DIVSI Milieu Study on Trust and Security on the Internet
Condensed version

www.divsi.de
DIVSI Milieu Study on Trust and Security on the Internet
Condensed version

A fundamental social-sciences study conducted by SINUS-Institut of Heidelberg, Germany, for Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Hamburg, February 2012
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) is a non-profit organization based in Hamburg. Its declared mission is to promote confidential and secure online communications. The organization strives to carry out this mission with the support of the academic and research communities. It is also planning to conduct a far-reaching public-service campaign aimed at promoting an understanding of issues among users of the Internet.

The institute promotes an interdisciplinary dialogue among the academic, business and societal communities. With this mission guiding its work, it serves as the ideal forum for discussions about economic, regulatory, legal, societal, cultural and political issues. The basis of its work is formed by far-sighted strategic projects in which the worlds of business, academia and politics are linked.

DIVSI was established by Deutsche Post AG. Its patron is Joachim Gauck.
Table of contents

Foreword by DIVSI patron, Joachim Gauck ................................................................. 4
Introduction by DIVSI director, Matthias Kammer ................................................... 6
The DIVSI Milieu Study on Trust and Security on the Internet ................................. 8
Background and scope ................................................................................................. 11
Key findings .................................................................................................................. 12

Internet milieus on trust and online security

   Digital Vanguard ....................................................................................................... 16
   Efficiency-oriented Performers ............................................................................... 18
   Carefree Hedonists ................................................................................................. 20
   Post-material Skeptics ............................................................................................. 22
   Responsibility-driven Individuals ........................................................................... 24
   Order-seeking Internet Laymen ............................................................................. 26
   The Internet Wary .................................................................................................... 28

Outlook ......................................................................................................................... 30
When Jürgen Gerdes, member of the Deutsche Post Board of Management (MAIL), asked me to become patron of the newly established non-profit organization “Deutsches Institut für Vertrauen und Sicherheit im Internet” (DIVSI), I hesitated for a moment. The first thought that came to my mind was that online security really is a job for knowledgeable IT specialists to handle. Admittedly, I do know how to use today’s means of electronic communication. But I would never be mistaken for an IT expert.

The deeper I ventured into the topic, the faster I realized one thing: Online security and data protection are not simply a matter of technology. The supposedly boundless world of the Internet forces us to grapple with questions that no app can answer for us. At the very latest, the outer limits of cyberspace rise up before us when we have to decide just how much risk, how much responsibility and how much freedom of online activity we are willing to concede to ourselves. It is a decision that, ultimately, is left up to each user to settle.

Language is the starting point of freedom, a fact that moves this question beyond the realm of software programmers. For a long time now, the Internet has been something more than a concern of technicians. It has evolved into a cultural achievement, one that shapes people’s everyday lives. Words that were once the sole possession of specialists have worked their way into the layman’s vocabulary. As a result, the term “data protection” implies a level of security that hardly exists at all. And data protectors cannot protect data. At best, they can control whether data is adequately protected. We see how important it is to pay close attention to the precision of words when we are talking about freedom and self-determination in the world of the Internet, where we now spend more and more time of our lives.

Joachim Gauck
Patron of Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Joachim Gauck served as a member of the Eastern German People’s Chamber for the political movement Neues Forum. The People’s Chamber was freely elected following the fall of the Berlin Wall. Later on he served as the special representative for documents that East Germany’s Ministry of State Security maintained on individuals, special representative of the German government for these documents and then federal commissioner for them.

He is the German member of the Management Board of the European Monitoring Centre on Racism and Xenophobia and chairman of the association “Gegen Vergessen – Für Demokratie” (Against Neglect – For Democracy).

When Jürgen Gerdes, member of the Deutsche Post Board of Management (MAIL), asked me to become patron of the newly established non-profit organization “Deutsches Institut für Vertrauen und Sicherheit im Internet” (DIVSI), I hesitated for a moment. The first thought that came to my mind was that online security really is a job for knowledgeable IT specialists to handle. Admittedly, I do know how to use today’s means of electronic communication. But I would never be mistaken for an IT expert.

The deeper I ventured into the topic, the faster I realized one thing: Online security and data protection are not simply a matter of technology. The supposedly boundless world of the Internet forces us to grapple with questions that no app can answer for us. At the very latest, the outer limits of cyberspace rise up before us when we have to decide just how much risk, how much responsibility and how much freedom of online activity we are willing to concede to ourselves. It is a decision that, ultimately, is left up to each user to settle.

Language is the starting point of freedom, a fact that moves this question beyond the realm of software programmers. For a long time now, the Internet has been something more than a concern of technicians. It has evolved into a cultural achievement, one that shapes people’s everyday lives. Words that were once the sole possession of specialists have worked their way into the layman’s vocabulary. As a result, the term “data protection” implies a level of security that hardly exists at all. And data protectors cannot protect data. At best, they can control whether data is adequately protected. We see how important it is to pay close attention to the precision of words when we are talking about freedom and self-determination in the world of the Internet, where we now spend more and more time of our lives.

Joachim Gauck
Patron of Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Joachim Gauck served as a member of the Eastern German People’s Chamber for the political movement Neues Forum. The People’s Chamber was freely elected following the fall of the Berlin Wall. Later on he served as the special representative for documents that East Germany’s Ministry of State Security maintained on individuals, special representative of the German government for these documents and then federal commissioner for them.

He is the German member of the Management Board of the European Monitoring Centre on Racism and Xenophobia and chairman of the association “Gegen Vergessen – Für Demokratie” (Against Neglect – For Democracy).
The global Internet has everything it takes to undermine the rights of all citizens contained in the first ten articles of the German Constitution. This is particularly the case for the freedoms of speech and the press contained in Article Five – a basic right of our living democracy – and, in the end, it is also the case for the core sentence in our Constitution, Article One: Human dignity shall be inviolable.

