DIVSI

Deutsches Institut
für Vertrauen und
Sicherheit im Internet

DIVSI Opinion Leader Study

Who shapes the Internet?

www.divsi.de

DIVSI Opinion Leader Study

Who shapes the Internet?

A study conducted by
SINUS Institut, Heidelberg,
for Deutsches Institut für
Vertrauen und Sicherheit
im Internet (DIVSI)

Heidelberg/Germany, October 2012

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 142, 20148 Hamburg, Germany
Matthias Kammer, Director
Joanna Schmölz, Head of Research
Dr. Dirk Graudenz, Project Team for Studies

Sinus Institut, Heidelberg
Project lead: Dr. Silke Borgstedt
Text: Dr. Silke Borgstedt, Cornelia Appel, Dr. Marc Calmbach
Project team: Matthias Arnold, Manfred Tautscher, Susanne Ernst

Table of contents

Page

Foreword **4**

1. Status quo, objectives and methodology **7**

2. Opinion leaders map out current Internet challenges **13**

3. Internet players' perspectives **17**

3.1. Politics and public administration: On milestones, guardrails and trust anchors . **17**

The Internet has narrowed the gap between politics and the private citizen 18
Security of the citizens as the primary goal of politics 19
Dominance of global corporations threatens the ability to keep control of the state 21
The need to define mandatory security standards and to improve media literacy 23

3.2. Business: On opportunities, speed and good prospects **25**

Internet as a determining factor of the present 26
Companies see themselves as captains on the sea of opportunities 27
Government is an "overly cautious" impediment to economic growth and innovation 28
Ensuring competitiveness by actively shaping public and political opinion 31

3.3. Civil society representatives: On endangered visions, limited participation and the search for a consensus on values **35**

The Internet as the engine of social change 36
Personal commitment to a free Internet as a knowledge resource for all 37
Industry and government are locking people out of the Internet 38
The need to democratize knowledge and decelerate regulation 39

3.4. The Media: On conflict areas, power constellations and necessary relativization of opportunities and risks **41**

Internet as key technology and topic generator 42
Media as observer and commentator on fast-moving change 44
Opportunity and risk assessment of other players lack balance 45
Making technological innovations more user-friendly and secure 46

3.5. Academia:
On structural change, design imperatives and new social divisions 49

The Internet as the trigger for a cultural transformation 50
Describe, compare and gain an overview 51
All sectors need to catch up regarding the Internet – except for business 52
Reinforcing the significance of research and defining concrete needs for action 54

4. "Babylonian Confusion of Tongues":
Security between law and freedom – but without consensus 59

Comprehensive Internet security does not exist 60
Security on the Internet as a challenge for economy and politics 61
Little common sense in the discourse about security on the Internet? 62
Security as a "hot potato" 65
Passing the buck on responsibility 66

5. OSI Layer 8: The user is responsible and bears all risks 67

Recommendation to users: Invest in security and act smart! 69
Trust begins where personal responsibility ends 70
Trust as the key currency on the Internet 71
Trust without security? The alleged legal framework as fallback strategy 74

6. Summary – Four theses on the current state of the Internet debate 77

No one is offline anymore – life without the Internet is an illusion.................................. 78
Ultimately, responsibility lies with the user – and no one wants to take it
off his shoulders 79
The Power is in the hands of the movers:
The world's leading companies shape the rules of the game 79
The Internet does not exist (anymore) 81

***Matthias Kammer**, Director of DIVSI, the German Institute for Trust and Safety on the Internet*

DIVSI Opinion Leader Study: Who shapes the Internet?

In line with our self-formulated working basis, DIVSI aims to facilitate an open and transparent dialogue on trust and safety on the Internet and to vitalize this dialogue with new aspects. In order to achieve this goal we provide the general public with the latest facts which can then serve as a foundation for broad-based discussions.

With our “Milieu Study on Trust and Safety on the Internet”, which has now gained national recognition and acceptance, we achieved an important interim goal. This first study focused on people living in Germany and examined the motives and attitudes that determine their relationship with the Internet as well as their expectations regarding safety and data protection.

The new DIVSI study published today goes a step further, focusing on an important and clearly defined group of people. Continuing our established collaboration with the prestigious SINUS Institute, we asked this organization to conduct a scientific, nationwide survey to reveal the attitudes of opinion leaders in Germany to the Internet.

We wanted answers to the following questions: Who actually shapes the Internet? How conversant are opinion leaders with the Internet? How do they estimate their own influencing possibilities? How do they regard the needs for both safety and freedom? What opportunities, areas of conflict and risks result from this?

In-depth personal interviews were conducted with leading representatives from the areas of politics, business, media, social organizations, the public sector and science. This is the first time that such a specific and targeted study has been undertaken in Germany. The results of the study point to four essential statements, which I will here describe in brief:

– Private-sector enterprises are the drivers of current developments in the Internet. This means that companies not only take the role of service providers but are also the ones who determine the rules – and who continually change them, too.

– No one is really offline any more. The Internet is becoming important in ever more areas of life. Online and offline spheres are increasingly intermingling and merging. It is growing ever harder to separate the two states.

- The opinion leaders do not believe that an overall structural responsibility for “the Internet” is possible, nor do they consider it desirable. Their solution is to pass a large proportion of the responsibility to the users.

- It is becoming ever more difficult to create generally applicable rules and to make mutual agreements for the Internet as a ‘negotiable space’. The discourse is increasingly shifting from a purely technological perspective to a question of the ‘digital culture’.

Those familiar with our first study will immediately note that the statements of the opinion leaders stand, in some respects, in clear contrast to the attitudes and approaches of the general population as revealed last year. According to the previous study, 39 per cent of people living in Germany were “Digital Outsiders”. However, in the view of those who shape the Internet, these people too are living in an environment that is increasingly being affected by the online world. We believe that further analysis of such findings is sure to provide valuable impetus for future debate.

It is to be expected that the presented results will not bring undivided praise for DIVSI. But this cannot and should not hinder us from submitting potentially unwelcome facts as a basis for discussion. Steering clear of any superficiality and sensationalism, the study is intended to create a starting point that can help to make our networked world a more trustworthy and safer place.

On this note I wish you informative and absorbing reading with the DIVSI Opinion Leader Study. In the coming months we will – in collaboration with the SINUS Institute – further extend this survey to create a nationally representative study. This work will be presented at CeBIT 2013.

Matthias Kammer
Director DIVSI

1.
Status quo, objectives and methodology

1. Status quo, objectives and methodology

Status quo and objectives

Up until now, research on the subject of the Internet has focused almost exclusively on the user perspective. We therefore know a good deal about user behavior and user profiles, i.e. who is on the Internet and where, how often, and why.

But who actually shapes "the Internet" – its design, configuration and evolution? Who are the opinion-leaders and how are they influencing developments? How knowledgeable and experienced are they, themselves, when it comes to the Internet? How are requirements for security and freedom evaluated and negotiated? What new opportunities does the Internet offer society as a whole? What new risks and potential areas of conflict does it introduce?

The DIVSI Opinion Leader Study is designed to help answer these questions based on in-depth interviews with leaders from government, business, media and academia as well as civil society representatives. This volume presents the results of Part I of the investigation, which included in-depth interviews with over 60 experts. Part II of the investigation will employ a representative survey to assess the opinion-leader landscape in Germany. The combined result will provide the first detailed look at how the Internet is viewed by the people involved in defining the rules of the game.

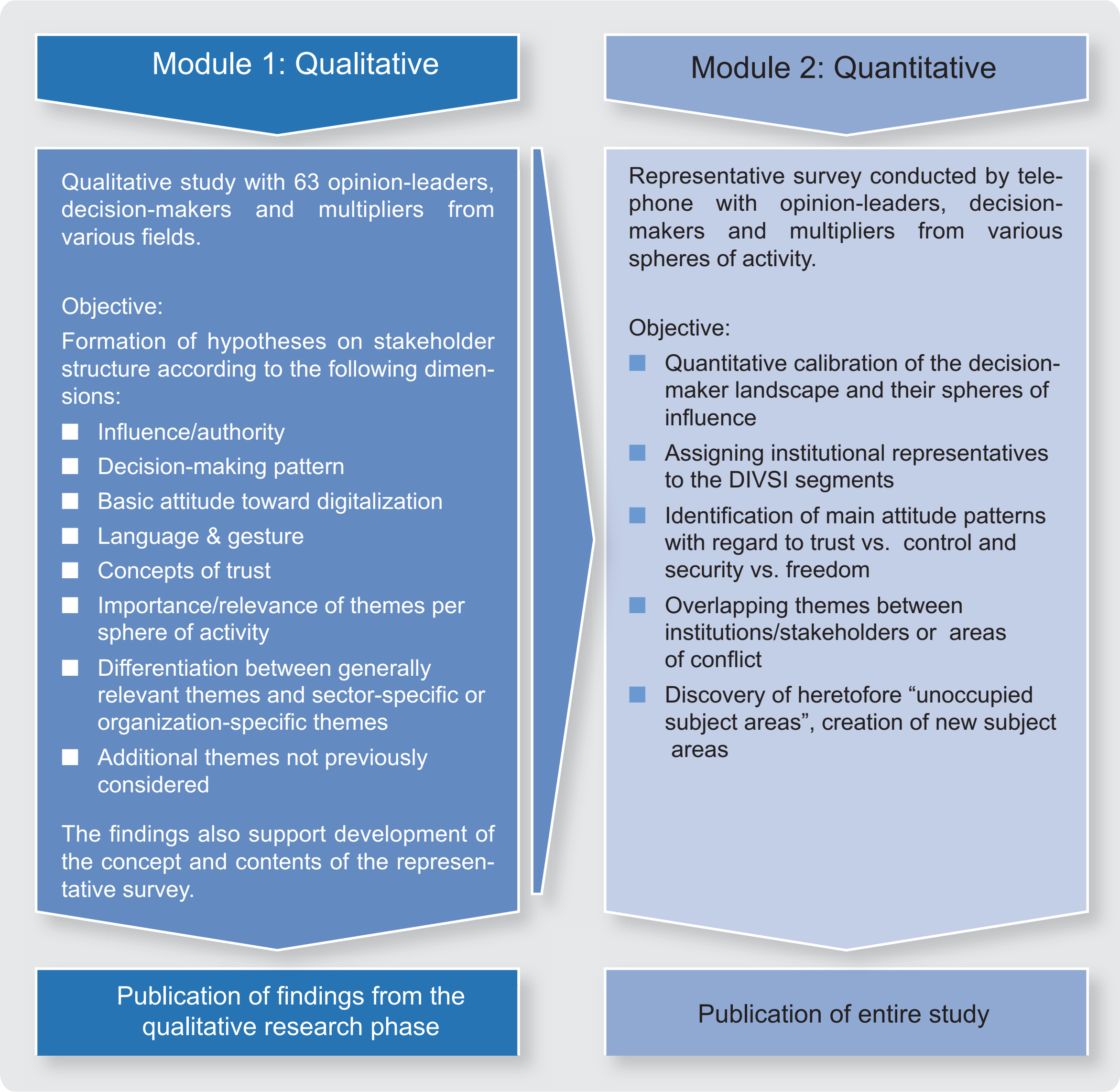
Methodology

The object of the investigation is to analyze the stakeholder structures on the Internet and shed light on who is shaping the Internet ...

- … with what means?
- … with which strategic partners?
- … against what kind of resistance?
- … with what kind of know-how?
- … with what kind of basic attitude towards digital media and the digital world?

This involved a two-step approach, which is depicted in the following graphic:

Methodology



Module 1: Qualitative

Qualitative study with 63 opinion-leaders, decision-makers and multipliers from various fields.

Objective:

Formation of hypotheses on stakeholder structure according to the following dimensions:

- Influence/authority
- Decision-making pattern
- Basic attitude toward digitalization
- Language & gesture
- Concepts of trust
- Importance/relevance of themes per sphere of activity
- Differentiation between generally relevant themes and sector-specific or organization-specific themes
- Additional themes not previously considered

The findings also support development of the concept and contents of the representative survey.

Publication of findings from the qualitative research phase

Module 2: Quantitative

Representative survey conducted by telephone with opinion-leaders, decision-makers and multipliers from various spheres of activity.

Objective:

- Quantitative calibration of the decision-maker landscape and their spheres of influence
- Assigning institutional representatives to the DIVSI segments
- Identification of main attitude patterns with regard to trust vs. control and security vs. freedom
- Overlapping themes between institutions/stakeholders or areas of conflict
- Discovery of heretofore “unoccupied subject areas”, creation of new subject areas

Publication of entire study

The interviews treated the following main topics:

- Overview of the participant's own working environment
- The role of the Internet in the working environment
- Attitude towards the Internet and digitalization
- The relevance of trust/security on the Internet; assessment of opportunities and risks for one's own field
- Perception of other players taking part in the discourse about the Internet
- Assessment of the public's level of awareness/knowledge
- Responsibility for risks on the Internet and promoting digital participation
- Assessment of contrastive pairs (e.g. security vs. freedom, bottom-up vs. top-down, trust vs. control, benefits vs. costs)
- Assessment of the future development of the Internet

To do justice to the various levels of professional involvement in the Internet among the survey participants, the interviews were guided but conducted openly and with varying focus, depending on the interviewee's respective area of responsibility.

Survey participants were selected according to a range of criteria:

- Involvement in the main sectors politics/government, business, civil society, media and academia
- Selection of survey participants at the highest decision-making levels in the respective sectors
- Individual sectors weighted differently depending on variation within the sector with regard to positions, requirements, spheres of influence/activity (e.g. larger number of survey participants from the private sector in order to include various industries and service areas, i.e. IT service providers as well as social media platform providers, financial service providers, etc.).

This broad-range of survey participants ensures that the many dimensions of today's Internet discourse are represented, and allows for the identification of the major aspects, important conflict areas and required action areas. At the same time, the interviewees introduce additional topics and the necessary differentiation for achieving adequate operationalization of the subject/topic areas.

The following table provides an overview of the number of interviews in the respective areas. A total of 63 interviews were conducted from June through September 2012.

Number	Area	Function
18	Politics/ Public Administration	• Members of the German Bundestag, Members of the German parliament's Enquete Commission “Internet and Digital Society” • Party heads • Mayors • State secretaries and State council members • Department heads from the federal ministries • Presidents of federal agencies • CIOs of federal states • IT heads from state ministries or similar
25	Business	• Senior management executives/board members • Chief Executive Officers • Chief Information (Security) Officers • Heads of public policy or similar
7	Media	• Senior management executives • Chief executive officers • Senior online editors and division heads • Freelance journalists, etc.
9	Civil society	• Board members and officers of associations, clubs and foundations • CEOs or academic/research directors • Internet activists (e.g. bloggers)
4	Academia	• Professors in respective fields

Total = 63 interviews

2.
Opinion leaders map out current Internet challenges

RISK
DEVELOPMENT
CULTURE
ACCELERATION
CHANCE
TECHNIK
MONOPOLIZATION
DIGITAL/ANALOG
CHANGE
POWER
CONTEXT
VISION
HACKER ATTACKS
SOCIETY
INFUENCE
INFRASTRUCTURE

2. Opinion leaders map out current Internet challenges

All of the opinion leaders surveyed for this study are heavily involved in the current and future development of the Internet and Internet-related policy. Many of them are also avid Internet users themselves – always eager to try out the latest devices and applications, and to discover new communication and participation opportunities for themselves. Their interest in the Internet – and the issues that is raises – is great and, in their view, it is an issue of increasing relevance due to four main developments:

a) **Massive changes on the Internet**, and a rate of change that has accelerated in the last three to five years. The increased penetration of online infrastructure and services into everyday life, new data scandals, and market concentration on a few large companies are but a few examples.

