutz.info/home
Institut für Digitale Ethik (IDE) (Hrsg.) (2014): *Das Internet der Dinge. Der vernetzte Alltag im Jahr 2030:* http://www.digitale-ethik.de

Films, adverts and other media

Film *Big Data* (LfM): http://www.youtube.com/watch?v=otWN5o1C2Bc
Film *Mobile Payment – Die Zukunft des Einkaufens* (LfM): http://bit.ly/102ok8j
Film "Der gläserne Deutsche": https://archive.org/details/Der_glaeserne_Deutsche
Beitrag "Das Internet der Dinge – Die Macht der künstlichen Intelligenz" von Edith Lange und Carola Wittrock aus der Sendung ttt – titel, thesen, temperamente vom 30.03.2014: http://www.daserste.de/information/wissen-kultur/ttt/sendung/hr/2014/sendung_vom_30032014-102.html
"Das Netz – die große Falle?" Peter Voß fragt Frank Schirrmacher. 3sat, 27.01.2014: http://www.3sat.de/mediathek/?mode=play&obj=41271
Viktor Meyer-Schönberger auf der Republica 2014 zum Thema Freiheit und Vorhersage: *Über die ethischen Grenzen von Big Data:* http://www.youtube.com/watch?v=XRPFSbxybxs
Anschauliche Präsentation zum Thema Big Data: http://www.jakkse.com/big-data-big-brother-folien-von-meinem-vortrag-bei-am-puls-im-albert-schweitzer-haus/

Work in schools

Das Online-Spiel "Data Dealer" beschäftigt sich mit den Praktiken der Datenerhebung und des Datenhandels: http://demo.datadealer.net/
Das PRISM-Rollenspiel zum Datenschutz für den Unterricht: www.lehrerfreund.de/schule/1s/datenschutz-prism-spiel/4407

Projects and activist associations

Big Brother Awards – Die Oskars für Datenkraken: www.bigbrotherawards.de/2014

Media ethics roadmap with questions for reflection on "Privacy and big data"

1 Raising awareness of the importance of privacy

1.1 Definition
What do I understand by "private/public"?
What would I describe as being "private" and "public"?

1.2 Forms and functions of privacy
What are the forms and functions of privacy?

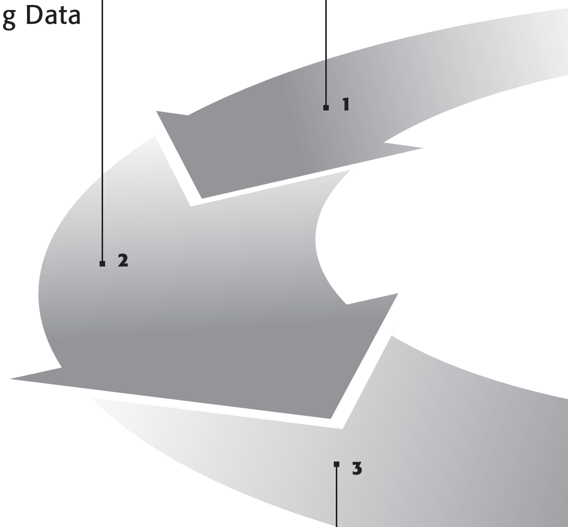
1.3 Privacy in the digital age
How has privacy changed since the advent of the social web?
What disadvantages could handing over private information have for me?

2 Recognising the mechanisms used to reveal and collect data

Who gathers, processes and, potentially, distributes private data?

2.1 Data trails on the Internet

2.2 Big Data



3 Confronting the risks posed by big data

What can happen to the private information you reveal – voluntarily or involuntarily?

3.1 Tracking

3.2 Scoring

3.3 Profiling and classification

3.4 The "Big Four" Apple, Google, Facebook and Amazon

7 Identifying options and tools for taking personal, political and instrumental action

What can people do to protect their privacy?
What should government, politics and companies do?

