# User Perceptions and Attitudes in the Data Economy and their Contradictions

Uwe V. Riss, Edith Maier
Institute for Information and Process Management
Eastern Switzerland University of Applied Sciences
St.Gallen, Switzerland
email: {uwe.riss, edith.maier}@ost.ch

Michael Doerk
Institute of Social Pedagogy and Education
Lucerne University of Applied Sciences and Arts
Lucerne, Switzerland
email: michael.doerk@hslu.ch

Ute Klotz
School of Computer Science and Information Technology
Lucerne University of Applied Sciences and Arts
Lucerne, Switzerland
email: ute.klotz@hslu.ch

***Abstract*—The data collection through digital applications in the evolving data economy is becoming an increasing risk for the users in terms of possible manipulation and misuse. Although users have obtained more rights (e.g, EU General Data Protection Regulation GDPR), there are doubts that users can actually exercise them. In parallel, the service providers' data collection becomes more ubiquitous and the tools for data analytics more powerful, which exacerbates the problem. The paper aims at identifying design targets for digital systems to better support users in this respect. The suggestions are based on the analysis of videos that three groups of workshop participants produced in a design fiction approach. The participants' goal was to anticipate the challenges of the data economy in 2037 and how they might be addressed. The aim of the study was to learn more about the perceptions and attitudes of the participants that they expressed in their videos. To this end, we analysed contradictions in the videos. These contradictions illustrate problems which the participants could not resolve. The analysis of the contradiction identifies targets for design of digital applications to better support users in the face of the challenges of the digital economy.**

***Index Terms*—privacy; data protection; contradictions; data economy.**

## I. Introduction

The economy becomes increasingly data-driven and affects how users interact with digital applications. Devices become personalised and more interactive. To achieve this, companies continuously and pervasively gather and analyse high volumes of personal data. In the VA-PEPR project [1], a multidisciplinary team of experts in design, human-computer interaction, digital service economy, and computer science investigates how the private use of voice assistants or smart home devices affects people's lives, routines and attitudes [2]. These omnipresent systems are typical examples of how data-collecting devices penetrate people's lives today.

Big tech companies, such as Google, Amazon, Facebook, Apple, Baidu, Alibaba, and Tencent, which provide these systems, gain control of an increasing amount of person-related data. In this way, they expand their influence, which unsettles users, who do not fully understand the underlying data flows; users only guess the possibilities behind data collection and analytics [4]. They have mixed feelings about the aggregation [2] and distrust the data-aggregating companies [3]. Although they regard the collection of personal data as a significant risk for their privacy, they rely on digital applications every day while they try to keep pace with the digital evolution. This results in a dilemma because people are forced to choose between the use of digital applications for their convenience and the protection of their privacy [5]. Moreover, in the course of the progressive exploitation of data for commercial and other purposes, users feel increasingly manipulated by Internet content and social media [6]. This increases their discomfort even more.

All this leads to a wide range of concerns in terms of ethics, economics, politics and other areas [7]. Likewise, it leads to phenomena, such as the so-called privacy paradox: people continuously use massively data-processing applications although they are concerned about the consequences—they just have no alternative [5]. In a previous study we conducted empirical investigations to examine the feelings and observations of people using digital applications, such as voice assistants in their homes [2]. The present study uses an indirect approach to users' perceptions and attitudes in the data economy. It rather resembles the image analysis with respect to people's understanding of privacy in [8]. However, we have used videos instead of images. Videos allow people to express their views in a creative way and express their attitudes and feelings, even those that are rather subliminal.

To this end, we held a Summer School, in which we asked the participating students to create videos on the challenge "Data protection and privacy in the use of virtual assistants in 2037" with regard to the individual, organisational/economic and legislative/societal levels, respectively. Each level was handled by a group of 6 students in separate workshops. The videos were then analysed for hidden contradictions. The aim was to identify issues for which the participants had not found

 ISBN: 978-1-68558-078-0 

a unambiguous solution. We see these issues in relation to design targets for digital systems that better respect users' privacy.