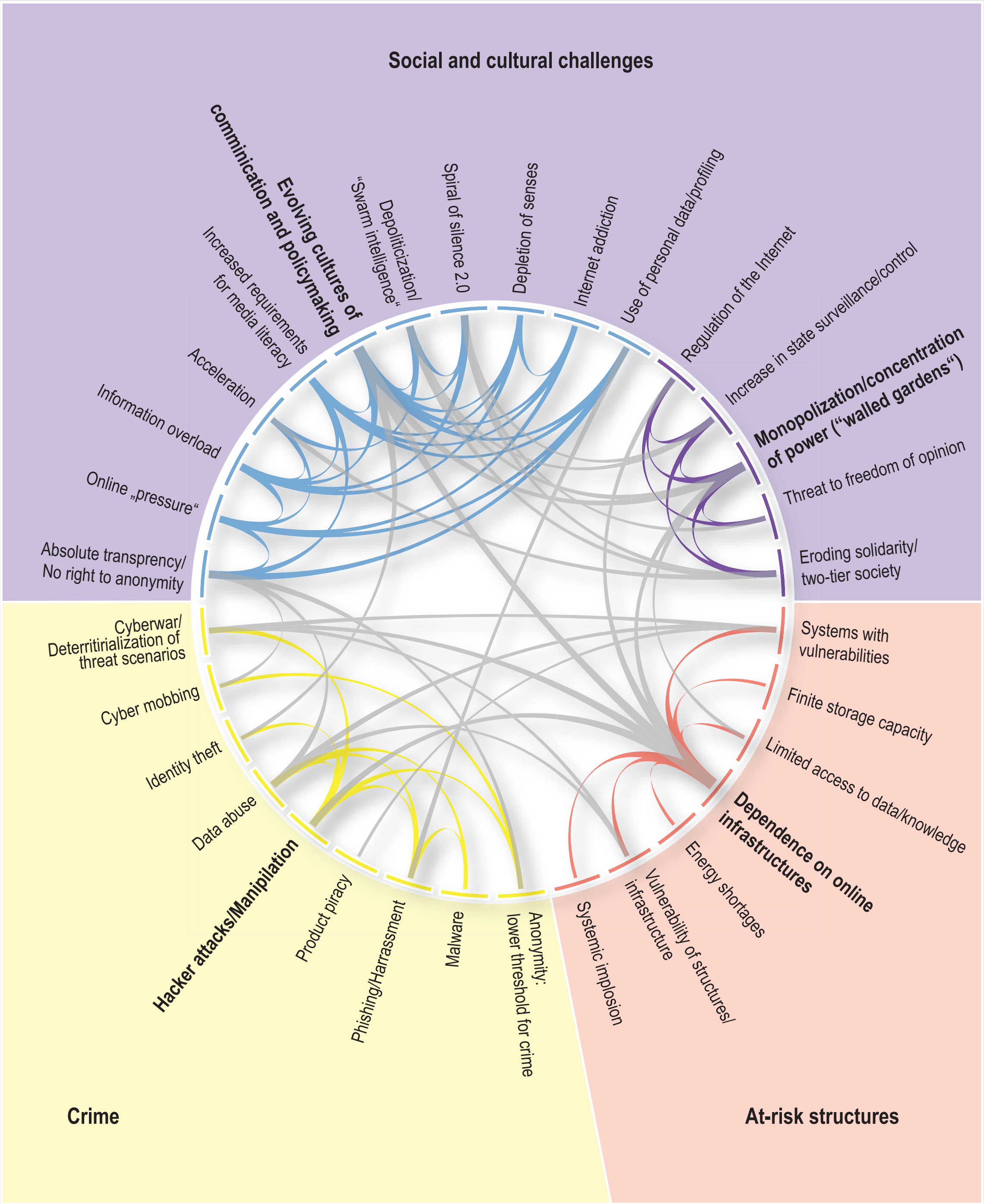
b) **Increased sensitivity – and vigilance – with regard to trust and security on the Internet:** alert users, new interest groups, new debates on fundamental issues

c) **Perceived time pressure**. Players from various sectors feel that there is a rapidly closing window of opportunity to assert oneself into the debate, to participate in the process of configuring the future Internet according to one's needs and requirements, and to initiate possible re-direction processes

d) There is still **no common language on Internet issues**, i.e. no agreement yet on fundamental orientation/direction or with regard to areas of responsibility and accountability.

The following chapters will provide a broad look at current discourse about the Internet with a focus on challenges related to trust and security on the Internet. First, one must consider whether the opinion leaders on these issues have a fundamentally different perspective on the Internet than the general population. One difference between these two groups is that opinion leaders inevitably approach the issue from a different perspective and judge developments according to how these developments directly impact their own field or area of responsibility. With an eye for both technical and cultural aspects, opinion leaders might bring a broader perspective on the issue of risk on the Internet, for example. Or they might be focused on a very specific field and bring more detailed knowledge. While not all opinion leaders necessarily have a more comprehensive view of developments on the Internet, taken together, they provide a broad and far-reaching guide to the current challenges, adding facets that expand the associative field of the public. The following graphic provides an overview of the perceived challenges. It highlights main themes and illustrates the interconnectedness of the individual issues:

Overview of the perceived challenges on the Internet


Social and cultural challenges
Evolving cultures of comminication and policymaking
Depoliticization/ “Swarm intelligence“
Spiral of silence 2.0
Depletion of senses
Internet addiction
Use of personal data/profiling
Regulation of the Internet
Increase in state surveillance/control
Monopolization/concentration of power (“walled gardens“)
Threat to freedom of opinion
Eroding solidarity/ two-tier society
Increased requirements for media literacy
Acceleration
Information overload
Online „pressure“
Absolute transprency/ No right to anonymity
Cyberwar/ Deterritirialization of threat scenarios
Cyber mobbing
Identity theft
Data abuse
Hacker attacks/Manipulation
Product piracy
Phishing/Harrassment
Malware
Anonymity: lower threshold for crime
Crime
Systems with vulnerabilities
Finite storage capacity
Limited access to data/knowledge
Dependence on online infrastructures
Energy shortages
Vulnerability of structures/ infrastructure
Systemic implosion
At-risk structures

This illustration was created with the freeware CIRCOS

This map does not yet prioritize the specific action areas, but highlights instead the major themes gleaned from the many interviews. One such major theme is the increased dependence on online infrastructures combined with the growing uncertainty regarding its vulnerability to disruption, breakdown, etc. On the Internet, criminal activity is contingent on technical structural weaknesses. This opens up another area where the need for further discussion and action has been identified. Interesting here is the significance of social challenges that result from the tension between the culture of users and culture of providers.

The following chapters will demonstrate how opinion leaders approach these challenges from their respective fields, which objectives they pursue and how they achieve these objectives. Their respective views are often shaped by their underlying attitude towards the Internet and digitalization. Their proposed solutions for increased trust and security are influenced by their own perception of **the relationship between analog and digital life**. The study was able to identify three distinctive attitude types underlying these individual perceptions:

a) **Equivalence principle.** These individuals stress quite emphatically that the discourse on this issue is nothing new. Security challenges, they maintain, exist both online as well as offline ("it has always been this way …"). Accordingly, it is not about creating new agreements and regulations, but about transferring existing regulations and applying them to the online context. They make comparisons to examples from the analog world (road transport, house construction, etc.) and invoke the idea of historical relativization ("every new medium has triggered some kind of hysteria").

b) **Summation principle.** There are indeed areas where existing regulations can be transferred and adapted, but there is also the need for new guiding principles and regulations because transfer is not always possible (in the case of cyber war or clouds, for example) and we are seeing new forms of organization and thought.

c) **Permeability principle.** In the future, the distinction between online and offline will be made less and less, as major industrial and service infrastructures will be controlled online. There will be continual feedback loops as existing analog-world regulations will be transferred to the Internet and, at the same time, new mechanisms and rules will be created for the Internet that will be transferred to the analog world.

The following chapter will introduce the players in the various sectors and consider their perceptions of current developments on the Internet, their self-perception, their appraisal of other Internet players and what they consider to be the main challenges. The subsequent two chapters will then outline various perspectives on security, responsibility and trust and address the similarities and differences among these players. The findings will then be consolidated and summarized in the conclusion.

3.
Internet players‘ perspectives

3.1.
Politics and public administration: On milestones, guardrails and trust anchors

3. Internet players' perspectives

3.1. Politics and public administration: On milestones, guardrails and trust anchors

The Internet has narrowed the gap between politics and the private citizen

For politics and policymakers, the Internet is an area of increasing relevance and importance and, at the same time, not the area that many would choose to focus on. But it is no longer an option to avoid taking a hard look at both the opportunities and risks associated with the Internet, as online infrastructure and services continue to penetrate nearly all aspects of everyday life. The rise of the Pirate Party, news reports about data scandals and the copyright debate – these are all issues that require urgent attention. These issues are out on the streets; they are not just being discussed quietly in back rooms. Fellow citizens previously thought to be more apathetic than engaged are suddenly out demonstrating against ACTA. Data privacy and security is the subject of small talk – even around the grill in small town backyards.

There are new opportunities for political participation and a narrowing gap between people and politics. Policymakers have recognized that they can no longer afford to insulate themselves from the many pressing issues regarding the Internet. At the same time, they have hardly begun to tap the potential that these issues represent. With the rapid development and pace of all things on the Internet, policymakers see themselves in a competition to acquire knowledge and get up to speed ("you need to learn and get up to speed very quickly on many issues"). It is hardly surprising that Internet policymakers often owe their success to their affinity for the Internet and to being among the first to "go online" within their respective party. But it remains an enormous new field and each individual issue requires detailed, specific knowledge.

> *"That goes for all areas – from copyright law, to the threat of phishing in the context of online banking; from e-commerce to business-to-business communication, machine-to-machine communication, and so on. And everywhere you look there's this question – who is responsible? Who is going to take on responsibility? And maybe it is simply too early for this discussion, because this is a discussion that does require certain background knowledge and some grounding in the subject matter."*

An additional challenge is that policy-makers cannot afford to just concentrate on the issues being discussed and decided upon today; they need to make the effort to increase awareness and engagement on these issues within their own ranks ("politics and politicians are among the latecomers to the Internet"). In their view, Internet policy works the same as women's policy, for example – first one must do a lot of persuading with broad strokes before addressing specific issues in a way that is relevant to the individual stakeholders.

"This is what you see in transition periods. In the early phases of industrialization there were so-called industry ministries. Today it would be reasonable to ask what the ministry of economics actually does – other than getting involved and interfering with everything. Of course you could say that the energy ministry belongs in the ministry of economics as well – and the environment ministry too – but then maybe also the ministry for social affairs and so on. That's nonsense. In my opinion, we clearly need to try to integrate [Internet policy] into the classical branches as they exist today. And the problem we have now is that in certain of these classical branches we still have blinders on when it comes to modernity."

Those working in public administration mainly regard the Internet as an instrument for improving workflow efficiency and speeding up processes. It is used, for example, to coordinate exchange and communication between individual departments and as a way to simplify communication with private citizens, even if it means giving up some control and letting things run their course a bit more. In this sense, the Internet is mainly regarded as a tool – a means to an end, but not an end in itself.

"A very important issue for us is participation. I believe that the Internet represents a great opportunity to significantly narrow the gap between politics and the people."

"IT is not an end in itself. It is there to streamline administrative processes and enable other processes that were not technologically possible up until now."

Safety and security of the people as the primary goal of public policy

Public policy and administration sees its primary duty in the care and protection of the people. With the Internet becoming more and more essential to more and more aspects of daily life, it has become one of the most important jobs of policymakers today to ensure that people can use the Internet safely, securely and with confidence.

Policymakers see themselves as the ones responsible for the framework that defines what is possible, allowed and desirable for society. They want to apply structure to the Internet, make it more tangible and understandable, and bring it in line with existing political logic. Analogies from the offline world are applied here more than in any of the other sectors (see "Analogies from the offline world", Ch. 2). Here, the equivalence principle, i.e. the transferability of principles and processes, is applied with regard to offline and online.

"And I believe strongly that we very much need to stick to conventions and maintain consistency – that we need things like compliance, validation, certification, and so on, to make sure this digital world becomes a bit more manageable for consumers. […] The new identification card or "De-Mail" and the like are building blocks that are relevant to certain goals that we have, to make the Internet more secure, to create trust anchors and to put up some guardrails."

> *“It is the job – the obligation – of policymakers and legislators to establish regulations that are fair and reasonable. […] The government must define the rules of the road, just as they do in other areas.”*

At the same time – because of the huge discrepancies in the way people use the Internet and speed with which they navigate the web – there are clear limits to what can be done. Inevitably, the political decision-making processes (the traditional march through the official channels) lag behind the development of online services and structures. A sense of obligation to time-honored democratic values and principles may in fact be out of step with a constantly changing landscape of new conditions and situations, which can then become all the more difficult to manage.

> *“Things are progressing so rapidly and dynamically, that every effort to create guidelines or adjust the parameters is always a step behind. We are constantly having to build a framework around something that already exists.”*
>
> *“And the risk grows with each passing day that the framework for any given situation does in fact not exist, because the legislative process is much, much slower than the pace at which the Internet continues to evolve.”*

When it comes to the speed and responsiveness of policy-making, an important aspect to consider is the size and scope necessary for regulations to be fair and functional. The goal should be to provide as much security and protection as possible for private citizens, while placing as few restrictions as possible on Internet culture and its innovative power. Policymakers want to function as leaders in the information society and help secure Germany’s position as a leading business location and, at all costs, avoid being perceived as an enemy of business.

> *“A positive vision of the future is that we take advantage of the opportunities that our country has in this information age – and the opportunities are great – that we seize upon these opportunities and, in a country that is becoming ever smaller due to demographic change and gradually losing its ability to compete internationally in areas such as manufacturing, that we create conditions that allow people here to enjoy growth and prosperity over the long term by developing and implementing intelligent information technology systems and creating a general framework that allows people in this country to use information technologies in a way that is exceptionally safe and secure.”*

The dilemma is obvious: Protecting the rights of the individual (the private citizen) means limiting the freedom of the other (the company) – a freedom which of course also must be preserved. This tension between these conflicting priorities is neither new nor surprising. But what happens when so-called “freedoms” run up against the existing laws?

> *“This is not a fight against business, but a fight for a part of the Internet in the sense that companies cannot be allowed to have everything. The users need to be protected. But my basic stance is to say: where would we be without Apple, YouTube and other companies? So I have a positive view of business. Business brings us forward. When businesses manage to make a profit, they invest and develop new business models. That is always positive. It becomes questionable when businesses and business models become too dominant and do not include sufficient provisions to protect users.”*

Dominance of global corporations threatens the ability to keep control of the state

Political opinion-leaders focus their attention, on the one hand, on the big “players” on the Internet – their legal infringements, their growing dominance, and the speed at which they are evolving. At the same time, they concern themselves with Internet users, i.e. those individuals who need to be protected from shams and other dishonest business practices.

Policymakers see themselves up against a certain indifference on the part of global corporations, who make it difficult for them to pursue their social/political goals and defend traditional social/democratic values.

> *“The fear that I have is that we begin to lose the accountability of our democratic institutions or that it will at least be limited as developments in the area of information technology are predetermined by market players, international developments and other forces, and that our institutions are no longer capable of putting up any opposition or resistance – that they are too slow on the European level, that we cannot agree quickly enough and that we no longer have much ability to influence developments at the national level. That is indeed a source of concern.”*

From the point of view of policymakers, companies today are not investing nearly enough in security (mainly in software). They need to be held liable for damages to a much greater extent than they are today; especially since the negative impact affects not only their own company but also the interests of other members of society. There are simply too many clearly foreseeable “cracks” for hackers to get in and compromise data confidentiality or the security of Internet payment systems.