To correctly assess such threats to our freedom in the future and to be able to promote trust in the medium, we must devote more sensibility, more attention and more research to the Internet and its users. This is a responsibility that an institution like the Deutsche Institut für Vertrauen und Sicherheit im Internet can assume – and it is the reason I support its work.
The Internet is becoming a part of the lives of more and more people – in the office, at home or on the go via smartphones. It is used as a source of information both privately and professionally independent of time and place. The Internet serves as an important work platform. At first glance, the opportunities provided by the Internet seem unlimited.

Increasingly, though, we hear friends and relatives express their uncertainties and concerns about using the Internet. At times, they lack the necessary routine. But isn’t it said in many studies that 80 percent of the digital society is already online? If so, wouldn’t the daily use of the Internet now be intuitive for nearly 60 million people in Germany?

A basic condition for routine use of the medium is always to “feel secure in using it,” “to be familiar with it” and to place trust in it. There is no such thing as total security, neither in the real world nor in the virtual world. This always boils down to a personal choice between security and freedom and between trust and control. It is a question of “tolerable uncertainty” and of “acceptable risk,” which each individual must answer for himself or herself.

This process of reflection piqued the interest of Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI). We wanted to know now the diverse attitudes about trust and security on the Internet within German society. To find out, we asked the highly respected Sinus-Institut to conduct a fundamental social-sciences study. You are now holding a condensed version of the results produced by the institute.
Let’s start with answers to the questions of who uses the Internet in what ways and why as well as what attitudes are held about trust and security on the Internet and what demands are placed on these two issues: Nearly 40 percent of Germany’s population views itself as digital outsiders. These are people who do not go online at all or do not dare to use the Internet at all or use it only occasionally because of their inability, fear, uncertainty or mistrust. Such people are light-years away from viewing the Internet as a natural part of social and business interactions.

This finding and many other exciting results of the study demonstrate how important it is to take a closer look at our digital society. We intend to do our part to promote additional trust and security on the Internet. I am looking forward to an open dialogue about this issue and cordially invite you to add your voice to it.
DIVSI Milieu Study on Trust and Security on the Internet

The “DIVSI Milieu Study on Trust and Security on the Internet” that DIVSI asked the Sinus-Institut to conduct provides new, valuable insights for anyone who has to do with the Internet – no matter whether he or she comes from the world of politics, the business community or the general public. The study’s findings also challenge a number of assumptions that have been considered valid up to now.

The degree of differentiation and the precision of the DIVSI Milieu Study are unparalleled in research conducted in this area up to now. For this reason, the central findings of the study form a very broad basis that can be used to identify measures designed to enhance trust and security on the Internet.

The DIVSI study breaks down Germany’s population into three groups based on their attitudes toward the Internet and their usage of it:

- **Digital Outsiders**: This group is either completely offline or very insecure about the Internet, which it has hardly ever used.

- **Digital Natives**: Members of this group have grown up with the Internet and have completely integrated it into their daily lives.

- **Digital Immigrants**: This group does indeed use the Internet on a regular basis, but only very selectively. It also takes a skeptical view of many developments, particularly in terms of security and data protection.

**Key findings**

The study found that about 40 percent of Germany’s population belong to the group of Digital Outsiders. This finding challenges the previously held view that about 80 percent of the country’s population is online and about 20 percent is offline. This, in turn, raises doubts about the related views regarding the state of the digital society in Germany. The results of the DIVSI study suggest that twice as many people in Germany live completely or almost completely without the Internet. This means that nearly 27 million of the approximately 72 million members of the digital society in Germany are Digital Outsiders.
The DIVSI Milieu Study also found that about 41 percent of all Germans belong to the group known as *Digital Natives*. These are people who have grown up with the Internet and have completely integrated it into their daily lives. *Digital Natives* can no longer imagine a life without the Internet. For this reason, their motto could be: “I surf. Therefore, I am.”

The remaining 20 percent of the German population could be called *Digital Immigrants*. On the one hand, they use the Internet only when they expect to gain a direct benefit – let’s say in planning a vacation or hunting for a bargain on a particular item. On the other hand, members of this population group have, to some extent, specific concerns about the Internet and take steps to ensure that they will not become dependent on that technology.

**The DIVSI Milieu Study on Trust and Security on the Internet provided significant findings.**

In the past, discussions have assumed that the digital society in Germany is split between onliners and offliners. But a breakdown solely between online and offline does not accurately reflect the reality. The crucial point is how people actually use the Internet. Drawing on this assumption, the study concludes that there are two boundaries, not one, running through the digital society.

The first boundary separates *Digital Outsiders* from *Digital Immigrants* on the one hand and from *Digital Natives* on the other. Digital Outsiders are either offline or are very insecure about using the Internet. For these people, the Internet represents a digital barrier blocking off a world from which they feel excluded and to which they have no access.

The second boundary separates *Digital Natives* on the one hand and *Digital Immigrants* and *Digital Outsiders* on the other. Digital Natives view the Internet as a normal part of their environment, a place in which they roam freely and naturally. The digital world represents a fundamental part of their life. They have a very positive attitude toward it, and they cannot believe that some people do not feel equally at home on the Internet as they do.

In addition to these central findings, the DIVSI Milieu Study reached another, very important conclusion. There are two aspects to this finding.

First, people’s behavior on the Internet and their attitudes toward trust and security are primarily based on differing concepts about responsibility. While one group demands more government support in efforts to ensure secure usage of the Internet, the other group stresses the importance of individual responsibility. Specifically, the DIVSI Milieu Study found that nearly three out of four Germans (74 percent) expect the government and business community to actively ensure online security. By contrast, the majority of *Digital Natives* (26 percent) thinks the issue of security should be left to individual users. This group feels competent enough to recognize the Internet’s risks and is able to deal with them. Freedom, usage and flexibility take absolute precedence over government regulations, something that is categorically rejected by some of them.
Second, the population is also shaped by various views about the question on how secure the Internet can actually ever be. The DIVSI Milieu Study found that about one-third of all Internet users in Germany believe that total security on the Internet could be achieved. Surprisingly, many Digital Natives feel this way. On the other hand, about half of users think it is impossible to have total online security. The remaining respondents had no clear position on this question.