The paper is organised as follows. Section II describes related work (on topics like data economy, data-based manipulation, users' perceived vulnerability, privacy by design). In Section III, we explain the methodology that we have applied in setting up the workshops and analysing the results. In Section IV, we present the results. We conclude the paper with a discussion of the findings in Section V and derive recommendations.

## II. Related Work

There are several studies that have investigated the impact of the digital economy on users. They discuss and illustrate how users perceive the influence on their lives. This includes users' fear of losing control and manipulation.

**Data economy:** Allen states that the massive collection of data by big tech companies, such as Google, Amazon, Facebook, Apple, Baidu, Alibaba, and Tencent, presents major challenges to the users of digital applications in terms of control over personal information [9]. While initially the digitalisation was expected to bring empowerment and better lives to people, we can now observe a downside of digitalisation that challenges individual privacy and autonomy. Zuboff refers to the business model related to this as surveilance capitalism [4]. Users of digital applications do not really understand the privacy-related terms of service they agree to when they use digital applications [10]. The new world is not as bright as expected bringing forward issues in quality and reliability of data, ethics, privacy and other areas [11]. Investigations have shown that users are even willing to pay a fee to avoid the collection and commercial use of their data [12].

**Data-based manipulation:** After it became known that Cambridge Analytica used social networks, such as Facebook, to manipulate users by using their personal data for microtargeting [13], many users became aware of the threats related to such procedures. However, many see the danger more in the security of sensitive information (e.g., credit card numbers) than in the insidious collection of data and the building of user profiles that allow manipulation [14]. Users do not always realise that the transition between friendly persuasion and unfriendly manipulation is continuous [15].

**Perceived vulnerability of users in the data economy:** Users' vulnerability in the data economy has been identified as a sociotechnical problem that determines how people use systems and which choices they make [16]. It is the task of system designers to resolve users' concerns and give them more control [17]. Although the use of personal data is very common today, users and their needs are not sufficiently reflected in research and practices as studies have shown [18]. It has been argued that it is important to include users in the discourse about the evolution of the data economy [19] but this requires that we understand their situation and know what is at stake for them.

**Privacy by design:** The attempt to integrate privacy-preservation in the design and development of applications is known as *privacy by design* [20]. Although the principles of *privacy by design* are generally accepted, there are no clear guidelines on how to implement them [21]. It is the complexity of privacy, which causes problems for methods that realise *privacy by design* [22]. For this reason, the principles have mainly theoretical relevance [23].

## III. Methodology

After we had already obtained a picture of users' perception and attitudes regarding privacy from our home studies [2], this study investigated how users imagined alternatives to the current situation in terms of privacy. Since this required a more elaborate approach, we conducted this study with a smaller group of appropriately prepared students in a Summer School that took place at the end of August 2022. The participants consisted of 18 students of the University of Applied Sciences and Arts, Lucerne, who had different backgrounds and major subjects—see Table I. As preparation for the Summer School, the students had a preceding kick-off meeting with two instructors in May 2022, where they gained a first overview of the Summer School programme on "Creativity and Future Studies". It also included pointers to the overall challenge described "Data Capitalism, Data Colonialism and Possible Future Scenarios". The students were provided with the online toolbox *becreate*, which included the web-based training "create – Free thinking, creative stimulation and ground-breaking solutions" with an introduction to the topics *creativity*, *innovation management* and instruction for *(inter)connected media learning and projects* [24]. A guideline with detailed quality criteria and indicators was offered as additional orientation. This was to ensure that each group used a comparable approach. At the end of the kick-off meeting, three tasks were assigned to the students:

1) They were asked to research four publications relevant to the given challenge and upload the sources to an online platform. In addition, they were asked to explain why they regarded the publications to be relevant.
2) They were asked to study the web-based training.
3) They were asked to produce a short video, in which they talked about their competences in the areas of creativity, innovation management and media competence and about their motivation.

Finally, the instructors assembled the teams for the different workshops in a way that ensured the best possible interdisciplinary mix and the participation of at least one person with strong media skills in each team.