> *“What you need in this case is a legal framework that requires companies to meet certain requirements or take certain precautionary measures; if they fail to do this then they are liable – perhaps not for the full extent of damages, but liable for a portion of the damage to be determined. […] Certainly I could say to any company: that’s your own economic risk, whether or not you secure your data or ensure data security in your company. Except that we don’t go telling a chemical company: it’s your own economic risk whether your company functions or not, if your factory blows up in your face, then it’s your economic risk, then you face the loss of production. Instead we say: as soon as it moves beyond the factory grounds, where employees are impacted, if you contaminate the environment, when third parties are involved, then you are liable. So why shouldn’t that also apply to the large IT installations of big corporations?”*

In addition, policymakers look at the business practices of the corporations – and here one often refers to the "Gang of Four": Google, Apple, Facebook, Amazon. In their view, these dominant companies are increasingly defining their own reality, own rules and own code of values that goes against established value structures, including basic democratic values. They view this gradual concentration of power not just with concern, but with fear.

> *“We really do need to be careful that we don’t end up with just a few companies worldwide, who set very strict standards and whose corporate policies play a big role in shaping the Internet.”*

Policymakers are also tuned into the user perspective and see themselves as mediators between business and consumer interests. And they all agree on one point: users know virtually nothing about Internet security. This is partly due to general naiveté, but in many cases, users simply cannot keep track of the consequences of their actions on the Internet (privacy settings on the social networks are often mentioned in this context). In these cases, basic legal parameters should be in place to protect the user from deception and manipulation on the part of providers – a legal frame of reference so that users know better what to expect and providers know that they will be held liable for damages. This liability also applies, of course, to users who behave unlawfully.

> *“[…] aside from how the technology works, the users actually know very little about what actually happens with their data! There is a general lack of awareness on the subject of data usage. Many people who say ‘anyone can have my data’ have no idea what actually happens with their information. When you explain to them what goes on with their data, they will often say right away: ‘that should be illegal’.”*

Government protection begins at the point where the user can no longer protect himself. But where do we draw the line? How much can we count on people’s ability to protect themselves? What should users be expected to know and understand? Even within the policy sector there is a broad range of opinions on these questions (see Ch. 5).

Finally, politics and administrative entities have their eye on the media as well. Because both individual users and media companies procure their information more and more online, policymakers are troubled by the lack of quality standards for journalism. But because the Internet has continued to evolve towards being the main, authoritative source of information, they consider a certain level of journalistic quality and reliability to be absolutely necessary.

> *“How can we make sure that, at the end of the day, there is good journalistic content on the Internet, so that people have some orientation and access to relevant information? Of course mass information does not always correspond to relevance – it can be part of what is considered relevant. But there needs to be quality journalism as well.”*

The need to define mandatory security standards and improve media literacy

The focus is on four areas:

a) Expanding participation in the digital world
b) (Technical) security standards
c) Protection from Internet crime
d) Awareness and education for greater Internet competency

Access to the Internet is considered the most important element of inclusiveness and broad participation. But policymakers also know that universal access has not yet been achieved. This is in part a technical/infrastructure issue. Especially in rural areas, fast Internet service (broadband) is not yet available to everyone. But modernizing the government and its administrative bodies is another important way to achieve better communication and more effective interaction with private citizens. This will require significantly higher acceptance among users, which is something that more user-friendly systems can help facilitate. Policymakers consider this the early phase in a process towards greater transparency and more open lines of communication between politics and private citizens. While some countries are working towards opening up all bureaucratic processes to the public and letting the people co-determine processes and outcomes, the prevailing view is that “offline channels” need to be maintained. Moreover, there is some uncertainty as to how much private citizens actually want to be involved in the political process.

The first and most urgent priority for policymakers is to define mandatory, binding security standards for the Internet – ideally on the EU level. It's a race against time. Critical infrastructure is becoming more and more dependent on the Internet while processes and providers are operating more and more independently. Malware is becoming a threat not only to individual networks and companies, but to entire countries. In the view of policymakers, providers have often purposely introduced faulty software to the market. And most feel that reliance on self-regulation mechanisms alone will not get the job done.

> *“As the Internet becomes more and more important, the government’s responsibility – to make sure everyone is playing by the rules – becomes more and more important too. This is already the case. My opinion is much different from the proponents of self-regulation who say ‘if everyone just watches out for himself it will work out in the end, the Internet is basically a big process of self-organization and government has no business getting involved.’ I think they are simply wrong. And it’s because this infrastructure has become far too critical to our lives.”*

Policymakers see a critical role for education – improving people’s media literacy and overall savvy. The goal of policymakers is to establish more critical attitudes towards the Internet and a greater sense of responsibility among users when accessing the Internet and its many opportunities. Schools are considered an important facilitator and a natural way to sensitize young people to the issues as early as possible. Other institutions, such as organizations, foundations and associations, are seen as possible vehicles for imparting knowledge and raising awareness among adults.

> *“Our approach is to try and teach people to take responsibility, which basically means making them competent enough so they know themselves what the actual risks are and how best to navigate the Internet so they can truly take advantage of the opportunity it offers. And that is certainly something that one can influence very strongly with policy. For example, we could include a subject like ‘Risk and Opportunity in the Digital Age’ in the school curricula and make sure that kids are learning about this. After all, this is something that is just part of our lives now, and the job of the schools is to prepare people for their lives.”*

3.
Internet players‘ perspectives

3.2.
Business:
On opportunities, speed and good prospects

3.2. Business: On opportunities, speed and good prospects

Internet as a determining factor today

Life without the infrastructure of the Internet would be unthinkable for companies today. By opening new sales and marketing channels and enabling more effective customer relations, the Internet makes it easier to conduct business – in home markets and around the world. But more than that, it serves as a source of inspiration for innovative ideas, products and services. For many new companies, the Internet is the foundation of their business model. It therefore comes as no surprise that some in the business community are downright euphoric about the Internet and the opportunity that it represents.

> *"I associate the Internet with incredible potential. Not just for new business models, which we have now also realized in our own company, but also for existing companies, which can seize upon this opportunity to really re-invent themselves with regard to process optimization and customer relationships."*
>
> *"I myself am convinced that the Internet has brought one of the most defining changes in the last 100 years. I won't say the last thousand years, but certainly for my generation and the next generation it will bring change more than any other single thing […]. This means a huge opportunity. And it goes for all areas of life – from work to entertainment, to the way people communicate with each other. Everything is changing."*

The Internet is considered less a means to an end (as is common in the public sector, for example), and more an all-encompassing feature of modern life. The Internet is taken for granted as the natural setting for business and work. It is simply there. Like water or air, it is a given, a natural feature of today's reality, a "force of nature" that one can neither avoid nor call into question.

This is one reason why opinion leaders in business only rarely talk about the risks associated with the Internet. When it comes to the Internet, many business leaders seem to regard a standard risk vs. opportunity analysis as out-of-place, inappropriate, and even annoying.

> *"For us it is an opportunity more than anything else. […] I really don't think you can argue against a mega-trend like this in terms of possible risks. It's like saying you need to be able to swim before you know whether the ocean is an opportunity or a risk. Yes, the ocean is there. And if you live on the ocean you need to be able to swim. That's how I see the Internet. We simply don't think in terms of opportunity or risk. It is like a force of nature. The ocean is simply there."*

> *“I don’t see it in those terms at all. What are the risks of a water main? What are the opportunities associated with a water main? For us, the Internet is like a water main or an electric cable.”*

While business leaders are certainly aware of the risks, they consider them inherent to the system, and by no means do the risks devalue the opportunity that the Internet represents. It is much more about accepting the existing risk and dealing with it head on. Overall, they believe risks should be regarded more as challenges and tasks rather than hazards or threats. Risk management and security management are simply part of the challenge, and part of the process of tapping the potential of the Internet.

The prevailing attitude among business leaders is characterized by great optimism, a “can-do” mentality, self-confidence and faith in progress. Risks – especially those of the technical nature – are considered eminently manageable. There is no desire to turn back from what has been achieved so far and, in their view, there is no “collective coercion” towards digitalization.

They acknowledge the fact that 39 percent of Germany’s population is still classified as “Digital Outsider”*, but are quick to explain this as a natural part of this transitional period.

> *“Yeah, yeah, it is a large group of people, but the Neanderthals were also a large group and they of course died out in the end. Quite honestly, I don’t understand this group of people at all. Let’s move on to the next question.”*

Companies see themselves as captains on the sea of opportunities

The private sector lives with, in and from the Internet. Its use and configuration makes up more or less the core business – not only for designated Internet companies but also for other large corporations. Business leaders see their own business activities, ideas and innovations – along with the increased use of social media – as the key drivers of the Internet revolution. It is their initiative that has made it possible for the Internet to evolve with such blinding speed into such a gigantic marketplace of infinite possibilities (“without us there would actually be no Internet”). They see themselves as captains on the sea of opportunities. They are the ones with a clear orientation and grasp of the situation; they understand their business and know what it takes to succeed. While the policymakers see themselves as slightly behind the curve of developments, these "captains" see themselves at the forefront of the movement – as the (technological) avant-garde. This is where new things are being created and the future defined; this is where the content and course of the Internet is being decided.

* See the DIVSI Milieu Study, https://www.divsi.de/divsi-milieu-studie

"Change is always a challenge, but ultimately also an opportunity. We want to take advantage of the opportunity and take part in shaping the future – not sit idly on the sidelines. […] It is playing a role in more and more areas of life. […] IT continues to enter into more and more areas of life. I personally feel a certain obligation to recognize this trend, to take part in it and further its development."

These business leaders have worked hard and invested a lot in the development of innovative products and services; they have gradually gained the trust of users and customers; and they, themselves, have made the commitment to new ways of doing things (such as managing their own financial transactions and internal communications). They have created new jobs and helped ensure that Germany remains among the world's leading IT locations. So they do not want other players putting up any unnecessary roadblocks. In their view, the trend is towards more and more regulation, and forced attempts to initiate a debate driven by fear. And many of them decidedly reject this approach.

"I find some of the solutions being proposed – mainly those involving increased government control – to be dangerous and totally misguided. I just don't want the minister of the interior protecting me while I do business."

Government is an "overly cautious" impediment to economic growth and innovation

In order to survive in the fast moving and constantly changing environment of the Internet, and to continue to expand and strengthen their market position, business leaders emphasize how critical it is to not only understand the rules of the game on the Internet, but to play a role in defining these rules. They want to tap the potential of the Internet in its entirety, develop innovative products and new business models. In their critical eyes, policymakers have succumbed to a kind of "regulation craze". Companies fear that government regulation will knock them off course – or at least limit their cruising speed – and that they will lose their ability to compete internationally. At the same time, they stress the futility of this approach, saying that the global Internet space cannot possibly be controlled anyway.

"To continue along this track of overly fussy legislation on the national level will lead us absolutely nowhere. I believe this impedes economic progress; it will have a negative impact on business locations, and the legislative process will never be fast or efficient enough to really protect people. That's my take on it. This doesn't mean, of course, that our politicians will drop the issue. It's too big an opportunity to promote a cause and attract attention. That much is clear."

"The notion that we can somehow censor the Internet is just not realistic. It's like the ban on alcohol in Saudi Arabia. If you're in a hotel, you won't find it anywhere, you can't get it. But if you're invited into a private home, they'll open the cupboard and offer you any kind of wine or whiskey you could ever dream of. And your Muslim hosts will be offended if you don't get drunk. It's really the same with the Internet. You can access anything your heart desires – because it is simply impossible to control access to the web."

The insinuation is that decision-makers in the political arena suffer from impaired vision – and that they are even a bit clueless. But it's not a subtle insinuation. In fact, the competency of policymakers on the issue of Internet regulation is being openly called into question. And in the view of business leaders, the prospects for effective and productive dialogue are not good. Politicians and policymakers are, in their view, simply too far removed from the issue. Their knowledge and experience is insufficient for them to understand the scope, importance and consequences of their decisions.

"If I just try to imagine who I could talk to about these issues in the Bundestag or in the federal government or at the second-level of government, on the state secretary level, I come up with exactly this [uses hands to form a giant zero]. One more time for the audio tape: zilch. There is no one."

But it's not just politicians and government officials that get in the way. Business leaders also accuse the media of weakening the position of Internet companies with their one-sided reporting, which tends to highlight the risks of Internet commerce without talking enough about the added value and many advantages. According to this picture, the media is striving too hard towards greater transparency and is often overly critical. Their reporting tends to exaggerate and unnecessarily scandalize, they publicly discredit the Internet companies, bring disrepute upon them and the industry and ultimately cause users to become insecure or even to lose their confidence in the system.

"But as we all know, the media is also responsible for conducting honest and thorough research before printing the big headlines – not just for publishing half-researched stories that continue to upset and unsettle consumers."

"The media landscape has been thinned out so much in the last several years that serious journalists are now few and far between. I guess everyone gets a voice today, regardless of substance. And that has nothing to do with fairness. It's just stupid. But that's exactly what's going on. So if someone represents a minority opinion – as long as it's extreme enough or good enough for ratings – he'll get his seat at the talk show table."

When comparing Germany to other countries around the world (in particular USA), business leaders note the conspicuous trend in Germany – of all places – towards exaggerated public criticism of Internet companies for their business practices. This stirs up fear and insecurity on the part of users, which, in their view, is both unnecessary and avoidable. According to business leaders, security concerns in Germany result in totally excessive measures, especially when it comes to data security.

Germany’s data protection laws are already some of the world’s most rigorous, but this is apparently not enough, since policymakers insist on grappling with them on a daily basis.

From the point of view of business leaders, a company that is committed – and indeed obliged – to making a profit is bound to certain practices inherent to the business model. And this doesn’t necessarily make these practices objectionable. For example, providing free online services is not economically viable without some form of “payment” on the part of users in return for these services. The view is that companies are already under enough pressure from the competition and they should not have to face additional hurdles in a battle with regulators and policymakers.

Business leaders suggest that a lot of people in Germany are misguided. The virtual character of the Internet often “tempts” users to regard hidden processes or procedures with greater skepticism as compared to similar situations in the offline world. Business leaders see it as an important task to raise awareness on this – to make people understand how often they trust service providers in the "real" offline world without fully understanding the situation or its implications.

> *“I don’t think that monetizing data should be regarded as fundamentally wrong. The question is how the data is then used. I have the feeling that in Germany, one stops right there and says: oh, the data is being monetized – that’s really horrible. The media is of course happy to scandalize it. And that makes people insecure. You could even say the media upsets the users more than necessary about 95 percent of the time. […] I mean, no one is interested in the individual data. Take Mrs. Schmidt in Stuttgart. Who cares?! No one is looking at her! The data is simply organized according to segments so that Mrs. Schmidt can receive segment-specific advertising and information. I’ve often asked myself: what is so bad if, for example, Mrs. Schmidt, who never buys pork roast anyway, no longer gets any pork roast advertising in the future?”*
>
> *“There are a lot of people who say: hey, I’m not stupid enough to pay with my credit card on the Internet. But then they go to Naples and hand over their credit card for half an hour in every restaurant they eat in. The staff could be in the back room making as many copies as they want! […] On the one hand they’re running around with their paranoia saying ‘I'll never pay with a credit card on the dangerous Internet’. But, at the same time, if they feel they have it physically under control – like at the Pizzeria in Naples – then they think nothing can go wrong.”*

Companies complain that policymakers are allowing the most inexperienced and naïve Internet users to set the standard and using this as the basis and justification for their restrictions and censorship. This, they say, is rooted in the tradition of the protective welfare state.

> *“It’s getting to the point where I can’t stand Germany's do-gooder approach anymore […] I’m starting to get the feeling that I don’t actually belong to myself, but that the generous state has loaned me my body and my existence and is now making sure I don’t do anything stupid with it. More and more, I am seeing too many people with normative ideas about a proper existence who are trying to tell me how to live my life. […] I am very concerned that we really will become a paternalistic dictatorship.”*

Overall, the business leaders surveyed see themselves up against a critical social climate, in which the configuration of the Internet is the subject of a heated debate.