The study’s findings reveal one thing: To increase trust and security on the Internet, German political leaders face a major challenge of satisfactorily meeting diametrically opposed security needs. These needs arise from the following key points:

- Nearly three out of four Germans demand that the government takes steps to ensure online security.

- A majority of Digital Natives, who would be most strongly concerned by such government action, reject such steps and do not have, to a certain extent, any understanding of the problems and needs of other population groups in terms of the Internet and its use.

As a result, finding a common ground among these diverse points of view will be a major socio-political challenge. In Joachim Gauck, DIVSI has a patron who can help build a bridge between the various population groups in Germany’s digital society.
The DIVSI Milieu Study in brief

Background and scope

The mission of “Deutsches Institut für Vertrauen und Sicherheit im Internet” (DIVSI) is to promote the development of a secure, trustworthy Internet for economic and social purposes. All activities needed to carry out this effort require a deep understanding of how and why people use the Internet, of the motives and barriers regarding the use of certain Internet offers and of the attitudes and needs regarding online security that arise as a result.

DIVSI commissioned the Sinus-Institut of Heidelberg, Germany, to conduct a socio-scientific baseline study that, for the first time, presents the diverse attitudes toward the issue of trust and security on the Internet in a representative population typology in Germany.

Research design and methodology

Module 1: qualitative
- Explorative pilot study (60 qualitative in-home interviews): unbiased collection of existing perceptions and attitudes toward the issue
- Data-collection period: June-July 2011
- Output:
  - Deeper understanding regarding relevant attitude dimensions (concerns, risks, awareness, requirements etc.)
  - Understanding of milieu-specific approaches to the issue of trust and security on the Internet
  - Basis for preparing the concept and content of the main study

Module 2: quantitative
- Representative survey of the population to test, validate and quantify the hypotheses
- Sample: 2,000 cases; representative for Germany’s resident population aged 14 and older
- Data-collection period: September-October 2011
- Chief determining factors for type formation:
  - Attitudes toward data protection and data security
  - Internet usage
  - Environmental background (Sinus-Milieus®)
- Completion of report: December 2011

Result: holistic typology

Internet milieus on trust and security on the Internet

* The Sinus-Milieus® are the result of three decades of socio-scientific research. The starting point is an environmental analysis of our society. The Sinus-Milieus form groups of people who have similar attitudes toward life and lifestyles.
Key findings

- Eighty percent of Germans and nearly all people under 30 (98 percent) are online. But many think that the Internet is not transparent in terms of security and data protection.
  - The terms “data protection” and “data security” are confused or used almost interchangeably.
  - Half of respondents say they lack information on what they personally can do to protect their data.
  - A full one-third of onliners acknowledge: “I’d be lost in the Internet if my friends and acquaintances didn’t help me out.”

- 39 percent of Germany’s population is troubled by the issue of security and data protection on the Internet and feel uncertain as a result.

- Half of the population strongly believes one thing: Absolute online security cannot and will not be achieved. But one-third of the population thinks it is possible.

- One new aspect has become more significant than the (gradually fading) “digital boundary” separating onliners and offliners. This is the mentality boundary that has arisen between various types of users and their (subjective) Internet competence – depending on their respective attitude toward security and their risk behavior.

- Security is a question of attitude: Imagined competence can play just as important a role in decisions related to the acceptance of risk as the use of security software can.

- The subjective feeling of security increases as a person’s own experience with the Internet grows. This means that the lack of technical familiarity about the Internet is more frequently a reason for avoiding specific Internet activities than security concerns are.

- To provide systematic education about and understanding of the issue as well as to assess the expectations and concerns that exist about the Internet, seven different Internet milieus (types of attitudes and behavior) were identified – each with different lifestyles, various levels of access to the Internet and attitudes about trust and security on the Internet (see the overview on the following page).

- Nearly 60 percent of Germany’s population thinks responsibility for security and data protection on the Internet primarily rests with companies and/or the government, which should create the necessary conditions.

- This desire to delegate responsibility results, on the one hand, from ignorance and a feeling of being overwhelmed (Digital Outsiders: 39 percent) and, on the other hand, from skepticism about the current approach (Digital Immigrants: 20 percent).

- A latent feeling of mistrust of the system even exists among those users, who consider themselves to be self-confident navigators on the Internet and explicitly assume responsibility for their Internet activities.
Brief description of the seven Internet milieus

Digital Outsiders

The Internet Wary
Overwhelmed offline users and occasional users of the Internet. Self-sufficiency, moral principles and integrity. Desire for security and control mechanisms.

Order-seeking Internet Laymen
The middle-class mainstream that wants order and reliability. Defensive-careful Internet usage.

Digital Immigrants

Responsibility-driven Individuals
Educated establishment with a grasp of leadership. Selective Internet users. Responsibility-driven attitude toward digital progress.

Post-material Skeptics
Target-oriented Internet users with a critical attitude toward commercial structures and “blind” fascination about technology.

Digital Natives

Carefree Hedonists
Fun-loving Internet users looking for entertainment and adventures. Unconventional – no awareness or concerns about potential risks.

Efficiency-oriented Performers
Performance-driven Internet pros with distinct focus on convenience and benefit. Professionalization as guiding principle.

Digital Vanguard
Digital avant-garde with a strong interest in individualization. Interest in independent thinking and actions.
The measures needed to achieve further trust and security depend on attitudes, experiences and expectations regarding the medium: One measure by itself does not help. Rather, diverse courses of action tailored to the respective needs of individual target groups must be employed.

Individuals who have grown up with the Internet tend to underestimate the medium’s dangers and risks as a result of their familiarity with it.