7.1 Digital self-defence

7.2 Political activism

7.3 Big data codex

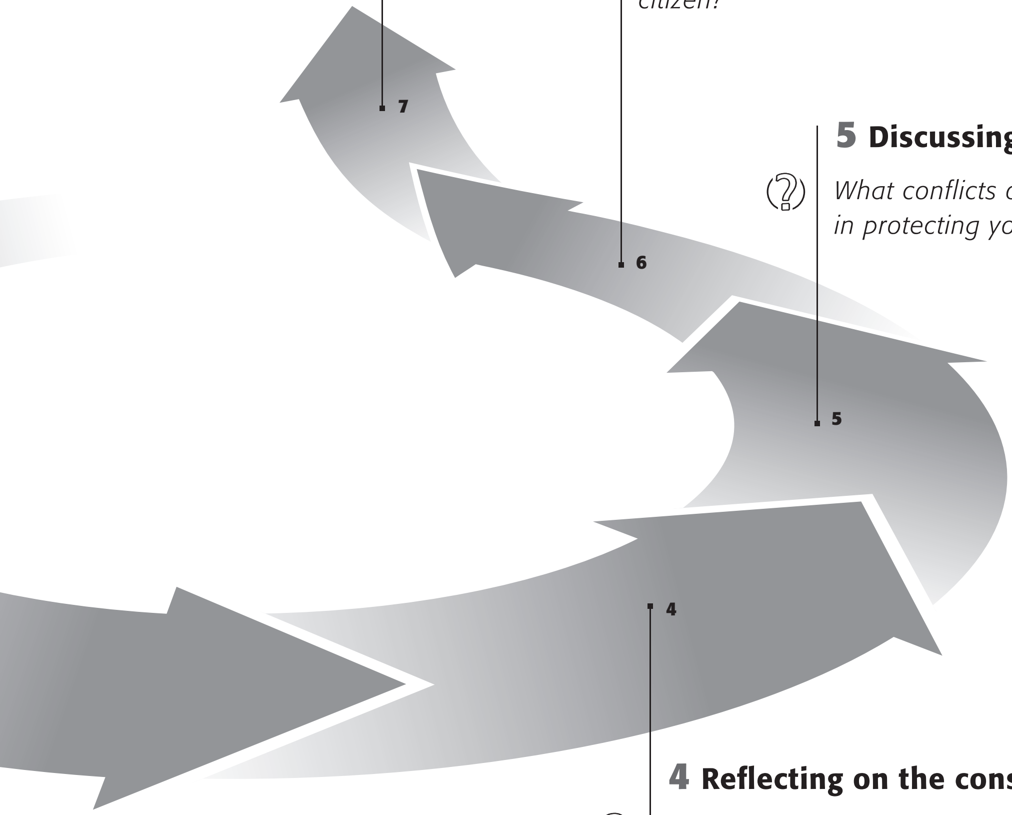
7.4 Privacy by Design

6 Developing an ethos of privacy

Why is privacy good, desirable or worth protecting? What has it got to do with the development of an autonomous and free citizen?

5 Discussing conflicts of values

What conflicts of values can you see in protecting your own privacy?



4 Reflecting on the consequences of breaches of privacy

What are the possible consequences of revealing personal data – voluntarily or involuntarily?

4.1 Damage due to the revealing of private information

4.2 Breaches of privacy by big data

4.3 A new paradigm?

Teacher's notes on the method – Overview of the projects

▶▶● **Intermediate difficulty (from 14 years)**

Pro-jekt	Titel	Competences	Methods	Materials	Time	Internet /PC access
1	**Privacy – What is it good for?**	Students are able to identify the value of privacy and explain the consequences of breaches of privacy.	Scale, scenario method "What if …", master copy "Statutory protection of privacy"	Cards (3 per student)	45 min	No (possibly show Stasi example)
2	**Tell me what you buy and I will tell you who you are.**	Students identify the profiling strategies of the consumer industry.	"Black story", discussions with partners	Film "Verräterischer Kassenbon" (The Treacherous Receipt)	45 min	No (show film)
3	**Big Data – Big problem?**	Students are able to identify the opportunities and risks of big data.	Role play, mind map	Trailer "Data Dealer", make films on "big data" available to students, role play cards, additional worksheets "Internet of Things" and "Surveillance"at www.klicksafe.de/medienethik	60 min	No (make videos available)
4	**How should I decide?**	Students learn to analyse difficult situations and make decisions based on the values they consider important.	Discussion of values	Cards, Sample dilemmas – cut out examples	45 min	No
5	**Activists wanted!**	Students learn about the action they can take to protect fundamental digital rights.	Group work	Task cards, help cards	60 min	Yes (for all groups)

You can find additional projects for this module at 🌐 **www.klicksafe.de/medienethik**.

Description of Project 1: Privacy – What is it good for?

Competences

Students are able to identify the value of privacy and explain the consequences of breaches of privacy.

Time

45 minutes

Methods

Scale, "What if …" scenario method, master copy for "Statutory protection of privacy" available at **www.klicksafe.de/medienethik**

Materials

Post-its (3 per student)

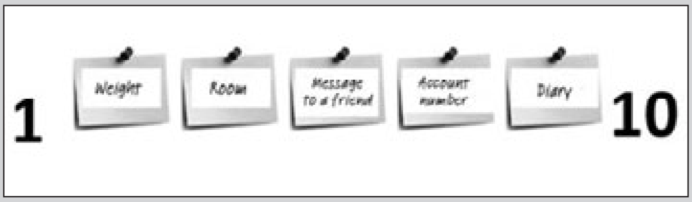
Internet/PC Access

No (possibly show Stasi example)

Introduction

Show the students something "private" (e.g. your wallet/purse) or be even more provocative: ask one of your students for his/her smartphone and its access code. "Why would you refuse to give that device and information to a stranger, for example?" It would be a problem because it is "private", i.e. it contains information that you want to control and protect.

Seated in a circle: Ask each student to write down three things that are private for him or her on 3 post-its. The examples can come from any area of life. Prepare some post-its with interesting examples (e.g. sexual orientation, account number) in case the students have difficulties coming up with examples of their own. Ask the students to read out a few examples and then arrange these according to the degree of privacy along a scale of 1–10 on the floor or the board (1= least private, 10 = very private). This enables the class to identify and discuss particularly private situations. **Evaluation questions:** Of these private things, how many are digital (as a proportion)? What do you think your grandparents would have written down?



Example of a privacy scale.
Source: klicksafe, own image

Elaboration

What would happen if private information were public information? Students consider the consequences of breaches of privacy using the scenario method. They can do the exercise at tables with partners or – if you prefer to remain in the circle – create possible scenarios for their own examples.

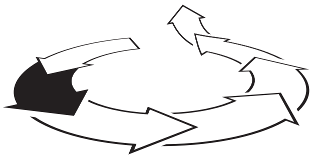
Scenario method: *What if...* the things the students classified as very private in the introductory section were no longer private but public? Ask the students to describe the possible consequences. *"If everyone could read your diary, everyone would know your most intimate thoughts and secrets. They could use this knowledge against you."* Expand on the possible negative consequences, e.g. exclusion, bullying, humiliation, blackmail.

Can the students think of further examples of breaches of privacy? Conversely, what is privacy good for? Work together to define the **functions** of privacy: protection, autonomy, self-determination (see information in section 1.2 Forms and Functions).

Anchoring

Make it clear that privacy is protected by law in Germany, e.g. by the "right to informational self-determination" (you can download the worksheet "Legal protection of privacy" at **www.klicksafe.de/medienethik**). This has not always been the case. A report about house searches by the Stasi is one powerful example of intrusions into privacy that you can show students at the end of the module: http://bit.ly/1uowIMY. **http://bit.ly/1uowIMY.**

Additional activity/homework:
"But I have nothing to hide!". Why is this statement a dangerous fallacy? See section 1.3 Privacy Paradox or **www.datenschutzbeauftragter-online.de/datenschutz-antrittsvorlesung-michael-schmidl-informationelle-selbstbestimmung-theorie-praxis/5594/** Chapter I. The Importance of Informational Self-Determination



2 Recognising the mechanisms used to reveal and collect data

Description of Project 2: Tell me what you buy and I will tell you who you are.