Ensuring competitiveness by actively shaping public and political opinion

A central challenge for companies is to secure their market position and to fend off threats to their competitiveness. Especially on the Internet, companies see themselves up against an increasing number of competitors and new levels of cut-throat competition – all of which is made even more intense by the relentless speed of it all. The leaders of today, they point out, can easily be forgotten tomorrow (“nobody even mentions Yahoo anymore”). The companies therefore consider it all the more important and desirable to do business in a social and political environment where decisions and public dialog reflect positively on the meaning and importance of Germany as an Internet location. Often enough, however, policymakers are making decisions on things that elude their own grasp. As a result, they fail to sufficiently consider the economic feasibility factor when pursuing their “socially desirable” goals.

This is why business is so intent on assuming an active role in the Internet discourse and influencing the process of public and political opinion-making. Business leaders see the need to direct the regulatory process into the right channels – if it cannot be avoided altogether.

> *“I think government can specify the framework to an extent, but the solutions ultimately need to come from the private sector.”*
>
> *“The regulatory environment of the future will of course have a huge impact on business. Take the whole discussion surrounding ‘the right to be forgotten’, as an example. Nice ideas, but you have to question whether we are realistically capable of living up to the standards we set. […] This is why we take a very careful look at what we consider feasible, what we support and then also the instances where lawmakers maybe have lost their grip on what is realistically doable.”*
>
> *“Before we become subject to government regulation (take the issue of cloud computing, for example) we would of course first try to create options for the providers and instill sufficient trust so that we do not actually need the government regulation at all.”*

However, business leaders do see the need for regulation where it pertains to the security and reliability of their own business model, i.e. to user trust and confidence. Users should be able to expect a certain level of security with regard to personal data protection and a certain level of legal protection that secures their Internet-based transactions, so they can navigate the Internet “safely” and remain willing to do business.

> *“I do believe that regulations are necessary that define how reversible transactions should be. If a business transaction is completed on the Internet, for example, there needs to be the option of canceling the transaction just as there is with door-to-door sales transactions. I believe these regulations are necessary – already exist to an extent – but that they are also sufficient.”*
>
> *“As I said, the regulation of data privacy, legal shelters with regard to identities and so on – I consider these things absolutely necessary.”*

Regulation is considered particularly important when it comes to the protection and sale of the companies’ own products and services (e.g. protection from product piracy, copyright regulations, secure processing of online financial transactions).

> *“I would say that sooner or later German material law will have to address and define the issue of private copying more clearly. For us, defining more clearly of course means putting greater limits on it. But I don’t see that as a disadvantage for consumers. I really think that on this issue – especially on this issue – the user is entitled to understand.”*
>
> *“For us, piracy is of course a huge problem; for us and for everyone else. There are even platforms on the web that do nothing more than collect content on their platform, or to link, and then make money with their own service by selling access, data access speed (data rates) and running advertisements on their platforms so that they ultimately even earn money with our content.”*

Security becomes most relevant for companies when a lack of trust threatens their own business success. This applies to their customer relations. Especially in the virtual world of the Internet, companies know the importance of taking seriously the fears and concerns of the customer and to be reachable and actually available to handle questions and problems. Long-term customer loyalty based on trust (understood as the sum of positive experiences with regard to security and reliability) is the foundation for doing business. Trust is often established by way of a slow and painstaking process. Inadequate internal (security) management and lack of transparency, along with negative reports in the media, can destroy this trust very quickly - and thereby threaten a company's ability to conduct business. Business leaders inevitably view investments in Internet security in terms of costs vs. benefits. The bigger the company and the greater the fear of damage to the company’s image, the greater the company’s investment in security measures is likely to be. This makes it less about maximizing security for the user and more about minimizing reputational damage and the associated loss of business.

> *“When you read in the newspaper that [name of company] has been compromised, that has business relevance for us. And of course economics is what drives our decision-making and operations as well. Investments in information security are a logical step designed to avoid reputational damage for one, but also fines and other penalties.”*

3.
Internet players‘ perspectives

3.3.
Civil society representatives: On endangered visions, limited participation and the search for a consensus on values

FUTURE

OPEN SOURCE

SOCIETY

FREEDOM

CONSENSUS OF VALUES

CODE OF VALUES

AUTONOMY

TRANSPARENCY

PARTICIPATION

EDUCATION

SELF-REGULATION

ACCESS TO KNOWLEDGE

ENGAGEMENT

RESOURCE

INTEGRATION

CULTURAL CHANGE

VISION

REVOLUTION

3.3. Civil society representatives: On endangered visions, limited participation and the search for a consensus on values

The Internet as the engine of social change processes

When it comes to the pros and cons of the Internet, civil society representatives have their eye on the "big picture". They want to broaden the focus beyond technological and economic factors and expand the limits of the discourse beyond the Internet's obvious – and in their view dubious – potential for greater efficiency or creating new markets for products and services. Champions of civil society are interested in the Internet as an agent for social change processes. They are less interested in providing answers to pre-formulated questions. Instead, they want to make sure the right questions are being asked. How can we use the Internet to make a positive contribution to society? How does the Internet contribute to a functioning community? How can the Internet facilitate more participation across different sectors of the population?

Civil society representatives regard access to knowledge and information as critical to participation in today's society. In their view, the Internet offers the revolutionary opportunity to increase access to knowledge – to make the knowledge resource available to as many people as possible and thereby significantly increase opportunities for education, integration and participation. The Arab Spring has become the classic example of how the Internet and social media can initiate democracy movements.

"If you understand information as the gold of the 21st century, then it's clear that access to information and the right to work with the information – in other words, not just the access but also the option to process or use the information – becomes an issue of social participation and integration."

"The Internet makes it easier to show up, makes it easier to participate. And if you believe in democratic theory, this will improve the quality of our decisions in the future, since more people are involved and participating."

Despite these more euphoric appraisals, there is also disillusionment. Civil society representatives say the Internet was intended to be different ("it wasn't meant to be like this"). They point to disquieting changes in the last several years that threaten to undermine the Internet's potential and original intent. There are signs, they say, that the Internet is increasingly being incorporated into the established power structures. They are disappointed by what they see as a trend towards increased economization of online content, increasingly cut-throat competition for a share of this valuable knowledge resource, and its resulting scarcity. These developments run counter to the original Internet ideals and, in their view, significantly limit user freedom.

> *"That is where I do indeed see a serious threat. More and more of the content on the Internet is no longer free in the sense of free access and usability. By no means do I mean this as an argument on behalf of the Internet's 'freebie culture', which is not my area of interest anyway. No, what's meant here is that the Internet offers tremendous possibilities for free access to knowledge and information for all people."*
>
> *"The problem is with the logic inherent to capitalism, which says that one always has to earn money with everything. So if I have something with which I can potentially earn money, I cannot then just share it with others for free."*

Personal commitment to creating a free Internet that is a knowledge resource for all

Most civil society representatives consider themselves to be among the first Internet users. In their view, they recognized and took advantage of the Internet's tremendous potential from the outset. Many even made tangible contributions to bringing the Internet into the world and making it available to the public. The history of the Internet is often closely tied to their personal biographies, even on the emotional level. They remember exactly when they went online for the first time or remember clearly the first feedbacks they received on their blogs.

> *"Back then there was, de facto, no Internet access in Friedrichshain. So together with the free broadcasting initiative that was emerging at that time, we used directional antennae […] to transmit Internet into town and set up the first open Internet café on Boxhagener Square. We wanted to provide people with free Internet access, but we also offered several courses […]. It was really about empowerment, about learning how to acquire knowledge for yourself, by yourself with the help of technology […] and to find your own approach. It was for individuals as well as for groups such as political groups."*

These players believe strongly in the Internet as an open-access space that essentially unifies the world's history and knowledge. Through their personal commitment and initiative, they work to establish and defend values such as transparency, personal autonomy, freedom of speech and unlimited access to the Internet's knowledge resources. They see themselves as important influencers of policy – as Internet experts who are in a position to educate policymakers, point out the potential consequences of proposed actions, and help policymakers make better decisions when it comes to trust and security on the Internet.

> *"When you speak to Wikipedians, they are at least aware of the fact that what they're doing here is classical volunteer work. They are not getting paid, they are under no obligation to do anything, but they are getting involved on behalf of the community, society, the common good, and are building a common knowledge resource."*

Industry and government are locking people out of the Internet

In the early stages of their Internet advocacy, these civil society representatives were focused mainly on the users and ensuring more and improved Internet access. Today they have shifted their focus on to the social sectors that, in their view, are hindering both participation and transparency. Their two main culprits are large international corporations and government, and although the interests and goals of these two players are quite different, the civil society representatives maintain that both interest groups are pushing ahead with processes that could potentially close off the Internet.

> *"The Internet is at risk – at risk of being regulated by interested parties and losing its freedom, its room to maneuver, and its potential to expand and enhance democracy. We are trading this in for the reward of increased security and control, which of course may be very relative."*
>
> *"For me, the Facebook example runs counter to the spirit of the Internet. It's exactly the opposite of Internet. You could actually say that Facebook is the death of the Internet. It's a closed off space, where very specific strategies are being pursued that make it as difficult as possible for users to ever get back out of this space."*

Civil society representatives see government and the private sector pursuing a common goal – to "lock up" and "lock in". Even if their intent is different, the result is the same: the user's access to the Internet becomes neither unrestricted nor unconditional. And if he does get in, he cannot get back out, because the Internet (whether in the form of data-gathering companies or government regulatory agencies) forgets nothing, retains everything and continues processing and exploiting contextualized data, i.e. profiles.

According to civil society representatives, government and the private sector pursue different legitimization strategies to justify their actions. Government, they say, intimidates with its fear-driven discourse and offers people care and protection (welfare) as an antidote. Regulatory control measures are sold as protective measures to gain people's trust. Instead of empowering people, government takes the paternalistic approach, which can then lead to almost absurd forms of over-regulation.

Meanwhile, the business landscape is characterized by increased monopolization. "Data kraken" hoard entire cultural collections and libraries, then require users to release personal data before they can take part in interaction or gain access to content. The user feels pressure to accept these conditions, especially since some providers have evolved into infrastructure service providers, who have no competition and are the user's only alternative. Civil society representatives remain hopeful that the self-destructive power of competition will, at the very least, allow new players to emerge onto the market. And they suspect that today's top players in business underestimate the power and influence of the users.

"The players that have highly desirable products and services have a lot of power, that's for sure. There are the Googles and Facebooks, who have achieved the status of 'infrastructure players' for one reason or another. But ultimately their power is finite, of course. Take Yahoo. No one even mentions Yahoo anymore – at least not in Germany. So even these players can't afford to take too many liberties. And if someone comes along who does it better, then it's a new game, although that is certainly difficult to do, no question. Take Ebay. To be honest, Ebay is total garbage, but there still isn't anyone better on the market."

The need to democratize knowledge and decelerate regulation

In line with their goals to preserve the Internet as a free, open and accessible instrument for use by any and all people, the civil society representatives see it as their primary task to protect the Internet – from government's regulatory efforts, and from the forces of unfettered capitalism.

"This classic idea that we can just 'leave everything to the natural play of forces' has not exactly proven itself a success over the last 10,000 years of human history."

Civil society representatives see open source initiatives as one alternative to economically-oriented, commercial business models. But many such alternatives have very limited distribution and remain relatively unknown (Diaspora as an alternative to Facebook, for example).

Civil society representatives want government to abstain from additional regulation. In their view, the legal framework of Germany's basic law (constitution) can be applied just as well to the Internet. They also advocate a more relaxed approach to security issues and see themselves as decelerators of overly hasty legislative action.

"For me there is a very clear need for government action – they need to allow more and try less to solve problems that do not exist."

Civil society representatives want to see a coordinated and consistent Internet policy that does justice to the Internet's dynamic evolution. They also want to lead negotiations – ideally an international negotiations process – to establish a consensus on common Internet values. In their view, we are now in a sensitive transition period. There are still things that are technically possible that have not yet been done; and it is not yet technically possible to do everything that one could do. This makes it all the more important, in their view, to establish an international code of values that is accepted by users around the world. As the civil society representatives search for new ways of self-regulation, they remain highly optimistic about what they consider the core values of the Internet community.

> *“No, you certainly cannot hash out a system of criminal law by way of social consensus. That goes for the road traffic laws too – I’m very thankful that someone else has established those rules. And there is a need for that kind of thing on the Internet too. Criminal law has to apply to the Internet just as it does everywhere else. Nobody is ever going to seriously challenge that logic. But in other areas I would really like to see us rely more on the possibility that we can negotiate and work out rules, regulations and procedure amongst ourselves. […] Especially from politicians and policy-makers, I would like to see more trust in what we call common sense, more trust in what we call citizen involvement, less compulsion to take political action, and the occasional willingness to wait out the possibilities. Even if this means risking a gap in the regulation, which will certainly be taken advantage of.”*

Today’s Internet community is in the process of negotiating minimum standards, guidelines and codes of values. According to the civil society representatives, extreme phenomena and even taboo breaches are always going to accompany the introduction of a new medium, but these phenomena will be relativized and marginalized with time through mutual agreements and consensus building. The principle of self-regulation, they point out, does include the possibility of punishment if the agreed-upon code of standards and regulations is violated. This means that Internet users, for example, should have some leverage against providers – also in areas beyond criminal or legal concerns. It’s not clear who will guarantee this. Ultimately it is just as important, if not more important, for users to be able to protect themselves on the Internet.

> *“There are no neat and tidy enforcement mechanisms. I can’t go to Facebook, for example, and say, ‘hey, you said this is your code, you said you would abide by it, but you don’t abide by it.’ You’ve got no chance of being taken seriously there.”*
>
> *“Of course I cannot assume that everything will work out fine and just sit back and make myself comfortable in my hammock. That’s a false assumption and I can’t let that happen. I need to develop a kind of healthy skepticism with regard to certain mechanisms and things out there. Even if I wish these things were different, in this case they just aren't. This could apply to data protection regulations or things like that.”*

3.
Internet players‘ perspectives

3.4.
The media:
On conflict areas, power constellations and necessary relativization of opportunities and risks

3.4. The Media:
On conflict areas, power constellations and necessary relativization of opportunities and risks

Internet as key technology and topic generator

The Internet has fundamentally changed the media sector. The majority of media professionals surveyed for this study have experienced, themselves, the speed with which work processes and techniques have changed over the course of their career. They often recall with a smile their introduction to the Internet, and how the Internet gradually made its way into their everyday routine over the course of their career and became more and more indispensable. Many experienced the Internet in its earliest days and talk about this time as if it were ancient history (“it all started with BTX”; “in the old days we still would print out and send a fax”).

Today, no one disputes the Internet’s status as a key technology. In the media sector especially, the Internet is both the beginning and the end, it is both the tool for work and the focus of work, and it is difficult to imagine business without it. It is, in today's globalized world, the all-encompassing channel through which everything flows. And for media professionals, it is difficult to find anything in their environment that is not controlled and managed online ("perhaps the coffee machine").

“The Internet is everything. Everything we do is Internet. We publish on the Internet, we research on the Internet, we communicate through the Internet, write dozens of emails on a daily basis. The telephone gets used comparatively little. Even our internal communication – here among the editorial staff – happens mainly via networks, computer screens and keyboards. With all the detail work and all the things that need to be constantly reviewed and changed, it would be impossible to get it all done in face-to-face meetings. The Internet is inherent to our work, it is simply inseparable from what we do.”

“The Internet makes it possible to even find like-minded people; I can meet them, coordinate with them and develop and plan new projects. The Internet has made everything much, much simpler. […] Simpler, faster and more flexible. It is much easier to track down experts on specialized topics, for example, and I am no longer as dependent on the mainstream media filter.”

Media professionals are tuned into the far-reaching implications of the Internet and its impact on society as a whole. With its all-encompassing character, its penetration into all sectors of society and all spheres of life, the Internet provides media professionals with extremely topic-rich terrain with a lot of conflict potential. It provides them with all the news elements they are looking for – proximity, consequence, conflict, variation, etc. – and all at a tremendously fast pace.