- In particular, Carefree Hedonists act recklessly and rashly online, also because they spend little time reflecting on the consequences of their actions.

- Even though they are highly aware of the problems, the Digital Vanguard and Efficiency-oriented Performers tend to underestimate the growing dangers and risks, also and precisely because of their high level of Internet skills.

- Responsibility-driven Individuals and Post-material Skeptics have a fundamental understanding of the problems and an increased awareness of risk as a result.

- A distant attitude exists among the group of Order-seeking Internet Laymen and the Internet Wary, created by their lack of experience with the medium and a general lack of familiarity with it. As a result, many Internet services are not used by these groups.

Given these findings, the issue of trust and security on the Internet becomes a pressing socio-political matter. The aim must be to eliminate the barriers and concerns as well as to offer programs and services that provide or have the potential to provide increased security.

Efficiency-oriented Performers and the Digital Vanguard can serve as the central target group for the issue of trust and security on the Internet. On the one hand, they are affected to the greatest degree by the security risks as a result of their intensive use of the Internet. On the other hand, they are key messengers who can raise the awareness level about the issue among other groups. They play the role of a guide, particularly for inexperienced Internet users, and act as important points of contact about appropriate ways to use the medium.

At the same time, a liberal, individualist attitude is widely found among both of these groups – just as it is among Carefree Hedonists. Digital Natives have very little understanding for the problems of inexperienced Internet users: It is up to the user, above all, to assume responsibility for his or her online activities (self-responsibility principle). For this reason, it is necessary to help Digital Natives realize that not everyone has the same level of “Internet expertise” as they do and are thus subject to higher risks and dangers under certain circumstances.

The graphic on the following page shows the types found in the Sinus-Milieus® study with the two main axes reflecting fundamental values (horizontal) and social situation (vertical). Within this socio-cultural context, the seven types are positioned in accordance with their dominant milieu background.
The higher a group is located in the graphic, the higher its level of education, income and professional status is. The farther to the right it reaches, the more contemporary its fundamental values are in socio-cultural terms.

The Internet milieus can be grouped into three segments.

- **Digital Outsiders** (39 percent): They are either completely offline or are very insecure about going online. Of the 72 million people aged 14 and older in Germany, 27 million individuals fall into this category. These people feel the Internet forms a digital barrier to a world from which they feel shut off.

- **Digital Immigrants** (20 percent): They use the Internet regularly, but very selectively. They did not grow up in a digital world and are very skeptical about many aspects of it, particularly in terms of security and data protection on the Internet.

- **Digital Natives** (41 percent): To this group, the digital world is a natural part of their lives. They move about the Internet like fish in water – their motto is: “I surf. Therefore, I am.” They have a very positive view of the Internet and view the continuing digitalization of the world primarily as a personal opportunity.

### Internet milieus on trust and online security

<table>
<thead>
<tr>
<th>Attitude toward Internet</th>
<th>Retaining Tradition</th>
<th>Having &amp; enjoying Modernizing / individualizing</th>
<th>Being &amp; changing</th>
<th>Doing &amp; experiencing New orientation</th>
<th>Exceeding limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower middle class</td>
<td>Unease, overload, exclusion</td>
<td>Feelings of responsibility, skepticism</td>
<td></td>
<td>Multi-optionalism, connected, free of borders</td>
<td></td>
</tr>
<tr>
<td>Lower class</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retaining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preserving</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preserving Tradition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preserving Tradition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order-seeking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Laymen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Efficiency-oriented</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Efficiency-oriented</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Vanguard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Vanguard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Natives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Natives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Immigrants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Immigrants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Outsiders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Outsiders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Segment: Digital Natives

Internet milieu: Digital Vanguard (15%) – 10.3 million

The Digital Vanguard feel right at home in the Internet, and most of them have grown up with it (Digital Natives). They have extensive IT skills and, as a result, spend significant amounts of time online. To this group, being online is not a technical activity. Rather, it represents a description of a situation and, thus, a natural moment of their everyday private and professional lives.

The Digital Vanguard are young, unattached and flexible users from upper, post-modern social milieus. They do not systematically acquire IT knowledge. Instead, they obtain it in a creative, playful manner, that is, intuitively to a large extent. Even though they know that security and data protection are not always assured online, they rarely impose any limits on their activities. Rather, they put their faith in their own skills and their “imagined” self-assurance: “Who is most likely to survive online? – We are!”

In a comparison of types, the Digital Vanguard have the most self-confidence about going online. Drawing on their self-image as representatives of the digital avant-garde, they not only are committed to developing the unlimited possibilities of the Internet, but also view themselves as being at the forefront of a social movement striving for more freedom, participation and democracy. This attitude is reflected in particular by the call for a maximum amount of self-responsibility in terms of security and data protection.

The Digital Vanguard think they are capable of expertly navigating their way through cyberspace and, as a result, think they are immune to the dangers and threats posed by it. This milieu has no understanding for the insecurities of many inexperienced users and their desire for more government control and monitoring. Instead, the Digital Vanguard view the debate about more online security as a guise for further monitoring and control – a change that would serve the interests of business and government, not consumers. As a result of this narrow view, inexperienced users who are insecure as a result of their lack of know-how and thus reject the medium are not the only group that moves out of the picture. The Digital Vanguard themselves also underestimate their own need for protection.

<table>
<thead>
<tr>
<th>Internet expertise*</th>
<th>4.4</th>
<th>(index 143)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective security**</td>
<td>51%</td>
<td>(index 129)</td>
</tr>
</tbody>
</table>

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”
** Agreement with the statement “personal data on the Internet is very secure/secure”
The Digital Vanguard (15%) – 10.3 Mio.