Competences	**The students identify the customer profiling strategies of the consumer industry.**
Time	45 minutes
Methods	"Black story", discussion with partner(s)
Materials	Film: "Verräterischer Kassenbon" (The Treacherous Receipt)
Access to Internet/PC	No (show film)
Introduction	Ask the students the riddle below – based loosely on the card game "Black Stories" – in order to awaken their curiosity in the following story. A father asks his daughter *"Why didn't you tell me you were pregnant?"* How did he find out? Methods: A "black story" You describe a usually odd situation. The students have to reconstruct the story behind the situation. To do this, they ask questions that you may only answer with "yes" or "no". Solution: Show the film "Verräterischer Kassenbon" (The Treacherous Receipt) from the TV series Quarks & Co to solve the riddle: **http://bit.ly/13CCi2T** An American father complains to a department store (Target) because they keep sending his 16-year old daughter vouchers for pregnancy/baby products. At this point, he does not know that she is actually pregnant. The company, however, has already worked this out using his daughter's shopping patterns.
Elaboration	Task 1: What exactly can you discover about people from their shopping habits? The students complete the worksheet and describe the consumers based on their purchases. Give an example: Person 1 *is ill, probably a gastrointestinal problem, female, between 17 and 23, very interested in fashion.* The students read out a number of the profiles they have created. TIP: The students can create shopping lists of their own and their classmates then have to guess the person who wrote it and his/her background. Full group discussion: How can companies find out even more about people? Recording and analysis of shopping patterns through discount cards (e.g. Payback), competitions or surveys, evaluation of video surveillance films in sales rooms, tracking RFID chips on products or in shopping trolleys, saving bank transactions, credit agencies, credit rating agency. Why do companies do this? Customer loyalty, trading customer data, personalised advertising, basis for scoring processes (recording and evaluation of modes of payment / information about payment behaviour), optimisation of company workflows.
Anchoring	Task 2: How can you protect yourself against customer profiling? Do not use customer cards like Payback, do not participate in bonus programmes, do not shop "exclusively" online, use different suppliers, install anti-tracking add-ons in your browser, e.g. Ghostery, Adblock, Trackerblock. Additional activity/homework: What can companies find out about the students themselves? Ask the students to pay special attention to personalised advertising. Ask the students to perform the same Google searches on different devices (e.g. on their smartphones) and compare the different adverts they are shown. What other advertising do you receive, e.g. via Facebook? Is it tailored to your interests? Film tip: Mobile Payment – Die Zukunft des Einkaufens *(The Future of Shopping)*: **http://bit.ly/102ok8j** Brochure: **www.lfm-nrw.de/fileadmin/lfm-nrw/nrw_digital/DK_Mobile_Payment.pdf** Film "Der gläserne Deutsche": **https://archive.org/details/Der_glaeserne_Deutsche**

Tell me what you buy and I will tell you who you are!

Task 1:
Even small purchases can say something about you. What can you find out about a person from their shopping habits? Write down who could have made the purchase and describe the person's current situation:

Food, clothing, care products, magazines, books, games, decorations, sports equipment/clothing – it is amazing what you can discover about people from their shopping. If your consumer behaviour is observed for a certain period of time, it is possible to find out whether you are young or old, rich or poor, healthy or sick, pregnant or not. The processes used to observe, evaluate and compare your behaviour patterns are known as "tracking" and "scoring". .

Person 1:
Supermarket shopping
fennel tea, pretzel sticks, rusks, DVD box set "Twilight", Vogue
Description
Description:

Person 2:
Website shopping trolley at Planet Sport
Bermuda shorts, bikini top, surfboard
Description:

Person 3:
Zalando shopping trolley
pumps, dress, handbag, hair accessories
Description:

Person 4:
Supermarket shopping
Zero-Cola, Blu-Ray "Marvel's The Avengers", Axe deodorant spray, Durex condoms
Description:

Person 5:
Invoice from DIY store
crowbar, fabric gloves, glasscutter, black work trousers
Description:

Person 6:
Amazon book list
"Backpacker Tips for Surviving Without Money", "What To Do When You Leave School?", "The World's TOP 50 Party Cities", "Travel the World for Free"
Description:

Person 7:
Google Play Store
torch app, The 10 best jokes, Subway Surfer, WhatsAPP, facebook, Bundesliga app
Description:

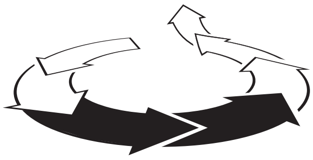
Person 8:
App Store
Dr. Zhivago's Memory Training, blood pressure measurement app, bus timetable app, best knitting patterns app, pet food deliveries to your home app
Description:

Person 9:

Task 2: Shopping online and customer loyalty cards allow companies to track and score your shopping habits accurately. How can you protect yourself against this type of profiling?
Collect ideas with others at your table and present them to the class.

Food for thought: *If you are not paying for something, you are not the customer. You are the product being sold.*
Andrew Lewis

Notes for teachers



3 Confronting the risks of big data
4 Reflection on the consequences of breaches of privacy

Description of Project 3: Big Data – Big problem?