"We are in the middle of a revolution, the biggest revolution since the printing press, probably bigger. The world in which we live in today is changing faster and more fundamentally than it has even over the course of the last several centuries. Sure, the airplane, automobile and television also changed the world, but not at this pace – and by no means did they penetrate daily life as quickly and extensively as the Internet. So it's a fascinating job, and very exciting, to be taking part in this revolution as a journalist and as someone who can – at least to a small degree – help us avoid the kind of political decisions we come to regret in the future."

From this perspective the Internet represents, without question, a huge opportunity for all of society. It facilitates communication and social coexistence, it expands life's horizons and opens up totally new possibilities. The Internet also changes our basic notions of social integration and participation; not only by offering new options and opportunity, but also by introducing new requirements. Today it is no longer just an option to learn "from the Internet" how to network. It has become a must. Even if you're not a journalist, say the media professionals, you simply have to be online and networked. You can no longer afford not to be.

"If you upload content today onto the Internet that isn't cross-linked or networked, it will fall through the net, it will be worthless. People in today's workforce who are not networked, will also fall through the net and be considered value-less. The Internet is changing our whole concept of value."

While focus among media professionals is largely on the opportunity that the Internet brings with it, there is also talk of the risks it poses. Despite their fascination with the Internet's achievements, they also want to raise awareness for its pitfalls and potential dangers. The Internet itself can become a risk, they say, when it is "poorly done". In their view, the Internet is becoming overloaded with a never-ending stream of new functionalities. New applications are constantly being added and integrated without knowing whether the basic underlying systems, on which we become more and more dependent, have even been adequately secured or backed up.

"These days we are adding so many new functionalities to the Internet and are becoming so dependent on the Internet in so many areas, that we are losing sight of fact that we are maybe moving too fast and not safeguarding certain things adequately. We're not thinking about it enough. And there is another risk. […] The techies overlook the fact that they're not doing enough for security and reliability. Huge buildings are being constructed on very, very weak foundations. Eventually parts are going to collapse. And when it does collapse, there will be a huge collective step backwards in terms of acceptance."

Media as observer and commentator on fast-moving change

The media professionals see themselves as specialists on the subject of the Internet and new communications technologies. They try to consider the Internet from different perspectives, to weigh the respective pros and cons, and to facilitate discourse among the various players. On a personal level, they tend to be optimistic about the digital future. But in the professional context, they are also happy to work with disaster scenarios, such as a “data Fukushima”.

Media professionals see themselves as critical observers of the fast-moving change happening before our eyes. They want to be the ones shaping the discourse in the media and raising public awareness for previously neglected aspects of the Internet debate. An example:

> *“I am amazed by the carefree attitude of companies like YouTube, Facebook, etc. They have these gargantuan data storage requirements and are having a significant impact on the overall data transfer rate on the Internet. But they skirt the responsibility of investing in this infrastructure and totally leave it to the carriers and network providers. […] It makes me very grateful that there are a few institutions out there who have at least forced Google to say how much energy it is actually consuming. We talk a lot about the big energy turnaround, new efficiency standards and all kinds of things. Meanwhile Google’s needs are the equivalent of a nuclear power plant or maybe two – and that’s just for Europe.”*

Media professionals want to ensure transparency and bring injustices to light wherever possible. One way to do this is to broaden the perspective to include the international playing field (“What is the situation in Germany?”, “How are the other countries dealing with these issues?"). Their approach is to consider the issues from as many different viewpoints as possible. They are well aware of their responsibility as reporters and want to remain as neutral as possible in their efforts to moderate the discussion in the media ("no Internet evangelism"). They want to relativize both excessive euphoria and unnecessary fear. In dialogue with the relevant decision-makers from other sectors of society (politics and business in particular), their goal is to influence social discourse, point out possible solutions and steer decision-making processes in the “right” direction.

> *“We consider it our responsibility, of course, to support and contribute to this process of social change so that it takes place in a sensible way – in a way that avoids excess in any one particular direction and thereby any undesirable developments.”*

At the same time, media industry professionals are being forced to adapt to a new concept of the public sphere and public opinion. The Internet makes it possible for the user to become his or her own broadcaster – by commenting on online articles or through the use of social media. This changes the position of the journalist significantly, who is then no longer the lone “gatekeeper”, but engaged in a dialogue with other players on the field. Journalists today tend to view this in a positive light, i.e. less as competition and more as an enriching new source of content that is faster and more “real”.

“Currently I am taking a close look at how the Internet is changing the public sphere, especially the impact of content published by non-journalistic players. […] I am focusing especially on the issue of leaking, which has always been associated with journalism, of course. But today leaking is also practiced more and more by non-journalists. This is of course a big help to journalists, since the law puts limits on what they can do.”

Opportunity and risk assessments of other players lack balance

The media sees government and the private sector as the two major players in the power struggle to define and shape the Internet (“here it’s the tortoise vs. the hare every day”). And the key element to this story, according to media professionals, is the game being played with people’s fears.

“The German mantra is: always keep an eye on the risks. […] There are lobbyist groups that play on fear by pushing the issue of data privacy and data security. They are trying to impede progress on greater transparency, because transparency is probably bad for their business. As a result, things are becoming so complex in Germany – and so excessively secured – that people can hardly use them anymore.”

But, according to the media professionals, political decision-makers often have only rudimentary knowledge of the Internet, its special characteristics and its many potential applications. And without more extensive knowledge and experience, they simply cannot perform their assigned oversight function when it comes to the private sector.

“The politicians themselves are also part of the problem in Germany. The people now sitting in the Bundestag, for example, don’t necessarily understand this issue very well.”

“Very few individuals in our regulatory agencies in Germany are active on the Internet themselves or particularly knowledgeable about it. I bet you could count them on two hands.”

Interestingly, nearly all Internet “players” from all sectors seem to think that they are more knowledgable or experienced on Internet issues compared to the other players. They even allege ignorance within their own industry (if not within their own specific medium). They themselves are experts who know the terrain; everyone else has trouble explaining things or relies on fear mongering, etc.

“If you watch the Tagesschau or read the Stern, the issues come across very strangely […] As someone in the business, you think to yourself, my God, they haven't even understood it. My God, they're just scaring everyone again, or they explain it in such a way that no one can understand it. The only thing the viewer understands is that he better be careful. It's a shame, really, that there are so few people who can talk about these issues clearly and understandably in the mainstream media.”

While media professionals acknowledge the risks, they argue that the downside tends to get exaggerated and overdramatized. In their view, the freedom that the Internet offers is inevitably accompanied by a degree of uncertainty and insecurity, but this is also something that an evolved society – and the users within that society – can cope with. People are being taken for fools, say the media professionals. Policymakers and business leaders assume that people are capable of nothing.

“One possibility is the normalization of the things that get broadcast. The famous example is the supposedly horrible moment when you get to your first-round job interview and are presented with images from the parties you’ve attended over the last 10 years. You hear this example all the time. I can picture a situation in 10-15 years where are no more job applicants [laughs] [...] And I can also imagine that tomorrow’s technology-savvy applicants have already accessed the party photos of the HR head interviewing them for the job.“

“I have always been a proponent of self-regulation and believe that government meddles too much in too many areas. It should concentrate on providing basic needs and services, maintaining infrastructure and those kinds of things, but not try to impose its ideal or ideals on grown men and women. The ban on smoking is just one example. These are almost absurd examples of a paternalistic state.”

Making technological innovations more user-friendly and secure

Media professionals are themselves great supporters of Internet technology. In their view, they not only stay close to the issues, but also keep their eye on “big picture” developments. To an extent, they see themselves as “lawyers” for the user community. They take the user seriously and add genuine value to the discourse by considering innovations from a broader perspective – not just in terms of the technologies themselves. In their view, there is room for improvement in the areas of user friendliness and operating security and reliability. And as the Internet continues to expand and pervade more and more areas of society, the less technologically-savvy users will have to be given the chance to “get on board”.

> *“That is the big challenge – to avoid leaving these people behind. The only way to achieve this is by communicating the advantages of the Internet and the new solutions it offers. But then the advantages need to be real. […] And they need to be idiot-proof and extremely secure. […] Business is often very weak on this point. […] The reason why user prompts and user navigation are so inadequate, is because the Internet and all the services in and around the Internet are almost always created by technical people who live and breathe this stuff.”*

Media professionals suggest that providers should meet the users halfway: they should make their products and services simple, accessible and transparent with regard to security settings.

Example: Uniform payment systems

> *“It would be nice if the operators/vendors could agree on, say, two or three standards for payment transactions as a way to simplify the structure and layout of certain web pages. To suggest a common Internet currency might be going a bit too far, but more uniform payment systems would make the whole thing more manageable. ”*

Example: Social media

> *“When I think about all the configuration options on Facebook or the Internet browser… The main setting is always the default configuration, since only a few users will bother to change them. And that is a job for policymakers. They should stipulate what the default settings should look like. If the user then decides to change the settings and go in a different direction, then he makes the conscious decision to do so. That is why the default settings should be more restrictive. But usually they are not. Usually it’s exactly the opposite.”*

According to media professionals, the Internet is no longer a luxury for a selected community of users, but a mass medium that should be considered part of the basic infrastructure and accessible to everyone. But it remains difficult for most users to keep up with the tremendous complexity of systems and the speed with which new solutions and applications are being introduced on to the market.

> *“I would say the user is basically in over his head. When you look at these social networks, for example, you’ve got 15 pages stipulating the terms of use and data use policies and the user is expected to read and understand this stuff. And it’s written in a language that is not only hard to understand, but also subject to legal interpretation.”*

Still, media professionals remain focused on the future. The further digitalization of our world is, their view, inevitable and will continue to penetrate more and more of our daily lives and routines. They develop very detailed scenarios of the future of the digital society.

> *“It’s going to change the way we do business and it's going to have a huge impact on our daily routines. The flow of customers through a city's commercial zone will be channeled differently, because various shops or lunch restaurants will be competing for whoever happens to be passing through. You’ll get a message from the Pizza Hut around the corner saying ‘Hey, here you can get two for the price of one. Come to us, don’t go to McDonalds!’”*

3.
Internet players‘ perspectives

3.5.
Academia:
On structural change, design imperatives and new social divisions

3.5. Academia:
On structural change, design imperatives and new social divisions

The Internet as the trigger for a cultural transformation

The academic community's very broad and multi-faceted view on the subject, extends far beyond the limits of their own fields or disciplines. The increasing digitalization of the everyday world is viewed as a great opportunity, but also as the trigger of a profound cultural transformation with far-reaching technological, economic, political and social implications (examples cited include: the "Internet of Things", diversified Internet-based business models, a new understanding of the individual person, communication and social interaction).

Academics are considering carefully the Internet's potential to bring about change, its opportunities and its risks. But the results of the discussion are quite clear: the opportunities ultimately outweigh the risks. They consider the risks to be manageable, as long as they actually get addressed.

> *"We basically need to understand the Internet as gift – a gift to mark the turn of the millennium. […] We can either accept this gift and nurture it, or we can be reckless and careless, and ruin it. The law plays an important role in this, but by no means the most important role. It will always be a combination of legal, economic, technological and sociological factors."*

The academic community is in a position to consider the Internet from a wide range of perspectives and levels of perception. They themselves are part of their own research subject; they see the Internet from the inside as well as from "outside".

Academics themselves tend to be enthusiastic Internet users and are especially active on social networks. They are fascinated by the enormous potential unleashed by the merging of previously separate spheres such as research and application. They might immerse themselves in the world of the "Internet community", but maintain a certain amount of reflective distance at the same time. They might have their own Facebook page, and use it actively, but explain this as part of their research – as a self-experiment.

> *"I myself am very active on Facebook, simply because I want to explore – and need to explore – how this network works. I conduct research on this, so I treat it as a kind of self-experiment. For example, how casual I am, in fact, about posting content? Or how complicated are the privacy settings?"*

Overall, the academic community sees the Internet in a very positive light – as a major asset that has enriched daily life and become indispensible to it. It is indispensible, on the one hand, at the everyday level by providing the supporting infrastructure for teaching and research (the Internet as a tool for acquiring information, facilitating communication and collaborating with other members of the academic/research community, as an e-learning platform). On the other hand, the Internet itself is the subject of considerable research. Much to the dismay of the academic community, however, this research remains very much underappreciated and tends to be oversimplified by the players in other sectors (especially in government/policy, but also in sectors such as education and media).

“What you need, first and foremost, is top people in government – in the federal government in the state governments – who can place this issue where it belongs, which is at the very top of the agenda.”

For members of the academic community, the Internet will inevitably bring fundamental change to conventional concepts of reality, legal order, social structure and democracy. While their assessment is sober and straightforward, they do emphasize the need for proactive design as a way to avoid new social divisions.

“This kind of ‘digital divide’ between the different ways people use the Internet will, I believe, continue to deepen. There already exists a kind of Internet elite who know how to use the Internet to advance their careers or climb the social ladder. And there are those who don’t manage to do this at all, who use the Internet as a kind of virtual space for their everyday tasks, but in no way use it to improve their social status. [...] Exclusion mechanisms are of course not just virtual; they remain social, so it remains to be seen how much this ‘peer pressure’ of the virtual society is superimposed on social structures/social behavior in real life.”

Describe, compare and gain an overview

The academic community, like the media, tends to relativize the issue. It is less interested in formulating its own point of view and more interested in considering the field as a whole and identifying future challenges of the digital society. Required is an interdisciplinary approach that is able to shed light on as many aspects of the issue as possible, so that they can then be introduced into the social discourse.

The academic community also sees it as their task to unravel and reduce the complexity of the issues being debated. They want to break the issues down so that they become easier to understand and more accessible to less-informed decision makers and to a broader cross-section of the population.

Some members of the academic community are linked to decision-makers from other social sectors such as politics, business, media and law. They use these professional networks to collaborate on solutions and call attention to new aspects and new demands. These academics like to see themselves as admonishers who are not afraid to “stick their finger in the wound” by focusing on the more challenging, troublesome and previously neglected issues related to the Internet. They also see themselves in a networking role – establishing connections between different social sectors and academic disciplines. It is their broad and well-grounded perspective on this issue that makes it possible for them to provide an accurate, reliable overall look at the situation.

“The concept of surveillance, for example, needs to be considered from different perspectives. We’re familiar with government control and monitoring, but Google also monitors my user behavior and gathers data on it. If I do a search for ‘homosexuality’, for example, Google knows that. Google includes that information in the data it compiles and this then becomes something that could be used against me. If I have a cell phone or smart phone, Facebook will know where I am at all times. So how do I monitor Internet companies, who themselves conduct monitoring, but in a much different way?”

The majority of academics see their role as consultants to decision-makers in government and business. They want to do more than just diagnose the situation and offer criticism; they also want to contribute their respective expertise to solving the urgent problems together with the decision-makers. They want to actively help shape the future of the Internet and demonstrate what needs to be done over the long term to promote a sustainable digital society into the future. They see a long road ahead. But it is a road that absolutely needs to be traveled because, according to their experience, today’s end-users know practically nothing about the issues.

“People will come up to me after I’ve given a talk and say ‘I had no idea that it works that way.’ And that’s just not right, that’s not good enough. It’s as if we all live in this country and have actually no idea how our political system is set up. Now I know that if people start asking about this stuff they will end up being pretty disillusioned, but stuff like ‘Bundestag’ and ‘chancellor’ – people have at least heard these terms before and can maybe say a word or two about them. This kind of rudimentary knowledge needs to be there too when it comes to Internet issues. It’s important – and it’s where we are trying to make a contribution.”

All sectors need to catch up regarding the Internet – except for business

Academics tend to think in terms of interdependencies, feedback loops, and the interconnectedness of all things. Their agenda includes not only the issues, social sectors and their mutual dependencies, but also the various players, i.e. decision-makers from the various sectors. They could easily generate and distribute a list of “to-do’s” for these decision-makers in each of the sectors.