**Attitude profile**

<table>
<thead>
<tr>
<th>Index</th>
<th>Typical statements*</th>
<th>Index</th>
<th>Typical statements*</th>
</tr>
</thead>
<tbody>
<tr>
<td>176</td>
<td>For me personally, I could not imagine life without the Internet. (88%)</td>
<td>21</td>
<td>Online, I am fairly reserved because I’m worried about making mistakes. (13%)</td>
</tr>
<tr>
<td>149</td>
<td>The Internet is a free medium and should not be regulated under any circumstances. (72%)</td>
<td>23</td>
<td>The idea that in the future much has to be done online scares me. (11%)</td>
</tr>
</tbody>
</table>

*Top 2 boxes of a scale from 1 to 4 (“strongly agree”/“agree”)

**Communication requirements and needs for action**

- Raise awareness of how to deal with personal data
- Education about potential security gaps and risks
- Create an understanding that not all people (can) roam about cyberspace confidently and so are exposed to a higher degree of danger
As the second-youngest Internet milieu, Efficiency-oriented Performers have a high level of IT and Internet expertise. As a result, the technology they use is state of the art. They are intensive users of the Internet – for both entertainment and (even more) for professional purposes. The Internet is primarily viewed from a utilitarian-pragmatic perspective and is generally used to make work easier, simplify things and accelerate them.

Members of this group are driven by a will to succeed and perform. They have tremendous self-confidence and generally belong to upper social milieus and the young, contemporary middle class of society. In a comparison of types, the Efficiency-oriented Performers have the highest income level, possess a distinct can-do attitude and intelligently, vigorously and flexibly keep up with developments, from which they want to benefit as quickly as possible. Even though they are aware of data-protection problems, they take an optimistic approach to security issues and put their faith in their own skills and technological progress. When they go online, security issues are a secondary concern because they use the best security technology and believe that they can move about cyberspace in a targeted, reliable manner.

This group is particularly interested in the freedom-oriented structure and organization of the Internet. After all, it is the openness of the Web that unleashes the enormous innovative potential that this group wants to profit from. The Internet should not be subject to bureaucratic regulations under any circumstances whatsoever. On the other hand, this group thinks that calls for an “anarchically” organized Internet go too far. Efficiency-oriented Performers want to find a compromise between freedom and security.

Above all, they think it is up to users and, thus, themselves to act responsibly, particularly by using security software and acting in a controlled manner online. But they are happy to delegate the details to experts. With the purchase of software, a certain amount of security is acquired, and this security flows into a personal account of good faith. Ideally, the residual risk should be reduced by taking systematic steps. In this regard, they think this responsibility rests with the government and, even more, with major brand companies. They primarily expect hard facts and concrete services from these companies, not public-service information.

<table>
<thead>
<tr>
<th>Internet expertise*</th>
<th>4.1</th>
<th>(index 133)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective security**</td>
<td>67%</td>
<td>(index 167)</td>
</tr>
</tbody>
</table>

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”
** Agreement with the statement “personal data on the Internet is very secure/secure”
Efficiency-oriented Performers (14%) – 10.0 million

Attitude profile

During the survey, typical statements were collected among Digital Natives. Of these, the following statements were noted as the most common:

- As far as the Internet is concerned, I always want to be on the cutting edge of technology. (87%)
- By using common sense and the latest security options, you can adequately protect yourself from online risks. (94%)
- I feel helplessly exposed to online threats. (9%)
- I require more information on how I personally can protect my data online. (15%)

Communication requirements and needs for action

- Need for professional security products
- Systemic actions by trustworthy institutions
- Raise awareness of dealing with own data. But: facts and specific services, rather than public-service information
Carefree Hedonists are fun-loving users with average Internet skills and experience. But they also have little fear about the medium. This Internet milieu primarily includes young people from the contemporary middle and lower classes who really enjoy the easy access to entertainment and communications that the Internet provides, and intensely use social networks as well as the music and games found on the Web.

When they go online, Carefree Hedonists are looking for entertainment, distraction and reassurance, not least because they are trying somewhat to compensate for the unspectacular daily lives they think they are leading. They want intense stimulation and are in the habit of using several media at the same time.

They have little awareness of online threats. As a result, they have few security worries and tune out the risks – they are more interested in fun and the personal usage factor (relaxed in the Web). One of the characteristic features of this group is its carefree attitude toward data security and data protection: “Why worry? The Internet is uncontrollable anyway.”

In a comparison of types, Carefree Hedonists have the lowest awareness level. They act without having major concerns about security and consciously disregard the risks (indifference) or unconsciously disregard them (ignorance). For this reason, Carefree Hedonists are the group that is most exposed to online dangers. Their intensity of usage is high, particularly with social media. In the process, private data are placed online with relatively little thought. Virtual locations where they pursue their diversions and interests, find inspiration and show off have become an essential part of their daily lives. Carefree Hedonists do not think that they are appealing targets for hacker attacks and sometimes cannot believe what companies could do with data about them.

While Efficiency-oriented Performers favor “both” self-responsibility and systemic measures, Carefree Hedonists have a rather fatalistic attitude of “either/or.” Self-responsibility runs head-on into their indifference and apathy. Above all, they would use services or pre-installed software programs that they would not have to spend much time dealing with. But they have a fundamental distrust of institutions and support an unregulated Internet as a result.