(from 16 years old)

Competences	**The students learn to recognise the opportunities and risks of big data.**
Time	60 minutes
Methods	Role-play, mind map
Materials	Trailer "Data Dealer", make films on "big data" available to students, copy role-play cards, additional worksheets for the "Internet of Things" and "Surveillance" at **www.klicksafe.de/medienethik**
Access to Internet/PC	No (make videos available)
Introduction	Show the trailer for the online game "Data Dealer" up to approx. 1:32 min (http://datadealer.com/de/). The game deals critically with the topics of data trading and data abuse. The students now have to assume the role of a data dealer and his potential customers (e.g. representatives of a bank). Divide your students into groups of 5. This gives each data dealer an average of four customers. Role-play cards provide a clear framework for the roles (data dealer, bank, online store, health insurance company, police state). The data dealer asks the customers what information they are interested in and takes notes. These will be presented to the full group of data dealers later. Each piece of data can be ranked according to its value ("Which bit of information is potentially more valuable than another?"). **Possible results:**

Bank	**Online-store**	**Health insurance company**	**Police state**
Debts, assets, profession, age, income	Interests/preferences, consumer habits, payment behaviour/ speed of payment (does the user settle invoices quickly or slowly), age, lifestyle, taste in music	Nutritional behaviour, weight, diseases, hobbies, family, alcohol consumption, sexual orientation, DNA profile	Political opinions, assets, communication behaviour, friends and acquaintances, patterns of movement

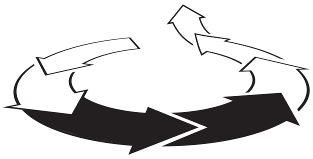
TIP: The students can play the demo version of the online game "Data Dealer" **http://demo.datadealer.net/,** e.g. in a lesson with a replacement teacher.

Elaboration

The above game gave the students an insight into the types of data that are of interest to companies and other organisation. Task 1 of the next step shows them what happens to this flood of information ("big data") today and how it may be used in the future. The students continue to work in the same groups as in the introductory task and watch various films on the subject of "big data". They can also watch one of the films as a whole class (e.g. "Big Data – Revolution in allen Lebensbereichen" (*Big Data – A Revolution in Every Area of Life*) by the student Mats). Task: *"Create a mind map on the worksheet to show everything that is possible using big data today. Then mark each aspect according to whether you consider it to be (more of) an opportunity or a risk (with +/- or green/red pen)."*

You can find further videos on the subject of big data:
1. "Big Data – Revolution in allen Lebensbereichen" **http://bit.ly/1wZwPzn**
2. "Big Data" (LfM) **http://bit.ly/1dALYhd** Begleitbroschüre zum Film: **www.lfm-nrw.de/fileadmin/lfm-nrw/nrw_digital/Publikationen/DK_Big_Data.pdf**
3. "Big Data einfach erklärt" (Telekom) **http://bit.ly/1x2iP6o**

Notes for teachers



3 Confronting the risks of big data
4 Reflection on the consequences of breaches of privacy

Elaboration

Possible solution:
Opportunities: create media and consumer worlds tailored to the interests of the individual user (search engines, news websites, online shops), create new business models, new traffic analysis tools (prevention of traffic jams and accidents), generate more accurate insights (dating agency, school), show how companies can operate more transparently and efficiently, provide new jobs, implement measures to tackle poverty and diseases (identify the transmission paths of diseases, e.g.: Google Flu Trends), calculate probabilities of crimes being committed (predictive policing) – increase security
Risks: suspicion/arrest based on a prediction rather than a deed, calculation of credit-worthiness, different prices/discounts (dynamic pricing), surveillance (comprehensive knowledge about us), higher costs (insurance), people are customers not citizens, no possibility of events being forgotten (youthful follies), manipulation ("effective approaches to customers")

Anchoring

Collect the results from the groups on the board as a joint mind map and discuss.

Sources:
www.spiegel.de/netzwelt/web/das-internet-der-dinge-erzeugt-2-8-zettabyte-daten-a-872280.html,
https://blog.telekomcloud.com/ist-eigentlich-big-data/

You are just starting out as a data dealer and are meeting potential customers for the first time.

▷ **Find out what data you can sell to each customer.**

▷ **Collect the data you need from your customers.**

Bank	Online store	Health insurance company	Police state

You own the bank. You want to earn as much as possible and make as few bad deals as possible.

▷ **What information about your customers would help you to do this?**

As a large health insurance company, you need plenty of healthy customers so you can make a profit.

▷ **What information about potential customers would help you to boost your profits?**

You are the dictator of a country. You want it to stay that way.

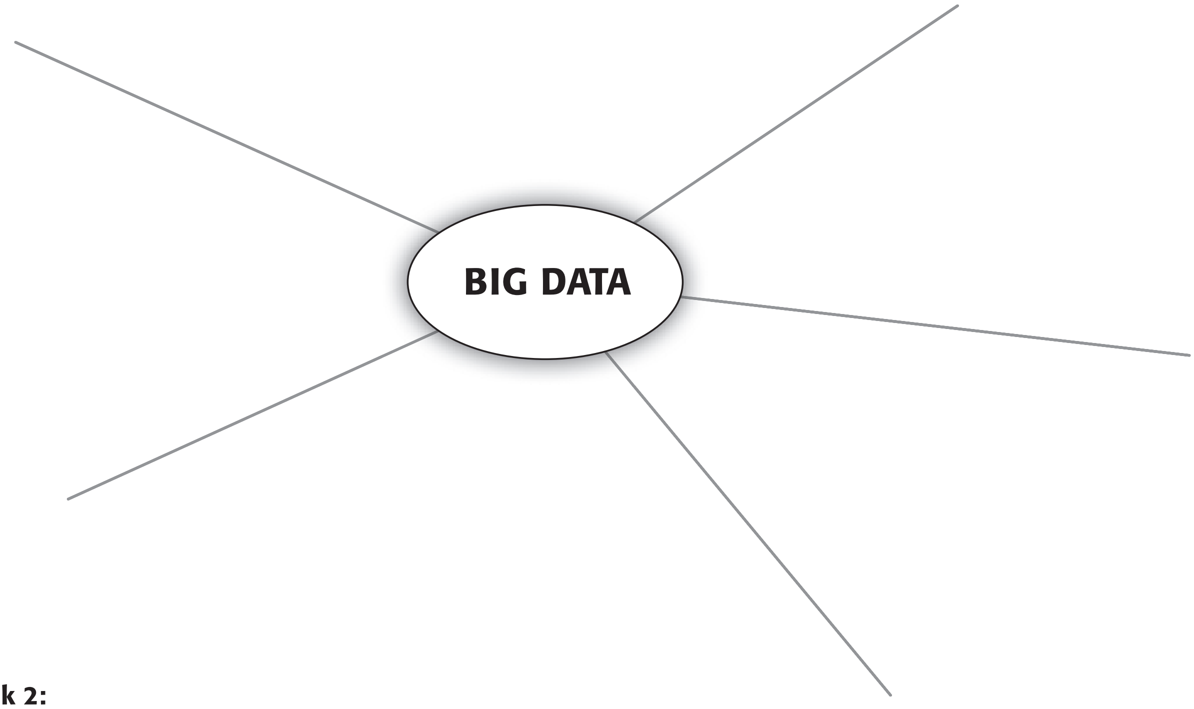
▷ **What information about the citizens of your country would help you to stay in power?**