In the area of government and public policy, academics point to a significant lack of experience and know-how in Internet issues and the challenges of the future digital society. While policymakers do recognize the need for action and demonstrate some commitment to the issue, they are rarely informed enough to make good decisions.

> *“Of course it’s crucial to first establish a basic understanding for the situation and interrelationships – otherwise you will have failed regulation. Unfortunately today, we will need to start at the very beginning; with the basics. That is the huge issue right now in the area of Internet policy-making: how to get even a basic understanding of ‘this Internet thing’. But this is just a prerequisite; alone it is not enough. One also has to consider – and this is a legal issue – how do I establish a legal doctrine for the Internet, a structure of norms, that is both effective and appropriate in today's world? It’s the issue of legal governance. Where can I use legal means to maintain the course and where does this approach no longer work?”*

Academics regard private sector companies as a decisively important group – and one which has amassed a tremendous amount of power and leverage in recent years. IT companies take advantage of the ignorance and negligence of politicians and end-users, which allows them to operate on the Internet with considerable freedom and independence.

> *“It's clear that companies like Facebook and Google have become unbelievably powerful, because they host a large part of the information that we either put on to the Internet or download from the Internet. And if you think about it, communication happens more and more through Facebook. “*

According to academics, users have the obligation to inform and educate themselves, and need to develop a healthy skepticism towards new media technologies and the Internet. Instead, they say, people’s dealings on the Internet tend to be characterized by laziness and negligence. Thus, the user himself poses the biggest risk to his safety and security on the Internet.

> *“Whenever the government does anything, people’s first reaction is to assume the state is after them – looking to limit their freedom. But people seem to have this basic trust in certain companies – for no reason whatsoever. […] They trust a company like Google with endless amounts of data, for no good reason, except that Google is so nice and so stylish. At the same time, they scream the whole time at the top of their lungs ‘help, help, we want our privacy protected!’”*

In the view of the academic community, the media sector is not yet doing enough to educate and sensitize users on the opportunities and risks associated with Internet usage. Academics suggest that this could be accomplished in the form of reporting and documentation, but also through the development of targeted education/training on the subject of the Internet.

> *“For adults this could be something like the 7. Sinn (earlier television program in Germany devoted to road traffic safety). Do you remember that? […] Back then, when 7. Sinn came on, people would sit down and watch it. But today television is no longer the medium of choice for everything […] You would need to find group-specific formats, [...] short video clips that people could view when they have a free minute, like on You Tube or something downloadable – that would be good.”*

According to academics, lawmakers are currently still in a process of orienting themselves with regards to the Internet and, since it remains a relatively new area, many issues and positions have yet to be conclusively defined:

> *“That’s the primary focus: IT security, threats, defense systems, Internet crime, combating crime. But there is also social media and the democratic processes that happen through these channels. The changes to society, to politics and policymaking; all that Web 2.0 brings with it. And then there are the technological innovations, such as cloud computing, and the question of how to create a legal framework around that, or how to create an effective legal framework around any technology or technical process.”*

Academics find themselves in a dilemma with regard to their sphere of influence. On the one hand, their research can shed light on certain phenomena and introduce critical aspects of the debate into the social discourse; they see themselves in this role as consultants, especially for decision-makers in business and politics. On the other hand, they feel the results of their research often do not get enough recognition and, in turn, fail to get implemented by the right people in the right places.

> *“In order to perform its intended function, research needs to be recognized. One problem in my view is that Germany is relatively anti-science, anti-research; people are not ready and not willing to really look at the research results and deal with them.”*

Reinforcing the significance of research and defining concrete needs for action

In nearly all relevant social sectors, academics see significant deficiencies in Internet experience and know-how. Because of its position as intermediary between the different sectors, and view of itself as the critical observer of the digital modernization process, the academic community considers it one of its most pressing challenges to help overcome these deficiencies, to define clear action measures and make the corresponding demands on the responsible decision-makers.

On the policy-making front, academics stress the need for lawmakers to formulate and establish fundamental minimum security standards for the Internet. Selected areas of the Internet should be subject to government standards; these are areas where there is already broad social consensus on the need for regulation. Important areas include youth protection (with particular attention to cyber mobbing), data protection (securing rights to personal data, transparency requirements for Internet providers). If it can succeed in establishing some norms in these areas, Germany could serve as a model for other countries.

> *"Regulation should focus on current challenges as they exist - on the national level, too. You constantly hear about the Internet as a global medium that can't possibly be controlled or regulated […] also in the context of issues like security measures for protecting young Facebook users. […] There is a whole series of problems. As I said, cyber mobbing is a problem that often turns up in the classroom. That is certainly something that can be regulated at the national level."*
>
> *"I still think we need to set regulations for national-level providers and things that we can indeed regulate here in Germany. We have our national data privacy act; that works on the national level. Maybe this can be circumvented by international providers, who have their servers running in some other country and are no longer subject to our laws – but that actually isn't so easy. A Facebook, for example, that operates here is also subject to our data privacy laws. So I really believe that we shouldn't let ourselves be intimidated and buy into the idea that everything is so big and powerful, that we don't have a chance and shouldn't bother trying to do anything – and just sit here on the sidelines. If it's important to us then we should do it, we should establish the regulations. And if it works well, it can be exported to other countries – like a model of regulatory success."*

At the same time, academics always see the other side of the coin. Calls for greater regulation can also be seen as movement in the direction of government censorship and abuse of power. Regulatory intervention on the Internet needs to be considered carefully. Are the regulations truly necessary? Are they commensurate to the situation? (Internet lockdowns are cited as an exaggerated means of regulation).

> *"There is a fine line between regulation and censorship. Especially on issues where people are calling for government intervention, there is still that close association between government and power constellations. And that is of course the problem: if we demand regulation, how do we ensure that this doesn't turn into an abuse of power."*

Academics regard principles such as self-regulation and fairness as potentially effective regulating mechanisms and possible alternatives to government intervention (and especially relevant for the players in the business sector).

> *"In television there is this system of volunteer self-regulation where the broadcasting companies monitor and regulate their content themselves. In my view, that could be a model for online companies – that they themselves develop categories for their products on the basis of categories such as transparency or data security. I think that would be a model, a solution."*

Along with government and business, academics also believe that the education sector needs to fulfill its responsibility of informing, educating and raising awareness among Internet users. Basic media literacy is an important prerequisite for being able to use the Internet confidently, effectively, responsibly and in a way that minimizes personal risk. Media literacy should therefore be integrated into the educational mandate. The proper use of new media can be taught using hands-on, practical approaches based on modern teaching methods.

> *"It's nothing less than a scandal – and it applies to Bavaria just as to all of the other states in Germany. It's a scandal how little the ministers of education seem to know about the Internet and digitalization – and the opportunity that this represents for education and our schools. It's just absurd how we continue to use these outdated teaching methods and outdated teaching materials here in Germany – even though the best materials and the best methods for motivating young people are available."*
>
> *"We could be doing a lot more in the schools. In Germany we still do not teach media literacy in the schools. It's not a regular part of the curricula. […] The government could certainly set requirements for the curricula, for example, so that things like Internet become a regular part of the curriculum."*

Besides addressing today's concrete issues, and developing appropriate courses of action, the academic community is looking into the future to understand how the Internet is changing specific social parameters, and what this means for society as a whole.

In the area of politics and democratic processes, academics see the need to establish a reasonable balance between the opportunities that the Internet offers with regard to open data/open government (citizen participation and co-determination) on the one hand, and the prospect of an absolutely, unconditionally open political decision-making process on the other hand. While citizen participation is, in their view, a democratic value worth defending and promoting, it is also important that certain negotiations and proceedings take place outside the public eye and that the representatives elected by the people have enough leeway to govern effectively and are allowed to make decisions in "secret" when necessary, so as not to jeopardize the government's capacity to act.

> *"Transparency versus secrecy. That is a very important issue, because the trend today is clearly towards more openness – opening everything up and declassifying everything. And I think that is problematic. Because our culture is not based on this kind of completely open society. We are not accustomed to complete openness. […] We're not at all ready for that. Secrecy does have its advantages. […] Policy-making is also about finding compromises and coming up with smart and reasonable policy solutions. If you completely open everything up from the beginning à la the Pirate Party, you won't, any under normal circumstances, be able to achieve any results whatsoever. [...] Or in the case of ACTA, I've got nothing against negotiations occasionally taking place behind closed doors if they are difficult or sensitive – if additional pressure needs to be applied to a certain country to get them to move. You can't do that kind of thing on the open stage. But the terms and conditions need to be communicated as such – and of course the people need to be given the opportunity to participate in the decision-making process. I am not for unconditional openness."*

Academics regard the Internet as still a relatively new sphere of social activity, for which a system of norms, values and legal rights has not yet been definitively established. Instead, society is in the midst of a process of constant coordination, decision-making and adjustment – a process which must weigh the many factors and carefully consider the future configuration of our Internet environment. Future scenarios include very different online environments – from "comfort zones" on the Internet, where users can move safely and easily through the space, to "jungle" conditions, where norms and order do not exist. Ultimately, members of society must decide for themselves what they consider to be acceptable and desirable.

> *"Users should have the option of choosing a kind of basic service, where providers or vendors are obliged to guarantee a certain standard of security and be able to certify this in some way. So when I'm a user and I need to take care of a few basic needs on the Internet, I know, OK, those are the institutions I can work with. If I go with them, then I'm on the safe side. And everything else over there – that's the jungle. If I want to go there that's OK, but then it's my problem, my responsibility."*

Academics see the Internet as a platform that offers people enormous new opportunity for individual actualization, for freedom of expression, for unleashing creativity and innovative power. But to truly take advantage of this opportunity, academics stress the importance of fairness as a guiding principle and call for a "culture of trust".

> *"And that means we will have to establish new systems and 'infrastructures' of trust, business models, for example, where responsible companies can actually take the lead on the market and be rewarded for being truly honest and reliable, while other companies fall behind because they have not earned the trust of users?"*

4.
“Babylonian Confusion of Tongues”: Security between law and freedom – but without consensus

FREEDOM
LAW
PROBLEM-ORIENTED
OPPORTUNITIES
RISKS
DISCUSSION
POSITIONING
INTERESTS
OPINION
DILEMMA
PUBLIC SPHERE
FRAMEWORK
CONFLICTS
COMMUNICATION
LANGUAGE
RESPONSIBILITY
DISSENT
SECURITY
TRUST

4. "Babylonian Confusion of Tongues": Security between law and freedom – but without consensus

The surveyed opinion leaders have specific views of the Internet that are determined by their own goals, their potential for exerting influence and the current business climate, including the user requirements and concerns that go along with it. The sector-specific positioning depicted in the previous chapters revealed the broad range of ways in which the Internet has been integrated into technological, economic, social and cultural contexts of interpretation and management processes.

These opinion leaders are clear that the Internet has come to represent an integral and indispensible component of private and public life. The magnitude of dependence on this infrastructure in their view raises not just opportunities, but also challenges as well. Regardless of whether the players here emphasized the potential or the risks of the Internet, the issue of security remains a central linchpin in their consideration of the current situation, both in terms of its respective meaning as well as in terms of perceived conflicts of interest and solution approaches.

Almost all opinion leaders emphasize that security is an absolute precondition for all citizens (including the most undiscerning users!) to be able to place trust in the Internet as a medium and to use it safely and freely.

Security and trust are thus closely linked both from an associative and rhetorical standpoint. For many, security is a precondition for trust, although at the same time it is also possible to have trust without real security. To depict these interrelationships systematically, the focus will now turn initially to the grasp and the respective approaches towards security. The reference to the issue of trust will be established in the chapters that follow.

Comprehensive Internet security does not exist

In the view of the opinion leaders, there can be no 100 percent security on the Internet, no more than there can be in the real world. The goal is thus not to eliminate all dangers, but rather to achieve the best possible containment, estimation and calculation of an often diffuse spectrum of potential threats. The opinion leaders soberly acknowledge that most security holes only gain attention when somebody discovers them.

> *"I'm of the firm opinion that there will never be 100 percent security. And naturally no 100 percent freedom for that matter. A total relinquishing of all freedoms won't gain us more security either."*
>
> *"Everybody thinks that security involves adopting a Fort Knox strategy. They think that if they build a huge secure fortress it'll be safe from attacks. The reality is that hackers get in everywhere and that entirely different strategies may be needed."*

"An admittedly somewhat dreadful example is the green traffic light that — quod erat demonstrandum — is anything but risk-free and which, tragically, teaches a few people the hard way each year that it is not risk-free. Nevertheless we all behave as if it were risk-free. It's not. We establish conventions or define things and derive from the actuarial statistics that in a majority of cases it will be risk-free. Because we design it that way, knowing that there are absolutely no guarantees. I think that if you apply this perception to the digital world, then it shouldn't mean that we can always expect security there — this isn't a call for a nonchalant interaction with the risks, but rather a more realistic assessment of what can be achieved if you talk about freedom from risk."

Security is thus defined as a generally accepted risk of danger — frequently described as the "limiting risk." From the perspective of the opinion leaders, in a best-case scenario security is established where systems are not being damaged by already known threats. Fulfillment of this condition can be referred to as "sufficient security."

Security on the Internet as a challenge for business and politics

As shown in the first chapter, the opinion leaders see a large spectrum of risk on the Internet, and yet at the same time also presume that users are hardly aware of most security concerns. This is a dilemma insofar as they — particularly politicians and businesses — expect and even require security.

The real risks are thus, in the view of the opinion leaders, larger than people believe and are less effectively manageable than people seem to think. The problem is: this is difficult to convey without potentially disrupting the audience's trust in one's own offered services.

Communication about security must therefore put it into perspective to ensure that it is not misunderstood by the user as freedom from risks or damages.

"But you have to choose the word security carefully and be very meticulous in not offering any room for subsequent attacks that claim you lied or that it's not all true or blah blah blah. […] And you have to be very careful when using superlatives and that kind of thing. I think that a careful selection of words is crucially important especially in the area of trust and security, so that one doesn't just simply call out your opponent […] or let's say the guardians of the real term security and antagonize them."

"The difficult thing is that the effort to communicate security measures in a purely positive manner based on best cases has never yet worked. That's been our experience as well. Nor can we advocate, let's say, simply washing and disinfecting your hands to prevent the spread of illnesses in some way without also pointing out that we've just suffered cases of it and just had EHEC and so on. And unfortunately security on the Internet is much the same way."

The public discussion about security and trust — in relation to their own possibilities and expectations of the users — is decidedly rejected (particularly by various players, especially those in business) and for ideological reasons viewed as exaggerated.

> *"I think that the topic of trust and security on the Internet is terribly overdone. And in particular through a tandem of media and politics, with a dash of that culturally ingrained German need for security. So, the topic of security and trust and threats and risks is part of our cultural identity. […] I believe that it's a topic that is at least very strongly construed by the aforementioned tandem."*

Little common sense in the discourse about security on the Internet?

The underlying attitudes and approaches to the topic of security among the players can be differentiated based on their self-image and sphere of activity. As already sketched out in Chapter 3…

- … **the opinion makers in government** are primarily interested in Internet safety as a part of the critical infrastructure. They link the security question closely to the question of a (fundamental) regulation of the Net, but warn against a limited ability of business to compete due to overly strong regulation.

- … **the opinion leaders in business** thematize security in equal measure as a business model and as a deterrent to innovation and cost factor. The opinion leaders from business want to handle security issues through voluntary commitments rather than through regulation.

- … **the opinion leaders in civil society** warn most clearly that security on the Internet comes at the price of liberty.

- … **the opinion leaders in the area of media and academics** are acting as a flanking pair of impulse generators whose observations on this issue are given little heed.

This means that the term is being laden with various associations and corresponding valuations, which in turn produces various formulations of intended behavior.