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”
** Agreement with the statement “personal data on the Internet is very secure/secure”
Carefree Hedonists (12%) – 8.7 million

Attitude profile

<table>
<thead>
<tr>
<th>Attitude profile</th>
<th>Overall</th>
<th>Carefree Hedonists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring/control</td>
<td>74%</td>
<td>68%</td>
</tr>
<tr>
<td>Selective trust</td>
<td>64%</td>
<td>71%</td>
</tr>
<tr>
<td>Skepticism/distance</td>
<td>60%</td>
<td>56%</td>
</tr>
<tr>
<td>Self-responsibility/liability</td>
<td>57%</td>
<td>64%</td>
</tr>
<tr>
<td>Online freedom</td>
<td>57%</td>
<td>69%</td>
</tr>
<tr>
<td>Delegation/restrictions</td>
<td>56%</td>
<td>61%</td>
</tr>
<tr>
<td>@home/online competence</td>
<td>51%</td>
<td>61%</td>
</tr>
<tr>
<td>Unconcern</td>
<td>22%</td>
<td>54%</td>
</tr>
</tbody>
</table>

Typical statements*

I don’t worry at all about online security. What could happen to me anyway? (62%)

If I lose data in the Internet, I’ll get it back sometime later. (59%)

I try out new online services and developments right away. (47%)

Communication requirements and needs for action

- Education about individual liability and the legal impact of online actions
- Raise awareness of using data
Internet milieu: Post-material Skeptics
(10%) – 6.7 million

Post-material Skeptics have an ambivalent relationship with the Internet: On the one hand, they like the information and convenience the Internet offers. On the other, they have doubts about virtualization, globalization and the faith being placed in progress. This Internet milieu is not technophobic. But members of this group do not want technology to dominate their lives and intend to maintain control of them.

A conscious approach to media is essential to Post-material Skeptics: They reject the growing infiltration of technology into daily life that is occurring as part of a general “acceleration mania” and assume a distant, culturally critical attitude toward the entire consumption- and media-driven society. But this also includes an examination of its challenges. This milieu does not include the laggards, and its use of the Internet is slightly above average – even if it is very selective: Above all, the members of this milieu are interested in the information and communications options available to them on the Web.

The members of this group cover a wide span of ages (20 years to 60 years) and are frequently part of the environmentally conscious mainstream. They lead a sustainable lifestyle and are prepared to give up something at once and put their needs on hold if they think that certain behavior will have a negative social and environmental impact over the long term.

Post-material Skeptics have doubts about online security and protection of personal data. They mistrust commercial providers as well as government agencies (fear of manipulation and monitoring). This milieu believes that many users are too careless and naive in handling their personal data, particularly in social networks. For this reason, their concept of responsibility primarily focuses on improving the media and Internet skills of individual users. In doing so, they place their faith in the responsibility of free citizens. In this regard, the government should provide support through public-service and education campaigns, but not create control mechanisms in the form of laws and censorship that could hurt democracy in the Web.

Post-material Skeptics believe that the opportunities and potential offered by the Internet (i.e., freedom of expression) do indeed require institutional security mechanisms – but they think it is a job for autonomous organizations. They think non-government organizations are in the best position to ensure transparency and uncover problems and security gaps as part of their public-service activities. This approach could create trust by casting doubt on the improbable guarantee of 100 percent security that places blind faith in the system. They think that systemic measures can only provide information about security gaps and strengthen individual responsibility. But they cannot take the place of the individual user’s own responsibility.

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”
** Agreement with the statement “personal data on the Internet is very secure/secure”
Internet milieu: Post-material Skeptics (10%) – 6.7 million

Attitude profile

Typical statements*

The quality of personal relationships suffers from excessive online communication. (79%)

You can’t have online data security. (65%)

Typical statements*

You have nothing to fear on the Web if you have nothing to hide. (17%)

I really believe that large, well-known brands handle personal data online carefully. (31%)

Communication requirements and needs for action

- Search for services provided by authentic, non-commercial institutions that guarantee transparency and systematically strive to educate the public
- Confidence building through education and proactive steps to increase transparency (self-imposed regulations, external audits and controlling)
- Improvement of the public’s competence to use the Internet
Use of the Internet in this milieu is characterized by pragmatism and utilitarian thinking (convenience benefits). Technology does not exert a strong hold on this professionally and financially established group. Rather, members of this milieu view it simply as a means to an end. As long as doing things online provides a specific benefit, Responsibility-driven Individuals are open to change and are willing to integrate technological advances into their everyday lives. They reject technological “coercion,” refuse to use certain online options to simply go along with the crowd (the “me-too principle”) and, in general, oppose the trend toward superficiality and sensory overload.

Responsibility-driven Individuals are demanding, selective users who are interested in technical innovations and the opportunities they create for users. But they have only average Internet expertise (many Digital Immigrants). Members of this group primarily use the Internet as a work and communications medium – and not for entertainment purposes. They take a very systematic and responsible approach to their online activities.

A strong awareness of security and protective measures, including the installation of virus scanners, firewalls, etc., has a high priority – this has less to do with fear and more to do with common sense. Responsibility-driven Individuals take a very active, exploratory approach to information available online, but are very reluctant to reveal their personal information. Having been exposed to media reports and recommendations about security measures, they do not want to take any unnecessary risks. This Internet milieu strives to protect its private sphere by exercising restraint, control and avoidance. Most of its members think the Internet is highly complex and that the security software they use does not provide 100 percent protection from the misuse of data.

Responsibility-driven Individuals have little faith in their own ability to navigate their way through cyberspace, even though they yearn for it because it fits into their view of themselves. For this reason, they have a great need for information about self-protection and a corresponding demand for professional security products.

At the same time, they believe the entire society and government institutions in particular should take steps to ensure more online security on the one hand and a more responsible attitude about using the Internet – particularly in terms of less reflective users – on the other.

---

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”

** Agreement with the statement “personal data on the Internet is very secure/secure”
Responsibility-driven Individuals (10%) – 7.3 million

Attitude profile

Typical statements*

<table>
<thead>
<tr>
<th></th>
<th>Index</th>
<th>Typical statements*</th>
</tr>
</thead>
<tbody>
<tr>
<td>I believe I’m capable of assessing online security risks correctly and of reacting accordingly. (66%)</td>
<td>132</td>
<td>Above-average agreement</td>
</tr>
<tr>
<td>The Internet offers more opportunities than risks. (84%)</td>
<td>124</td>
<td>Above-average agreement</td>
</tr>
</tbody>
</table>

Typical statements*  | Index |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Actually, I’m overwhelmed by the Internet as a medium. (3%)</td>
<td>9</td>
</tr>
<tr>
<td>I personally don’t care about what happens to my data online. (3%)</td>
<td>29</td>
</tr>
</tbody>
</table>

*Top 2 boxes of a scale from 1 to 4 ("strongly agree"/"agree")

Communication requirements and needs for action

- Need for more information on self-protection and for professional security products
- Desire for an expansion of online competence and awareness within the public, particularly among inexperienced, careless users
- Government action for more online security
Internet milieu: Order-seeking Internet Laymen (12%) – 8.2 million

To Order-seeking Internet Laymen, the World Wide Web is “uncharted territory”: They use it infrequently and very carefully. Because they worry about making a mistake, their approach to this medium consists largely of avoidance strategies – “playing it safe.” Their general attitude about the Internet is characterized by abstinence and vigilance.