Your online store is on the point of becoming a global force. To become the market leader, you want to target your advertising more accurately.

▷ **What data do you need to do this?**

Big Data – it's almost impossible to imagine …
Big data is the collective term for vast volumes of data, data analysis and evaluation tools based on enormous storage capacity.
Current forecasts estimate that there will be up to 40 zettabytes of big data by 2020. For clarification: a zettabyte is a one followed by 21 zeros!
According to scientists, 40 zettabytes is 57x the number of grains of sand on all the beaches on Earth! !

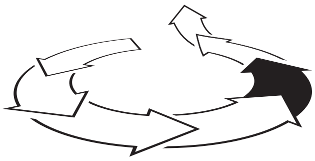
Task 1:
What is big data used for now and what will it be used for in the future? Collect these uses in a mind map.



Task 2:
Highlight the uses which are positive (+) and negative (-).

__TIP:__ The online game __"Data Dealer"__ deals with the subject of trading data. Data is power and money. Your goal is to receive as much data about people as possible and then to sell it on.
Become a data dealer yourself!
You can play the game here: __http://demo.datadealer.net/__

Source: © datadealer.net CC-BY-SA 3.0



Description of Project 4: How should I decide?

Competences	**The students learn how to cope with difficult situations and make decisions based on their own values.**
Time	45 minutes
Methods	Discussion of values
Materials	Cards, cut out examples of dilemmas
Access to Internet/PC	No

Introduction

The students sit in a circle and write down the three values that are most important to them personally on three cards (e.g. family, peace, health, honesty etc.). *Collect* these on the board (keep a tally) or using the program **www.wordle.net.** *Evaluation:* Which three values are most important for the class? What do these say about the class?

Note: Depending on the students' level of knowledge, before starting the exercise discuss what "values" are and why we need them. Values are often described as sub-conscious standards and ideas that guide us. You can also use the overview "fields of values" from the introduction.

Elaboration

How would your students decide? The aim of the sample dilemmas is to stimulate discussion among the students and get them to think about questions that have no clear answers, such as "yes" or "no". You can run a separate lesson with selected dilemma situations or use them at the end after doing a number of worksheets as a repetition exercise.

Method "Making a decision":

1. The teacher hands out or reads out an example.
2. Straw poll: What should the person do? The students vote by raising their hands.
3. As a full class, analyse the reasons for the decision. Write down the arguments as bullet points on the board.
4. Analysis of the arguments in terms of values (see collection of values): Which values underlie the arguments? Which values are they not taking into consideration? Which values conflict? Which values influence our decisions?
5. Final discussion: The teacher asks the initial question again and there is another straw poll. It becomes clear whether opinions have changed and which arguments are more convincing. It is also important to discuss the consequences or conflicts that result from each decision.

At the end of the exercise, the group can also discuss whether they have solved the dilemma.

Source: Method modified from Gugel, Günther; Didaktisches Handbuch, Werte vermitteln – Werte leben; Berghof Foundation

Anchoring

Evaluation: Which decisions were most difficult for the students? Why?

Additional task/Homework:
The students can create their own dilemma situations and present these to the class.

The characteristics of a good values dilemma:
Is there really a predicament? No easy way out of the quandary? Is the story short (not more than half a page) and easy to understand? Does it evoke curiosity, empathy, and suspense? Do the persons involved have names?

Source: Günther Gugel: Didaktisches Handbuch, Werte vermitteln – Werte leben, p.83

TIP: Card game for learning to make decisions
http://www.bpb.de/shop/lernen/spiele/34263/jetzt-mal-ehrlich

How should I decide?

Conflict: Private information in the public domain

Tim and Lisa have been together for two months. To show how much she loves him, Lisa has put together a slide show for Tim and posted it on his Facebook profile. It shows photos recording some of their favourite moments, trips and cuddles together. Many friends have commented on the film and "liked" it. Tim is torn. On the one hand, he thinks it is very sweet. On the other hand, he feels it is too private to be shown in public.

Should he delete the slide show?

Conflict: Data Deals

Lina has discover a new online shop, which offers unique items from famous fashion houses at big discounts. She wants to buy a beautiful new dress for a school ball. However, the shop has also had some bad reviews (data mishaps, hacking etc.). In the final step of placing her online order she is asked to provide specific information including her bank account details. Her mother has expressly warned her against providing this information and asked her always to pay by invoice. But this is not possible.

Should Lina enter the data?

Conflict: Nosy Apps

A new messenger app has just been launched and is all the rage. However, it accesses you phone's address book, photo memory, email inbox and connection data when you telephone. Joel actually knows this is not ideal and his father has warned him against using services that clearly aim to collect as much data as possible. But all his friends have this app.

Should Joel install the app on his phone?

How should I decide?

Conflict: Big Brother in the passenger seat

Matthew wants to buy a new car. At the car showroom, the salesman tells him that he can save a lot of money on insurance premiums if he agrees to have a "black box" installed. This would record his driving behaviour via wireless and GPS and evaluate when, where, how fast, how often and how safely he drives. Matthew's dream car is just a little too expensive for his budget but perhaps – if he saved money by agreeing to the black box – he could just afford it.