In politics, Internet security is a topic that demands action, yet one whose pace is not set by the politicians themselves and where they know that whatever demarcation they make of the scope of security requirements, those thresholds will inherently face opposition from business and digital natives. The security question is a delicate one for politicians, since it frequently must be defined as defensive ("as something forced") and where contrary security needs must be balanced out. Security inherently involves dilemmas, since security can have a price in freedom and purportedly can slow down economic development. The players in this sector are — depending on their nature of their protective duties — "risk-avoiders", with skepticism about the ability to cope being characteristic of the security discourse in the public sector, not least because they admit to being dependent on external experts.

Discourse on security among opinion leaders in politics and the public sector

Key terms

Freedom vs. Security

Anonymity

Data security and data protection

Own knowledge gaps

Crime

Costs

Mandate to protect

Security from attacks

Control

Lack of resources for cyber defense

Protection of critical infrastructure

Criminal prosecution

Legislation

Risk

Regulation

Liability

Surveillance

Awareness raising

E-Governance

Electronic passport

Basic attitude

- Defensive (reaction instead of action)
- Problem-focused
- Overextended
- Under pressure
- Lagging behind technological developments leads to skepticism vis-à-vis coping capacities
- Uneasiness due to dependence on external experts
- National and EU perspective

The business side sees itself more as "risk-takers", drivers and impulse generators for innovations. Despite the perception that 100 percent security is an illusion, the security discourse among decision makers on the industry side tends to feature a greater optimism/realism about the ability to manage the issue. There is a stronger focus on the opportunities brought by a desire for security than is observed among politicians and administrators. There is a feeling that regulation limited to the national level is pointless and that any efforts in this direction deserve sharp criticism.

Discourse on security among opinion leaders in business

Key terms

Protection of company data

Customer data

Customer loyalty through trust in security

Consumer

Costs

Security as innovation barrier

Voluntary commitment in lieu of regulation

Individual security needs

Global challenge

Usability

Basic attitude

- Optimistic, due to confidence in one‘s own expertise in security matters
- Strong desire to create and shape
- International perspective
- Critical of government cyber policies
- Customer-focused

Representatives of civil society primarily get involved in the debate on Internet security when it affects aspects such as education, equal participation and democratic structures. They view security both as a threat and as a precondition for the freedom of the user, and thus desire balance, not ill-considered procedures in areas like regulatory questions — and above all else, an initial discourse between all players on equal footing.

Discourse on security among opinion leaders in civil society

Key terms

Freedom

Transparency

Legal position

Discussion

Participation

Regulatory policy

Sovereignty

Basic attitude

- Informative, demanding
- Emotional (“our Internet“)
- Critical of politics and business
- International perspective

As such it is difficult to talk about Internet security and make decisions on the basis of a shared basic understanding.

Representatives of civil society and academia in particular have committed to examining the complexity of the term in more details. They are most likely to think in terms of a security architecture in which various levels are kept separate and attempt to understand their respective relationships.

"It's really a quite difficult field and for that reason I also say at the start I don't hold much of talking about the security of the Internet, but rather you really need to break it down into the individual services. E-mail is really different from this kind of online shopping — and even there you have to differentiate once again between the purchase of larger goods, as they have other security concerns."

"Security is generally speaking a gradual process. All security experts know, I'll start just as an example with the physical aspects, so, how can I enter into a building at all, what is the potential for accessing IT systems, how are these correspondingly protected, how is the network then protected, which operating system is being used, meaning the host itself, how are the applications protected and how is the data in and of itself protected. We've established corresponding protective measures on each of these levels."

Security as a "hot potato"

That security is understood in different ways and to some extent has highly fluid boundaries isn't just a factor of sector-specific fields of responsibility and personal competencies, but also with intentional caution. Why is this the case?

The conversations showed that security is a sensitive topic. How someone understands security and the concepts and solution approaches that are adopted based on that understanding are clearly taken by other opinion leaders — at least in terms of Internet politics — as indicators of an underlying attitude toward the Internet and society.

Those who accord the topic of security less importance are seen as negligent, irresponsible and self-centered by others. Those who strive for "a lot of security" are accused by others of being controlling, domineering and regulation-obsessed.

In many cases fundamental ideological discourses are being broached.

"I'm no communist, but I do think it's a problem that everything always has to be dedicated to making money."

"We live in an anti-business climate where one has to justify earning money."

It only takes one more logical step to come to the associated question of who then can and should assume responsibility for the presumed challenges on the Internet.

Passing the buck on responsibility

Responsibility isn't a term used actively by the opinion leaders. There is notably a problem-oriented treatment being promoted here, i.e. hardly any positive vision of responsibility for Internet security can be observed, and responsibility for security on the Net isn’t a virtue to be publicly touted. Responsibility instead seems to be more a matter of passing the buck, because it's clearly primarily linked with dealing with problems, and in particularly with the elimination of damages and bearing of costs.

Each party's own areas of responsibility are thus sketched as narrowly as possible and concentrated on fields that promise a burnishing of reputation (be it in relationship to voter opinions or business success). That said, there are also some first players (primarily in industry) who are starting to integrate the topic of responsibility into their business strategy.

> *"Media literacy is really the job of the state, but if they're not doing it, then we'll develop materials and distribute them in schools."*

How responsibility is really being distributed and the solutions proposed by decision makers are shown in the following chapters.

5.
OSI Layer 8: The user is responsible and bears all risks

CONSEQUENCES

MEDIA LITERACY

AWARENESS RAISING

CONSUMER

CITIZEN

HELP

DELEGATION

LACK OF TRUST

PERSONAL RESPONSIBILITY

FREEDOM

CONTROL

RESPONSIBILITY

LEGAL FRAMEWORK

NEED FOR PROTECTION

OPERATOR

USER

ERROR-40

CIVIC DUTY

5. OSI Layer 8:
The user is responsible and bears all risks

While decision-makers are reluctant to assume responsibility – and even feel they have been absolved of responsibility in many areas – the question remains how to involve stakeholders and establish a system that actually allocates responsibility for Internet security. Despite the general tendency to want to delegate this responsibility, there is a basic consensus on one point: ultimately it is the user himself who is responsible.

> *"I am very much in favor of personal responsibility, because the moment I ask a third party to take responsibility for me – if I say to the state, for example, 'please, please, protect me from the Internet' – then I give the state too much control over my private computer, I give up too much freedom in exchange for what may or may not be considered improved security. So I lose in the end."*

Ultimately it is the user's behavior and decision-making that determines, more than anything else, whether or not he is safe on the Internet. The user himself is thus the biggest risk to his own security. Not surprisingly, decision-makers consider users to be quite naïve in this regard.

> *"The most common is ERROR-40. You don't know that one? […] Error 40 means the error is sitting 40 cm from the monitor."*
>
> *"As long as we're on the topic of data privacy, I have to say that many users really are extremely naïve when it comes to the commercial mechanism driving the whole process. A lot of people just don't bother to ask the question, 'why am I not paying any money here?'"*
>
> *"The negligence is amazing, really. Yes, paying for virus protection can be annoying, and it's a pain to deal with, and so on. People are gullible, etc., etc., and they're curious and want to try things out. As a user there's this tendency to always make these kinds of hapless moves. In IT there's this layer model, the seven-layer ISO/OSI model, it's actually very technical - it goes from the hardware through to whatever kind of application software being used, which is the 7th layer. And then everyone always says the biggest problem is the 8th layer – that's the user."*

Opinion leaders agree that the Internet user needs to carry a large share of the responsibility for himself. It is less clear, however, where this domain of personal responsibility begins and ends. On the one hand, the user should assume responsibility for that which he alone can control. But at the same time, the average user is said to know basically nothing; he knows neither what he can control nor how to control it.

Recommendation to users: Invest in security and act smart!

For starters, the user should be considered responsible for everything that can be considered "reasonable". The comparison is most often made to driving a car and observing basic traffic laws. In this sphere too, one is expected to possess a minimum amount of basic knowledge and obey certain rules, but can also expect from the manufacturer a minimum level of basic security (a car free from technical defects, in good working order, etc.)

> *"Just like when people cross the street. They need to look left and then right to make sure they don't get run over. It's the same here. It's their job to inform themselves before they start doing business on the Internet."*
>
> *"If you drive drunk into a lamppost, then you are responsible. You can't then say 'Hey, sorry, I'm just the end user of this Opel here."*

Thus, there are certain basic civic responsibilities that apply to the Internet as well. An individual's basic sense of right and wrong is considered a given – or at least some sort of sense.

> *"Risks basically originate in a lack of awareness. As soon as the awareness is there, then people behave accordingly. The risk is actually always related to usage. If you open an email, for example, and there's an attachment and you've told your computer to always open and execute attachments immediately because it's just more convenient that way, well then you'll have the virus on your hard drive right away. You simply need to be aware – you need to know how to use the Internet. And if you've got that, then there actually is no security problem on the Internet."*

Often the assignment of responsibility is done in terms of platitudes. Especially things like social network privacy settings and an individual's own online profile are considered matters that a user should be able to manage by applying basic common sense ("you've got to know which photos of yourself to post on Facebook"). This also applies to the use of security software and the treatment of sensitive personal data (such as TAN lists). Decision-makers often draw the comparison to the requirements for operating a motor vehicle: you don't need to know how a car actually works, but you do have to know to fill it up with gas and to head to the service station when an unfamiliar red warning light goes on. They also see it as the user's responsibility to proactively search for information and answers if the situation seems unfamiliar or insecure.

> *"Ultimately everyone is responsible themselves for what they do. If I decide to use social networks, then I am the one responsible. Sure I can always try to assign the blame and say that their rules lack transparency and so on, but at the end of the day I'm the one responsible for going to the site and finding the terms and conditions, scrutinizing them, and asking questions. And if I feel I can't be bothered with reading all that, then it's my job to get the information somewhere else."*

"The limits of the user's responsibility are actually pretty clear. A responsible user needs to make sure that his TANs are secure and that he doesn't just enter them anywhere. He needs to make sure his anti-virus protection is working, which of course does not rule out the possibility of getting infected somehow, [thinks for several seconds] and he needs to be careful and make sure that he a) doesn't stumble onto something on the Internet that he does not want to see and b) that nothing happens to him on the Internet that he doesn't want to happen. And that's about all."

In the view of opinion leaders, security is, first and foremost, something that users are obligated to provide themselves. Personal responsibility is not directly coupled with external responsibility, for example, in the form of a mutual agreement that stipulates which party is actually liable for which aspects of security and where the border lies between personal and external responsibility.

Trust begins where personal responsibility ends

Opinion-leaders nevertheless acknowledge that the user cannot be expected to know everything and that the user's control over the situation is limited. Especially representatives of civil society – and policy-makers to an extent as well – tend to want to protect the user. In their view, it is not possible for a user to gage the actual consequences of a provider using his data, or the possible influence of third parties. This is partly due to the fact that personal data first needs to be combined and contextualized (i.e. via profiling) before its actual value can be assessed. But it seems that opinion-leaders have not yet agreed on where exactly the border between individual and external responsibility lies.

"Yes, personal responsibility ... the question is, of course, where do I draw the line. And in my view the line is not at all clear at the moment. Surely it has been defined in some court ruling – but in practice that doesn't help much."

One way out of the responsibility dilemma is trust as an organizing principle that is both overriding yet relativizing. Nearly all decision-makers regard trust as a possible key to diffusing the tension between security and responsibility. Trust also provides a guideline for understanding user-provider interactions for their own purposes and activities.

"Actually I think everyone would say 'Of course the individual carries the responsibility.' But I believe that is demanding too much of the individual. Sure, as a proclamation I think everyone would sign it. I, too, am responsible for my own security on the Internet, but I simply cannot know everything. To an extent, I need to be able to trust the other guy."

"The whole Internet can only function if there's a basic level of trust, or a basic level of naiveté – take your pick. […] But there's no way that I can control it."

But where does a healthy level of trust end, and where does naiveté begin? On the one hand, a minimum level of experience, knowledge and Internet literacy is considered a prerequisite (see above) before a user should be allowed on to the web. On the other hand, the user should rely on his instincts and do whatever he likes until he has a bad experience and learns from it.

> *“You should trust the other guy so long as the other guy doesn’t take advantage of you.”*
>
> *“In early childhood people’s default setting is still to basically trust other people. You’ve had little bad experience, so, in the beginning, the question is: Why should I not trust him? And then that changes. In kindergarten, as soon as that other kid hits me in the face with the shovel two or three times, I'll start to think about whether I really trust him and whether I get close to him when he has a shovel in his hand. So everyone needs to find their own way through – and it’s the same on the Internet.”*

Trust is considered a variable – and the user should apply neither too much nor too little to any given situation. This is the only way to ensure competent and secure use of the Internet.

> *“It’s both. You [the user] have both too much and too little trust. Sometimes there is too little trust and the result is too little e-commerce taking place. But then in other situations the users are too trusting and get taken advantage of by dishonest vendors.”*

The above statement demonstrates how much the decision-makers rely on user trust. The user has to trust the vendor, otherwise one’s own business model, and even the Internet itself, will cease to function. So trust is both the solution and the problem.

Trust as the key currency on the Internet

Opinion leaders regard trust as the Internet’s key currency. It paves the way for transactions and acts as a form of capital paid in advance to the vendor, which the vendor accumulates, and which the vendor can lose again if users decide that he is out of line and no longer worthy of their trust. No business can survive on the market without earning and retaining the trust of customers. But government, too, is dependent on the people’s trust. Without trust, it loses its ability to act – for example in the area of online government services or management of citizens’ personal data.

Lack of trust triggers activity, such as efforts to improve security standards, user boycotts of certain products and services, or political activity that puts certain Internet issues on the legislative agenda (e.g. possible bans on websites with child pornography or involvement in the debate over copyright law).

Even if trust remains a matter of subjective assessment and intuition, most opinion leaders nevertheless propose rational measures to build trust and confidence. These include (a) technical security standards, (b) transparency of commercial transactions and (c) promoting education for improved media literacy.

a) **Decision-makers often consider improved security to be the most important trust-building measure.** This includes the development of security concepts to contain potential infrastructural risk (such as compromised IT systems, data loss, hacker attacks).

> *"Of course we need to make sure, just as we do with banks and other such channels, that the connections are secure and that nobody else can gain access to these PINs and customer data. For us it would be disastrous if our customer data, which might even include things like account numbers, ever turned up somewhere. That would totally destroy people's trust in us and basically threaten our existence as a company. So this is a fundamental issue for us."*
>
> *"Trust is also extremely important when it comes to the behind-the-scenes processes, because sensitive customer data also needs to be saved and processed. And every customer – whether it's one of Google's business customers or an end user – every customer expects that this data is being properly secured and not being shared or distributed inappropriately."*

b) **Transparency with regard to data** and data-handling is considered another important trust-building measure. Decision-makers maintain that users gain trust in an online transaction if a vendor takes the time to explain certain functionalities and even outline possible breakdown scenarios (i.e., does not guarantee 100 percent security).

> *"Taking the time to explain something always creates trust. That's very important in my view. Vendors should always make the effort of explaining things, for example, 'We are managing your data in such and such a way, and we have taken the following technical precautionary measures to make sure nothing happens. And if something does happen, then the following will be done about it' etc."*
>
> *"Trust in institutions, regulations, compliance certifications and the like – these are basic requirements before Internet users can feel secure."*

According to opinion-leaders, an investment in trust-building measures is a clear win for the reputation of a company or organization over the long term.

> *"The whole concept and system of security on the Internet depends on having enough trust anchors. A big company with a well-known brand is considered trustworthy, for example, but also has a lot to lose, so it will go to great lengths to preserve and continue to earn that trust."*

Especially representatives of civil society and media professionals believe that vendors do not go far enough with these assurances of transparency. While they do not want to see a "transparency bubble", they do demand that specific user-vendor interactions be clarified and made explicit ("companies need to make clear to users how they earn their money"). Transparency with regard to vendor intentions and processes, a clearly defined commitment on their part, as well as binding enforcement mechanisms are necessary before the user can act independently and responsibly.