The instructors also used the kick-off meeting to obtain the students' verbal consent for the use of videos, collected literature (including explanations) and other results in the VAPEPR project. The Summer School was not compulsory for the students and their participation was voluntary. To make the results available to the project, they were stored on a research platform and password-protected. The students were informed that the results of the analysis would be anonymised and then

 ISBN: 978-1-68558-078-0 

used in the research project; the provision of data to the project was voluntary. Shortly before the start of Summer School, the students were asked again whether the videos and other work results could be used for research purposes; the access to the work results on the Internet or other generally accessible media was excluded.

The provision of the workshop results was not remunerated, however, as a special appreciation, the students were invited to an optional networking event at the end of the Summer School, where they had the opportunity to exchange experiences among each other and with the instructors as well as the accompanying researchers of the VA-PEPR project.

TABLE I. DATA PROTECTION AND PRIVACY—INDIVIDUAL LEVEL.

| Group | Major Subject | Gender |
|---|---|---|
| 1 | real estate | male |
| 1 | socio-cultural studies | female |
| 1 | value network management | female |
| 1 | mechanical engineering | male |
| 1 | social pedagogy | female |
| 1 | spatial design | female |
| 2 | real estate | female |
| 2 | communication | female |
| 2 | management and law | female |
| 2 | architecture | male |
| 2 | market and consumer psychology | male |
| 2 | social work | female |
| 3 | real estate | male |
| 3 | real estate | male |
| 3 | socio-cultural studies | female |
| 3 | architecture | male |
| 3 | finance and banking | male |
| 3 | marketing | female |

During the week of the Summer School students were asked to explore and answer the following questions related to the future of the data economy:

- What opportunities as well as dangers or problems will the data economy in 2037 be associated with?
- How can the challenges related to privacy and data protection in 2037 be addressed?

The latter question was split into three levels (individual, organisational/economic, legislative/societal) and assigned to one group each.

At the end of the week, each group should have produced a video as a result of the creative and discursive process as well as the documentation of the process that led to this result. The documentation should also include possible side paths or discussion threads that they had decided not to pursue.

The **video analysis** was conducted for each of the three videos in an iterative approach [25]. One researcher (R1 in Table II) described the individual scenes of each video one by one. The results were tabulated (timestamp, description) and can be found in Tables III-V. The interpretation team (R2-R4 in Table II) elaborated the core message in each scene and identified contradictions in these messages. According to [26], whole-media (audio and video) analysis results in higher accuracy, a denser description and reveals more informative reports than analysing the transcripts only. According to [27], the researchers of the interpretation team looked at core images of the scene, interpreting the content from their personal background and experience. Each researcher in the interpretation team looked for contradictions, which were then discussed and interpreted in the team. Only those contradictions that the team agreed on were included. Due to the small number of videos and the clear recognizability of the contradictions, intercoder reliability was not applied [28].

TABLE II. RESEARCHERS IN THE INTERPRETATION TEAM.

| No. | Research Focus | Gender | Education |
|---|---|---|---|
| R1 | Future of Work,<br>Information Technology | female | Political Economics<br>Information Science |
| R2 | Digital Business<br>Knowledge Management | male | Mathematics<br>Computer Science |
| R3 | Digital Health | female | Anthropology |
| R4 | Social Work<br>Digital health | male | Psychology |

In analysing the videos, we adopted an approach in which we considered the respective future scenarios as narratives in the sense of **design fiction** [29]. This was in line with the briefing, where participants were instructed to identify a problem in the specified areas and create a video with a fictitious content that described an approach to solve current and future data protection problems [30]. Each video can be understood as a narrative of how the participants envisioned the future protection of data and privacy. Narratives reflect people's perceptions and attitudes. Moreover, they can serve as boundary objects between people with different knowledge and backgrounds [31], a factor that was relevant beacuse of the interdisciplinary teams. According to [32], narratives are most valuable if they reveal gaps and contradictions. Such contradictions point to issues that the storyteller obviously cannot easily resolve. The advantage of a narrative is that it is cognitively processed in a different way than non-fiction. Thus, the producers and consumers of narratives are more open to accept multiple meanings and possibilities, ambiguity and contradictions [33]. Similarly, the workshop participants built their contradictions (unconsciously) into their videos, as there was no obvious solution for them. Studies of contradictions have a longstanding tradition in human-computer interaction, mainly related to activity theory [34]. They have been considered a suitable tool to carve out problematic user situations [35] and serve as a source of inspiration for the development of new ideas [36].