How should Matthew decide?

Conflict: Predictive Policing

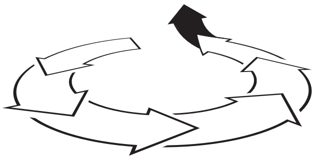
Since 11 September 2001, the USA has taken a much more stringent attitude to security. For example, it has developed a program, which analyses data to predict when and where crimes will take place. Authorities can also enter and analyse personal data about former prisoners in this type of program. Lilly reads an essay about the project and wonders whether Germany should consider using such a program.

Sollte ein solches Programm auch in Deutschland eingesetzt werden?

Conflict: To unsubscribe or not?

Sonia has given a presentation about data protection on the Internet at her school. Since becoming better informed, she feels uncomfortable whenever she is on the Internet or using her smartphone. She doesn't want to become the "transparent person" that everyone is talking about. Actually, she would really like to cancel all her subscriptions and contracts. However, as she makes the decision she begins to have doubts. After all, she keeps in touch with all her friends using online services.

Should she unsubscribe?



7 Identifying options and tools for taking personal, political and instrumental action

Description of Project 5: Become an activist!

Competences	**The students learn about the action they can take to protect their fundamental digital rights.**
Zeit	60 minutes
Methods	Group work
Material	Task cards, help cards
Access to Internet/PC	Yes (for all groups)
Introduction	*“This selection of table activities shows you what you can do to exercise just a little influence over what happens to your data”* Lay out the four task cards (Protect Your Personal Data, Government Watch, The Right to Informational Self-Determination, Privacy by Design) on 4 tables. The students walk around the classroom for approx. 3 minutes, read the task cards and sit down at the table with the task that interests them most. Tables can be doubled if there is interest in more than one task (please remember to copy the cards in this case). You can also ask everyone to work at only selected tables. You can distribute the help cards “Suggestions for the group” immediately or only if they are needed. **TIP:** The “Protect Your Personal Data” group is also suitable for younger/weaker students. The students produce their own files using tips provided by a student from the klicksafe Youth Panel (e.g. text files, photos, mobile phone videos), which they should then forward to the other students. **Criteria:** ▪ The content should be clear and easy to understand. ▪ The file should communicate the content in an interesting and creative way. ▪ It should be suitable for use as part of a data protection campaign. ▪ The young people should complete the file within an allotted period ▪ Please take account of copyright restrictions if you plan to distribute the content outside the school
Elaboration	The students have 45–60 minutes to complete the task.
Anchoring	One after another, the students at a table report on their approach and present their results.

Group: Protect Your Personal Data

Devise your own tips for protecting your personal data for your class, your friends and yourschool.

Tasks:

1. How can you protect yourself against the rampant data collection and data theft on the Internet? Come up with at least five tips for protecting your personal data.
2. Use these tips to produce a flyer and distribute it at your school (you can also do this digitally via your own school website or social networks). Remember to make it interesting!

You can find some ideas here:

http://www.youngdata.de/datenschutz/datenschutz-tipps/

Suggestions for group: Protect Your Personal Data

Data protection tips:
by Hendrik from the klicksafe Youth Panel.

1. Use an encrypted messenger (Telegram, Threema). Even when using encrypted services, remember to use a nickname if you can (this makes it impossible to associate the communication to you).
2. If you intend to supply private data on the Internet: always(!) check that the website is https-encrypted and valid (check the green bar in the address line). A browser add-on such as "HTTPS Everywhere" can also be useful.
3. When using apps, make sure that you are really using the official version of the app. In app stores, you will often find app clones which can take over your account (as with phishing), e.g. by asking you to enter your "SMS confirmation code".
4. Use alternative, secure cloud storage solutions if you really have to put documents/images online and share them with others, e.g. Spideroak (recommended by Edward Snowden). These allow you to store encrypted files.
5. Even if you appear to be safe and secure – just remember that even the best encryption has weaknesses. So always think carefully about what you send or write. Even Snapchat has been hacked and photos posted online.
6. Search engines also know a lot about you. Take a look at alternative search engines, such as Startpage, Duck Duck Go or Ixquick, which do not save any data.
7. Use a variety of services, i.e. do not use all the services from just one provider. For example, if you use Facebook and WhatsApp, Facebook has a complete overview of all your private communications.
8. Wherever possible, only use services which you know to be secure or which have received positive reports (e.g. in the media or from friends). There are thousands of services on the Internet. Many of these have never been examined closely because they are virtually unknown.

Group: Government Watch

Here you have the opportunity to ask a politician questions on the subject of data protection.

Tasks:

1. Research a topical area of data protection that interests you.
2. Prepare two questions about this subject that you would like to ask an MP.
3. Vote on the questions you would like to ask and post this on a website such as Abgeordnetenwatch (Government Watch – or the equivalent in your country). This website allows anyone to put a question to their MP or MEP: 🖱 **www.abgeordnetenwatch.de/ueber-uns/faq**
4. Even if you have to wait a while for the answer, don't give up and share the answer you receive with your classmates.

Suggestions for the group: Government Watch

Suggested topics:

- New European Data Protection Act (www.eu-datenschutzverordnung.de)
- Trade agreements with the USA (free trade agreement: SWIFT treaty, TTIP treaty)
- The power of the big corporations Apple, Google, Facebook, Amazon: 🖱 **http://bit.ly/1tDA20H**
- Big Data 🖱 **http://bit.ly/1zI1kYo**;

Suggested politician:

Put questions to Jan Philipp Albrecht, the German Green Party MEP, who is responsible for the issue of data protection in the European Parliament: 🖱 **https://www.abgeordnetenwatch.de/eu/profile**

For example, you could refer to his interview on the planned European Data Protection Act:
🖱 **www.zeit.de/2013/02/Big-Data-Interview-Albrecht**

Group: Privacy by Design

Develop suggestions about how to improve the area of data protection at Facebook.