> *"I think that would be a very nice development, if we could somehow make sure that providers or vendors are simply required to provide information on the actual monetary value and whether one just wants to pay that price."*

c) Finally, **educating people about the risks on the Internet and promoting media literacy**, especially among children and youth, is also considered an important means for developing and establishing trust. Trust in one's own ability is the basis for trust placed in others, and the key to correctly gauging other trust indicators. While decision-makers are in agreement on this point, it remains unclear who should be responsible for instilling this trust. While policymakers consider it their responsibility to define parameters (such as school curricula), decision-makers from other sectors suggest that government is not doing enough on this front.

> *"But I think it is also a social/political responsibility to point out the risk potential – in the educational system, in kindergartens, elementary schools, secondary schools up through university. I don't think there is a single occupational field today that doesn't require basic knowledge and competence with regard to technology and security."*
>
> *"I think schools should take on some of the responsibility in the future. I don't mean to suggest that we should introduce a new school subject 'Internet', but it should be included somewhere in the curriculum. And I think there should be organized events designed to educate and raise awareness. Media also has a role to play in educating people, especially the publicly-funded media."*

Interestingly, decision-makers give little indication as to whether these trust-building measures are actually effective in the context of Internet usage. No one raises the question, whether their own concept of trust even coincides with that of the user.

Trust without security?
The alleged legal framework as fallback strategy

Do the efforts of companies and government officials to inform, clarify and improve transparency actually increase user trust and confidence? Do individual security measures really add up to create an overall feeling of confidence and willingness on the part of the user to trust a given vendor/provider? And how much does the user even want to (have to) know?

Based on everyday experience – and results of the DIVSI Milieu Study* – it seems that actual user behavior on the Internet cannot necessarily be explained based on an overall sense of personal security. People do not always behave rationally or sensibly. And by no means do they behave consistently. This is, on the one hand, a function of the basic attitude characteristic of an individual's milieu (such as the "Carefree Hedonists" or the "Responsibility-driven Individuals" as identified in the DIVSI Milieu Study). On the other hand, individuals will tend to rely on their intuition or instincts if a given situation becomes too complex and can no longer be analyzed or understood. This is often the case with users in the context of Internet security. It seems, therefore, that factors such as social feedback ("over 900 million users can't be wrong") are more relevant to explaining individual Internet behavior than statements from vendors/providers ("your data is secure with us").

> *"Trust is a very important factor on the Internet, because one doesn't really know most of the people with whom one interacts. This can be seen especially with the social networks. You may have 600 friends, but of course they aren't really all friends. Many of them you probably don't know at all. Maybe you connected somehow through someone else. So it's always a question of: 'if I share this bit of personal information, do I trust them not to take advantage of me?' So trust turns out to be a very important thing on the Internet, even if it's a kind of blind trust that we don't really bother to verify."*

For users, trust indicators seem to be largely intuitive and quantitative, as reflected in today's popular web parlance ("250 people like this product" or "customers who bought this item also bought these items"). If I buy a product or make use of a service, it is not necessarily a conscious decision on behalf of that product or service, but simple pragmatism: It is less about making a selection and much more about joining in and taking part.

> *"It's the herd instinct – really pretty mundane actually. The thinking is: 'if a lot of people are doing it and not having any problems, then it can't be too bad, it must be OK.'"*

Trust in one's own instincts or "feel" for the situation is more important for users – and more expedient – than a rational analysis of opportunity vs. risk. Interestingly, while decision-makers emphasize the importance of trust-building measures, they seem to contradict this when talking about their own personal Internet behavior. Their own behavior more likely reflects the intuitive, common sense approach, and less likely involves careful analysis and a weighing of the options.

* See the DIVSI Milieu Study, www.divsi.de/publikationen

> *"If one looks at one's own online behavior – and my behavior surely cannot be considered representative, because I'm definitely online more than most people and am active in very wide range of contexts – personal responsibility plays a very important role, if not the most important role. It's about personal responsibility, common sense, reliance on your intuition and feel for the situation. It's just the same, really, as everywhere else."*

Finally, the question remains whether a user's intuitive feeling of trust is truly independent of other factors. Is it based solely on the sense that nothing bad will happen, because so many other users seem to be OK? The DIVSI Milieu Study revealed that 74 percent of Germans believe government and business are ultimately responsible for ensuring security on the Internet. And they place a significant amount of trust in the notion that the government will intervene as needed or that a company will assume liability in the case of fraud.

In this way, users secretly assume that "justice" will prevail in the end and that government will ultimately fulfill its obligation to protect. And users are often astonished to learn that they are actually vulnerable.

> *"When I give a talk at a school and tell people about all the stuff that can be found about them on the Internet, they always say to me: 'But that should be illegal.'"*

The current debate surrounding the Facebook mass party phenomenon reveals that some users feel so secure on the web, that they trust the state to absorb the costs for police deployment and damage control – which it usually then does.

> *"Consumers do very little fact checking. […] That basically means blind trust. But the only way I can have this kind of blind trust is because I believe that there is some kind of legal framework that will protect me in the end."*

Thus, trust in online products and services is not necessarily born out of a propensity for risk-taking or willingness to remedy damages incurred; instead it is based on faith in an implicit fallback strategy and the assumption that, ultimately, someone else will bear the responsibility. It remains to be seen who that someone will be.

6. Conclusion – Four theses on the current state of the Internet debate

6. Summary – Four theses on the current state of the Internet debate

No one is offline anymore – life without the Internet is an illusion

All opinion-leaders maintain that the Internet is becoming increasingly important to more and more aspects of daily life, and that online and offline spheres permeate in such a way that it becomes increasingly difficult to distinguish between these two “states”.

It is therefore not surprising, that many opinion-leaders view the problem of social division in a digitalized world not as a challenge or threat, but as a situation that will ultimately resolve itself. This is not because demographic change or more educational/training initiatives will get more people “online”, but because people will soon no longer have to “go” online. Most daily transactions will be running online anyway. In addition, “being” online will no longer mean having to turn on a computer, dialing in and connecting to the Internet.

> *“Whoever thinks he truly lives 100 percent offline is just as crazy as the person who thinks he is 100 percent online.”*

Being online will be taken for granted and no longer regarded as an activity per se. Just as one does not consciously go on to the utility grid to use electricity or access the water system to tap water, the Internet will be considered basic feature of daily life that hums along in the background and only gets noticed when it malfunctions. People are, in fact, hardly aware of how “digitalized” they have already become.

> *“People think they have nothing to do with it, and then you take a minute to explain to them that their cell phone is actually a small computer that converts their words into a digital signal, which then gets digitally converted back to analog sound on the other end so that they can even hear anything. And then they're completely surprised and say ‘Huh, really? This thing is digital?’”*

Internet “use” itself is thus becoming increasingly invisible. It takes place less and less in the form of communication between person and machine, and increasingly as communication between networked devices. With modern automobiles, people might think they’re just starting the engine when they turn the key, but in reality they’re turning on a sophisticated on-board computer. People underestimate the complexity and scope of the “Internet of Things” in a similar way.

Ultimately, responsibility lies with the user – and no one wants to take it off his shoulders

The conversations with opinion-leaders from politics/government, business, civil society, media and the academic community have revealed an extremely multifaceted, controversial and passionate debate on the opportunities and risks associated with the Internet. The debate is not only about asserting one's own position but often an attempt to first find a common language and establish a productive dialogue.

Still, participants in the debate often believe that their own Internet knowledge and experience is superior to that of the other opinion-leaders from other sectors. This attitude, along with their different priorities and goals, tends to hamper the discourse. At same time, they feel an enormous amount of pressure to allocate responsibilities, so that the stalemate can be broken and progress can begin to be made. Overall responsibility for "the Internet" is considered neither structurally possible nor desirable. The solution is, therefore, to pass on the lion's share of the responsibility to the user. Opinion-leaders do acknowledge that there are limits to the amount of responsibility an individual should be expected to shoulder, but it remains unclear where exactly a user's personal responsibility begins and where it ends. A clearer set of boundary markers is part of what the current discourse is trying to achieve.

Policymakers consider it their task to create a legal framework that defines and distributes responsibility, but they feel hindered by the current "balance of power" (business vs. government) and by the limited (local) reach and impact of their decisions. In addition, they feel limited by the pace of "analog" democracy.

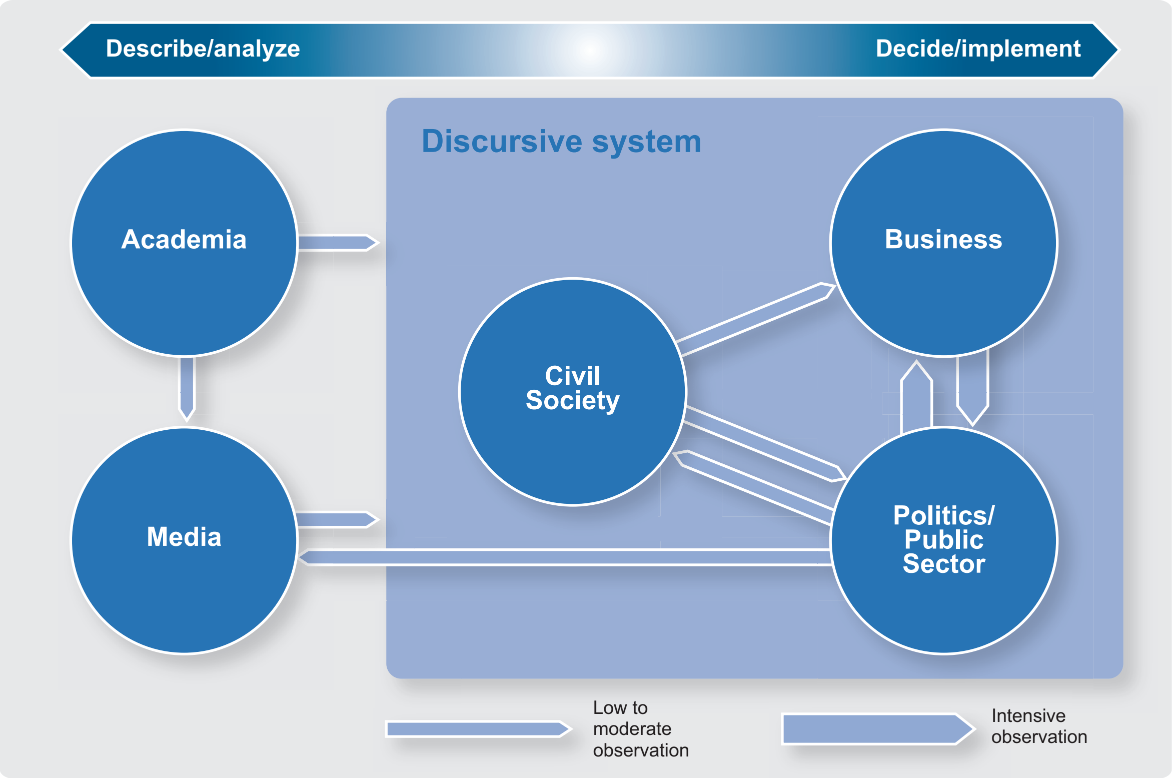
The Power is in the hands of the movers: The world's leading companies shape the rules of the game

Nearly all opinion-leaders from politics/government, media, civil society and academia see private-sector companies as the clear drivers of current developments on the Internet. These companies are not only players in the game offering their products and services, but also the ones defining and continuously changing the rules. This takes on added relevance as more and more areas of economic activity move online and as various providers evolve to become larger infrastructure providers, who then face little or no competition. It is striking to observe here that nearly all opinion-leaders notice a clear concentration of power in the hands of just a few global players who have "split up the Internet among themselves." They also make a clear distinction between business as a whole and "the big four".

"We're entering a totally new stage, where we find ourselves in an infrastructure that is white-male-western-American-Silicon-Valley-dominated, and nobody is talking about this. There is not a single European company that is really in the game. It's just the big four, and they're all sitting there in a single spot and shaping the Internet."

Opinion-leaders from the business community, on the other hand, stress the "power of the consumer" as the foundation and enabler of the private sector's ability to operate and succeed. They attribute their own sphere of influence to the forces of supply and demand in a highly competitive market. In their view, this market is at risk of being constrained by excessive regulation – and the user is the one who will suffer in the end. The solution? Users must learn self-reliance, assume personal responsibility and resist the temptation to have government step in and protect them from themselves.

Key players on the Internet



Business and politics/government are the two most prominent variables and serve as the most important points of reference for the other players. Media professionals, as well as members of the academic community, closely follow the action as policymakers and how business leaders "negotiate the terms" of the Internet; they also keep an eye on which players hold the upper hand at any given time. Representatives of civil society also have their eye on private and public sector players. They see themselves as consultants and idea-generators for policymakers, and as critical readers of proposed policies. Their main focus is on the rights and freedoms of private citizens, and on making sure government does its part to maintain these rights and freedoms. Representatives of civil society see themselves as an integral part of Internet culture and are thus part of the core Internet "shapers". The media and academic communities are located outside this core; they are responsible for observing, recording and classifying. The academic community sees itself, nevertheless, in a much more active role. Academics see themselves as consultants (and admonishers), who are in a position to assign tasks and responsibilities to decision-makers in business and government. As it is, they are largely ignored by these decision-makers.

The points of tension and conflict in the debate between policy-makers and business leaders are familiar. Just as with other controversial issues on today's agenda – such as the financial crisis or the transition to clean energy – core issues such as regulation, voluntary commitment, cost burden, and the interests of private citizens are at the core of the debate over trust and security on the Internet. The debate can thus be considered symptomatic of the relationship between business and government.

The Internet does not exist (anymore)

Opinion leaders see a small window of opportunity for influencing the future course of the Internet with regard to trust and security. This is because "the Internet" will not exist much longer. One can no longer refer to the "Internet per se", they insist, but must view all fields, issues, matters, aspects of life in terms of their online dimension. So it should come as no surprise that these key players question the feasibility – and the logic – of trying to define across-the-board guidelines for security vs. freedom or trust vs. control for the Internet as a whole. But this also means that it will become increasingly difficult to establish universally valid regulations and mutual agreements that actually apply to the space known as "the Internet".

"In the foreseeable future, for most members of society, there won't be an Internet. Instead, we will all simply be accessing online products and services – each in our own very different way. And in many cases we won't even be aware that this thing used to be the Internet."

"Sorry, but you keep referring to the Internet. The Internet doesn't exist. Sure, you can log on to the Internet, but you're probably not going to sit and watch the beautiful TCP/IP packets. You'll go to Amazon, to a travel agency, or maybe to a garden store."

"'The Internet'; that's like saying 'the Germans' – that doesn't even exist anymore. Just as the Germans are made up of many different population groups, immigrant backgrounds, or categories such as singles and senior citizens, etc. These are people who have little or nothing in common with one another. The same thing will happen with the Internet as well."

"You can't have a book of etiquette for digital use; instead, there is a book of etiquette and digital use can be considered a part of it. Because it doesn't distinguish between the ways in which I communicate with you right now – whether we're sitting across from each other, or we write an email or we speak on the telephone."

This demonstrates all the more clearly that developments in the "battle for the Internet" will have a significant impact on how we live in the future and what role that digital infrastructure will play. The issues being debated also make clear that the discourse is moving from a purely technological perspective increasingly towards a question of the "digital culture". Unlike with previous technological revolutions, the question is not just how this technology can make life better and best be integrated into existing economic and social structures. Instead it's about redefining core social values. Due to the tediousness and complexity of democratic decision-making processes and the relatively narrow scope of policymakers' sphere of influence (national or European level), it seems that the power of government to influence developments on this front is, ultimately, limited. At the same time, however, the general population in particular puts the responsibility for ensuring trust and security on the Internet squarely in the hands of the government.

Still, the normative power of the factual is the driving force on today's Internet. Those who have already arrived and established themselves will determine the rules of the game – because where there is open space, there is great opportunity to shape something new.