As a result, they use the Internet defensively and formulate no specific demands because they generally (would like to) use basic functions. Given their lack of self-confidence in using the Internet, they are happy to receive help from others.

Order-seeking Internet Laymen are members of the conventional mainstream who have a strong desire for harmony and security in simple to mid-level social strata. In a comparison of types, they are the second-oldest segment.

As a rule, members of this group mistrust the Internet, particularly in terms of security and data protection. Even though these issues do not play much of a role in the offline world in which they live, headlines about cases of data misuse attract this group’s attention: They intensify the calls by Order-seeking Internet Laymen for a strong government that will significantly limit and control the “risks and side effects” of the Internet. Demands for strict legal regulation of the Internet are widely supported here because this group hopes that the virtual world that seems so overly complicated to them can be “reined in” through such regulations.

They prefer to delegate responsibility for a secure Internet to the government because it is viewed as a shield against all types of criminal assaults. As a result of their limited Internet skills, members of this group think the chances that an individual can protect himself or herself from misuse in the Internet are very low. Digital abstinence is and will remain the most secure form of self-protection.

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”
** Agreement with the statement “personal data on the Internet is very secure/secure”
Order-seeking Internet Laymen (12%) – 8.2 million

Attitude profile

<table>
<thead>
<tr>
<th>Communication requirements and needs for action</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Search for simple, reliable services, guaranteed by trusted institutions</td>
</tr>
<tr>
<td>- Creation of legally binding rules of behavior</td>
</tr>
<tr>
<td>- Awareness-raising efforts regarding the issue of security, particularly by personally known people who are well versed in the subject</td>
</tr>
</tbody>
</table>
Internet milieu: The Internet Wary
(27%) – 19.1 million

The Internet Wary are occasional users of the medium (two-thirds are offliners anyway) who have very little knowledge about the Internet and little contact with digital media in their daily lives. To this group, the oldest of the milieus, the Internet is a strange world and seems threatening. Members of the group use only the basic functions and rely on the help of others.

They feel overwhelmed by the variety of information and communications technologies and suffer from the complexity, speed and amount of information. They have a hard time using the Internet, and they frequently feel helpless in this regard. At times, this leads to resignation and a general feeling of resistance – after all, they see few advantages or conveniences that the Internet can provide to their own lives.

Members of this group can be generally found in the traditional segment of society. In other areas of life, they also have a fundamental need for straightforwardness and a slower pace. The focus is less on searching for the new and unknown. Rather, it is placed on the achieved and the people and things a person already knows.

Their understanding of the dangers associated with the Internet is limited. As a result, they are extremely insecure. They have an exceptionally high desire for protection, triggered by their general skepticism and fear of data misuse. This feeling has less to do with the individuals themselves, but rather with their children and grandchildren because members of this group rarely, if ever, go online. The diffuse awareness of risks intensifies the feeling of living in an increasingly unsafe and threatening world.

The Internet Wary clearly think the government should provide online security and data protection. They support increased controls of the virtual world and call for the rules and restrictions that would make such controls possible. Just like in the real world, the government should assure law and order online, track down criminals and bring them to justice. Anonymity or the opportunity to pretend to be someone else should not be possible at all – and if someone deceives people online, actions should be immediately taken to “put the cuffs” on this person.

Segment: Digital Outsiders

Internet expertise* 1.5 (index 47)
Subjective security** 16% (index 39)

* Self-evaluation on a scale of 1 = “beginner” to 6 = “expert”
** Agreement with the statement “personal data on the Internet is very secure/secure”
The Internet Wary (27%) – 19.1 million

**Attitude profile**

<table>
<thead>
<tr>
<th>Attitude</th>
<th>Overall</th>
<th>The Internet Wary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring/control</td>
<td>74%</td>
<td>71%</td>
</tr>
<tr>
<td>Selective trust</td>
<td>64%</td>
<td>40%</td>
</tr>
<tr>
<td>Skepticism/distance</td>
<td>60%</td>
<td>76%</td>
</tr>
<tr>
<td>Self-responsibility/liability</td>
<td>57%</td>
<td>46%</td>
</tr>
<tr>
<td>Online freedom</td>
<td>57%</td>
<td>29%</td>
</tr>
<tr>
<td>Delegation/restrictions</td>
<td>56%</td>
<td>66%</td>
</tr>
<tr>
<td>@home/online competence</td>
<td>51%</td>
<td>7%</td>
</tr>
<tr>
<td>Unconcern</td>
<td>22%</td>
<td>9%</td>
</tr>
</tbody>
</table>

**Typical statements***

- I’d be lost in the Internet without the help of friends and acquaintances. (76%)
- I feel helplessly exposed to the dangers of the Web. (69%)

**Index**

- I’d be lost in the Internet without the help of friends and acquaintances. **188**
- I feel helplessly exposed to the dangers of the Web. **176**

**Typical statements***

- I couldn’t imagine life without the Internet. (3%)
- I keep up to date with developments regarding online data security and data protection. (8%)

**Index**

- I couldn’t imagine life without the Internet. **7**
- I keep up to date with developments regarding online data security and data protection. **19**

*Top 2 boxes of a scale from 1 to 4 ("strongly agree"/"agree")

**Communication requirements and needs for action**

- Need for steps to build confidence and to eliminate insecurity
- Desire for specific personal assistance
- Search for simple, secure services, guaranteed by trustworthy institutions
- Desire for control of cyberspace by government officials; call for order, rules and restrictions
Outlook

Who is responsible for security and data protection on the Internet?