Tasks:

Read Facebook's data protection policy: **https://www.facebook.com/policy.php**
Write down the aspects that you (as a young user) think are good and bad. Above all, pay attention to the clarity of the text and the design of the page. How could you improve this area of a website such as Facebook? Don't be afraid of making creative suggestions!

You may find some information or ideas in the terms and conditions of other services.

Group: The Right to Informational Self-Determination – Practical Test!

Request information about your data from Facebook, Amazon, Deutsche Bahn or Google.

Tasks:

1. Look at how and where data was collected about the politician Malte Spitz.
   http://bit.ly/1szImxA
2. Follow the example of Malte Spitz! Choose a service that most of you know or use and find out how you can obtain information about the data it stores about you.
3. Write a letter and a matching text.
4. Send the service a request for information about your data.

Suggestions for the group: The Right to Informational Self-Determination

Model letter: Request for information and cancellation of agreement to the sharing of personal data

Your name Date

Street House number

Postcode Town

Company

Address

Request for information and cancellation of my agreement to the sharing of my personal data for advertising purposes

Dear Sir/Madam,

In accordance with § 34 German Federal Data Protection Act (BDSG), I hereby request the following information:

What data do you possess about my person and where did you obtain this data?
To what recipients or other organisations have these data been forwarded?
For what purposes is my data being stored?

I hereby revoke my permission for my data to be used for advertising, market research or opinion polling purposes in accordance with § 28 Paragraph 4 BDSG. You are therefore legally obliged to block the use of this data for these purposes immediately.

Please comply with my request by the:
insert date (14 days later)

If you ignore this letter, I will contact the responsible state data protection officer. Moreover, I reserve the right to take further legal action.

Yours sincerely

Notes on using the model letter:

1. Copy the text to a word processing program (MS Word, Open Office, etc.).
2. Complete it with your sender address, a deadline (date) and the address of the company, to which you are sending the model letter.
3. Send this letter to the company.

Source: ©Copyright Verbraucherzentrale www.vzbv.de, Date: July 2013

Endnotes/References

[1] Heller, Cristian (2013): *Privatsphäre – ein Auslaufmodell? Ein Plädoyer für echte Transparenz*. In: aej information – Zeitschrift für die Evangelische Jugend in Deutschland, 3/2013, **p. 2–3**. Online: http://www.evangelische-jugend.de/fileadmin/user_upload/aej/Die_aej/Downloads/Publikationen/PDF-Ausgaben/aej_information_3-2013.pdf (accessed: 15.07.2015).

[2] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (2014): *DIVSI U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt.* Online: https://www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf (accessed: 15.07.2015).

[3] Rössler, Beate (2001): *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp Verlag. **p. 17**

[4] Boyd, Danah (2008): *Taken Out of Context: American Teen Sociality in Networked Publics*. Dissertation, University of California, Berkeley. Online: http://www.danah.org/papers/TakenOutOfContext.pdf (accessed: 15.07.2015). **p. 27**

[5] GfK Verein (2013): *Maßnahmen der Internetnutzer: Digitaler Selbstschutz und Verzicht. Die Studie "Daten & Schutz 2013" des GfK Vereins.* Pressemitteilung vom 21. November 2013. Online: http://www.gfk-verein.de/files/gfk_verein_pm_2_daten_schutz.pdf (accessed: 15.07.2015).

[6] Barnes, Susan B. (2006): *A privacy paradox: Social networking in the United States*. In: First Monday – Peer-reviewed Journal on the Internet, Volume 11, Number 9, 04.09.2006. Online: http://firstmonday.org/article/view/1394/1312 (accessed: 15.07.2015).

[7] Haller, Kai (2013): *Umfrage zum Datenschutz: User nutzen Smartphone-Apps zu leichtsinnig*. Focus Online, 06.08.2013. Online: https://www.mediatest-digital.com/wp-content/uploads/2013/08/Umfrage-zum-Datenschutz-User-nutzen-Smartphone-Apps-zuleichtsinnig-Kai-Haller-FOCUS-Online-Nachrichten.pdf (accessed: 15.07.2015).

[8] Lobo, Sascha (2014): *S.P.O.N. – Die Mensch-Maschine: Willkommen im Zeitalter der Selfieness.* Spiegel Online, 04.03.2014. Online: http://www.spiegel.de/netzwelt/netzpolitik/kolumne-von-sascha-lobo-willkommen-im-zeitalter-der-selfieness-a-956643.html (accessed: 15.07.2015).

[9] Kutscher, Nadia (2013): *Datenschutz und Privatsphäre im Kontext virtueller sozialer Netzwerke. Herausforderungen und Fragen für die Jugendarbeit.* In: aej information – Zeitschrift für die Evangelische Jugend in Deutschland, 3/2013. Online: http://www.evangelische-jugend.de/fileadmin/user_upload/aej/Die_aej/Downloads/Publikationen/PDF-Ausgaben/aej_information_3-2013.pdf (accessed: 15.07.2015). **p. 1–2**

[10] Albers, Marion (2013): *"Jeder hat was zu verbergen." Ein Interview mit der Rechtswissenschaftlerin Marion Albers* von Oliver Link. In: brand eins, Heft 08 (Schwerpunkt Privat), August 2013, **p. 123–125**.

[11] Rössler, Beate (2001): *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp Verlag. **p. 23**

[12] Kutscher (see above), 2013, **p. 1**

[13] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (see above), 2014, **p. 120**

[15] Mayer-Schönberger, Viktor/Cukier, Kenneth (2013): *Big Data. Die Revolution, die unser Leben verändern wird.* München: Redline. **p. 3**

[16] Heuer, Steffan/Tranberg, Pernille (2013): *Mich kriegt ihr nicht! Die wichtigsten Schritte zur digitalen Selbstverteidigung*. Hamburg: Murmann. **p. 26**

[17] ibid. **p.** 127

[18] Mayer-Schönberger & Cukier (see above), 2013, **p. 99 ff**

[19] Heuer & Tranberg (see above), 2013, **p. 101**

[21] Olejnik, Lukasz/Castelluccia, Claude/Janc, Artur (2012): *Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns*.5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2012), Jul 2012, Vigo, Spain. Online: https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf (accessed: 15.07.2015).

[22] Heuer & Tranberg (see above), 2013, **p. 120**

[23] Kluemper, Donald H./Rosen, Peter A./Mossholder, Kevin W. (2012): *Social Networking Websites, Personality Ratings, and the Organizational Context: More Than Meets the Eye?* In: Journal of Applied Social Psychology, 42, **p. 1143–1172.**

[24] Landesanstalt für Medien Nordrhein-Westfalen (LfM) (2014): *NRW digital – Digitalkompakt.* Online: http://www.lfm-nrw.de/nrwdigital/digitalkompakt/transkript-video-apple-google-facebook-amazon.htmls (accessed: 15.07.2015).

[25] quoted after Döpfner, Mathias (2014): *Warum wir Google fürchten. Offener Brief an Eric Schmidt.* Frankfurter Allgemeine Zeitung online, 16.04.2014. Online: http://www.faz.net/aktuell/feuilleton/medien/mathias-doepfner-warum-wir-google-fuerchten-12897463-p5.html?printPagedArticle=true#pageIndex_6 (accessed: 15.07.2015).

[26] jointly with Jared Cohen, 2013.

[27] Mill, John Stuart (2010 [1859]): *Über die Freiheit*. Stuttgart: Reclam.

[28] Assheuer, Thomas: (2013): *Überwachung: Wer blickt da durch?* Zeit Online, 03.11.2013.
Online: http://www.zeit.de/2013/45/ueberwachung-nsanichtwissen-big-data/komplettansicht (accessed: 15.07.2015).

[29] van den Hoven, Jeroen (2010): *Information Technology, Privacy, and the Protection of Personal Data.* In: Ders./Weckert, John (Hrsg.): Information Technology and Moral Philosophy. Cambridge: University Press, S. 301–321. **p. 319**

[30] Maier, Robert M. (2014): *Angst vor Google. Von der Suchmaschine zur Weltmacht.* Frankfurter Allgemeine Zeitung online, 03.04.2014. Online: http://www.faz.net/aktuell/feuilleton/debatten/weltmachtgoogle-ist-gefahr-fuer-die-gesellschaft-12877120.html (accessed: 15.07.2015).

[31] Döpfner (see above), 2014

[32] Mayer-Schönberger & Cukier (see above), 2013, **p. 242**

[33] Filipovi , Alexander (2014): *Big Data: Medienethische Fragen zur digitalen Vermessung der Welt.* Keynote beim XIII. Tag der Medienethik am 25.06.2014, Hochschule der Medien (HdM), Stuttgart. Online: http://geloggd.alexander-filipovic.de/wp-content/uploads/2014/06/Keynote-Filipovic-Stuttgart.pdf (accessed: 15.07.2015).

[34] Rössler (see above), 2001

[35] This includes Nissenbaum, Helen (2010): *Privacy in Context. Technology, Policy, and the Integration of Social Life.* Stanford, California: Stanford Law Books.; van den Hoven, Jeroen (2010): *Information Technology,Privacy, and the Protection of Personal Data*. In: Ders./Weckert, John (Hrsg.): Information Technology and Moral Philosophy. Cambridge: University Press, p. 301–321. and Nagenborg, Michael (2005): *Das Private unter den Rahmenbedingungen der IuK-Technologie. Ein Beitrag zur Informationsethik.* Studien zur Wissensordnung, Bd. 3. Wiesbaden: VS Verlag für Sozialwissenschaften.

[36] Rössler (see above), 2001, p. 218

[37] Kant, Immanuel (1999 [1786]): *Grundlegung zur Metaphysik der Sitten.* Mit einer Einl. hrsg. von Bernd Kraft und Dieter Schönecker. Hamburg: Meiner. p. 61

[38] Europäische Kommission (2012): *Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern.* Pressemitteilung. Brüssel, 25.01.2012. Online: http://europa.eu/rapid/press-release_IP-12-46_de.htm (accessed: 15.07.2015).

[39] European Group on Ethics in Science and New Technologies to the European Commission (EGE) (2014): *Ethics of Security and Surveillance Technologies.* Opinion No 28, 20.05.2014. Online: http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf (accessed: 15.07.2015). p.158

Quotes from the text

Sofsky, Wolfgang (2009): *Verteidigung des Privaten. Eine Streitschrift*. München: C.H.Beck.

Weichert, Thilo (2013a): *Big Data und Datenschutz*.
Online: ttps://www.datenschutzzentrum.de/bigdata/20130318-bigdata-und-datenschutz.pdf (accessed: 14.11.2014).

Schmidt, Eric/Cohen, Jared (2013): *Die Vernetzung der Welt. Ein Blick in unsere Zukunft*. Reinbek: Rowohlt.

Lanier, Jaron (2014): *Wem gehört die Zukunft? "Du bist nicht der Kunde der Internetkonzerne. Du bist ihr Produkt."*
Hamburg: Hoffmann und Campe.

Kuhlen, Rainer (2004): Informationsethik. Konstanz: UVK Verlagsgesellschaft.

klicksafe is co-funded by
the European Union

klicksafe.de klicksafe is the German awareness centre in the CEF Telecom Programme of the European Union.

klicksafe is:

Landeszentrale für Medien und Kommunikation (LMK)
Rheinland-Pfalz – www.lmk-online.de

Landesanstalt für Medien Nordrhein-Westfalen (LfM) –
www.lfm-nrw.de

in partnership with

Institut für Digitale Ethik (IDE)
www.digitale-ethik.de

at

Stuttgart Media University (HdM)
www.hdm-stuttgart.de

klicksafe – offices

c/o Landeszentrale für Medien und
Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
E-Mail: info@klicksafe.de
Internet: www.klicksafe.de

c/o Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
E-Mail: klicksafe@lfm-nrw.de
Internet: www.klicksafe.de