Depending on what an individual does online and how far the Internet is integrated into this person’s daily life, a number of different positions arise regarding the extent to which users themselves or other organizations (i.e., companies and government agencies) can, want to and should assume responsibility.

The graphic at the bottom of this page shows the intersection of self- and outside responsibility as well as the respective awareness levels of the seven Internet milieus. The level of self-responsibility among users tends to rise with the level of skills and confidence. Conversely, responsibility is increasingly delegated as the level of familiarity with the Internet falls. In a nutshell: People who are unfamiliar with the Internet want protection, and people who are familiar with it want freedom.

This results in a particularly complex challenge: Those people who intensively and extensively use the Internet – and would thus be affected to a greater degree by potential government measures – are the individuals who tend to want less responsibility to be assumed by governments and companies or take a critical stance toward this and “digitally detach” themselves as a result of their own knowledge – also because they have no understanding of the digital barriers that exist among other societal groups. They view the Internet – in a positive-empathetic way – as an unregulated region of possibilities, the control of which can be done only to a limited extent or is not desired at all.

Allocation of individual and outside responsibility in the target groups
The array of views about the division of responsibility clearly shows that the challenges of future measure-planning activities and communications will not primarily involve overcoming the boundary that separates onliners from offliners. Rather, within the context and trust and security, a yawning gap in user’s confidence has developed in the digital society. The critical factor is not (only) who is online, but also how users are online, what they do and do not do when they are online and which conditions must be created to enable trust in Internet activities to arise and barriers to be overcome. In this regard, three fundamental segments can be formulated, and each of the seven attitude types can be assigned to one of them:

**Responsibility and trust among Digital Outsiders**

In cyberspace, digital outsiders feel as though they are visiting an alien planet. In terms of digital cultural technology, they are novices who possess no or very limited skills. As a result, they feel as though they are hardly in a position to take responsibility when they use the Internet on their own because they have very little ability to assess the consequences of their actions. For this reason, they turn to third parties for help with online security and data protection, preferably the government, which they think should take action and write the necessary regulations. But this segment only has a vague notion about the details regarding such steps because members of this group know too little about the Web’s principles and modes of operation. The level of awareness about online security (see the dotted line on the graphic on page 30) is very low in this group. Digital Outsiders learn about data misuse and Internet crime only by chance in the media and frequently cannot grasp the extent of the problem. Nonetheless, such headlines grab their attention and reinforce their feeling that they are living in an increasingly uncertain and threatening world. In response, Digital Outsiders frequently become even more cautious when they use the Internet (if they use it at all).

This also means that potential protective measures must be as clear and understandable as possible when they are implemented and communicated to ensure that they promote trust and, thus, facilitate access to the medium and do not create higher digital barriers. This can be achieved by providing specific contact persons or testimonials, among other steps. After all, personal feedback is extremely important to this segment.

**Responsibility and trust among Digital Immigrants**

Unlike Digital Outsiders, Digital Immigrants understand the significant role that the Internet plays in commerce, democracy and globalization. Both Responsibility-driven Individuals and the Post-material Skeptics are very interested in current developments and actively use the media to keep themselves informed. They also pay attention to the issue of online security and data protection. Some of them are even better informed about the topic than Digital Natives are. As a result, their level of awareness is particularly high (see the graphic on page 30). On the one hand, they welcome advances in communication technology and systematically use online products and services for their own purposes. On the other hand, they are quite aware of the negative consequences of the digitalization process. They vigilantly keep abreast of the growing criminal tendencies arising in the unregulated digital world. They are concerned about the trend in which people are increasingly opening up their private lives in social networks – an action that could have unforeseeable consequences for users.
For this reason, they think responsibility for increased online security is primarily a job for the entire society to perform. They also believe that this responsibility should not be delegated to higher-ranking institutions and that it is an issue that should be addressed by all citizens. To form a solid basis for such action, this segment thinks the great need for education and information must be addressed.

**Responsibility and trust among Digital Natives**

Compared with Digital Immigrants and Digital Outsiders, Digital Natives worry less about the possibility that the security of their data could be threatened as a result of their lack of knowledge. It is primarily their familiarity with the Internet that enables them to use the medium as their playground without constantly thinking about security. Their level of awareness for the topic of security and data protection is low as a result. As beneficiaries of digitalization, Digital Natives primarily see the positive side of the Internet, even though they are well aware of the criminal activities of hackers and loose data-protection regulations – from their point of view. Every other member of this group expressed doubts about the security of online banking and social networks. The willingness of so many to play this game of “data-protection roulette” is not least the result of the fact that they have had no negative experiences thus far. Their immense, if not boundless, trust in the Internet has yet to be shaken. For this reason, they focus in particular on self-responsibility as a last resort. Even though they (particularly the Efficiency-oriented Performers) support systematic measures to a certain degree, their main interest is primarily directed at their own personal security needs. They rarely become a strong voice in the debate about data security and do not consider the perspective of the entire society.

**Conclusions**

The broad array of attitudes, expectations and the related willingness to act in terms of trust and security on the Internet clearly demonstrates that the solution cannot be found in individual measures.

In a reflection of this, a low level of awareness for the issue of online security and data protection can mean very different things – one group has a low level because its members assume that they already know enough and are so well-versed in the Internet that they do not raise any questions at all. Another group has a low level of awareness because its members believe that they lack the knowledge they need to seriously explore the issue.

As a result, the major socio-political challenge is to develop programs and measures designed to create additional trust and security on the Internet that address the large number of motivations, skills and potential conflicts in the respective Internet milieus and, thus, in the digital environment – be it in terms of content, formats or means of communication.