In a final step, we conducted an **analysis of contradictions** in the videos—as indicators for antagonistic forces that are inherent in the setting and cannot be easily resolved. We looked for deeper-seated challenges that could explain why the contradictions could not be resolved. In addition, we expanded the scope of these challenges and found several dimensions that helped us to structure the results systematically.

## IV. RESULTS

In the following, we present short descriptions of the three videos and the results of the subsequent analysis.

**Video 1 - Individual Level** (length 9 min.): The 2037 scenario assumes that all personal data, such as health or

financial data, will be deposited in a personal data wallet of a newly created Federal Department of Property. The fundamental problem identified in the video's future scenario is that every data repository can be hacked, today and in the future. This is in line with the conventional wisdom in the field of IT security that attacks happen wherever a security gap opens up. The proposed solution in the scenario is simple and complex at the same time: an avatar—a digital twin of the real person—is supposed to anticipate threats to personal data and defend the user against them. It is based on artificial intelligence, which makes the avatar powerful enough to protect the user's data wallet, while also making it intelligent enough to understand the users' requirements. Cf. to Table III for scene descriptions.

TABLE III. DATA PROTECTION AND PRIVACY—INDIVIDUAL LEVEL.

| **Scenes of Group 1's Video** |
|---|
| **Time Stamp 00.50-01.05**<br>In the future scenario, data ownership is handled the same way online and offline. |
| **Time Stemp 01.12-01.42**<br>A persona logs into the personal wallet using Face ID or biometric data. Personal data (e.g., health, insurance, financial data) are stored in a wallet at the Federal Department. |
| **Time Stamp 01.43-01.59**<br>The account is hacked: It is explained that even in 2037 not everything works without problems. |
| **Time Stamp 03.10-03.33**<br>The personal problems related to data are mentioned: Addiction and social media, plus the unresolved legal situation and capitalism. |
| **Time Stamp 04.30-05.13**<br>For the future scenario "ownership and property", an IT expert is interviewed: he sees the same problems as today also in 2037, i.e., passwords are revealed or databases are hacked. |
| **Time Stamp 05.18-05.40**<br>An IT expert: Security measures must be further developed, especially encryption procedures. Quantum computers bring new uncertainty.In addition, users should always remain up to date with the latest technology due to the constant development of the digital world. |
| **Time Stamp 06.16-06.43**<br>A well-known scientist is quoted warning against quantum computers. However, such computers do not yet exist. |
| **Time Stamp 06.46-07.30**<br>Blockchain technology plays a crucial role in protection, which is constantly being further developed by researchers. |
| **Time Stamp 08.04-08.44**<br>Two solutions to close security gaps in the future are proposed: (1) use of multi-factor authentication and (2) more education, T&Cs should become more user-friendly. |
| **Time Stamp 08.46-09.15**<br>An avatar (AI) is introduced (as clone of the real person) that prevents the hacking of the user's data. |

In the video of Group 1 (Table III), we find the following contradictions: (1) "Central repository, data must be controlled by the state" (Time Stamp 01.12-01.42) *vs.* "Distributed repositories, data must not be controlled by a single institution" (blockchain) (Time Stamp 06.46-07.30), (2) "Technology is a threat to the user" (quantum computing) (Time Stamp 06.16-06.43) *vs.* "Technology is a friend of the user" (avatars) (Time Stamp 08.46-09.15). If we look at these contradictions in more detail, we find in (1) the problem of protecting data, which is not a question of where the repository is located; a state-owned repository can be hacked in the same way as a private one. The critical point behind the contradiction is the confidence in the security and transparency of the storage. In the case of the state-owned repository users simply transfer their security problem to an authority. In the case of blockchain, it is the dispersion of data that ensures security because the data are everywhere and nowhere. The points that are important for users are that they **know that their data are secure and protected by an institution that is more powerful than themselves**. This is also closely related to contradiction (2), which reflects the users' attitude towards technology. On the one hand, users are aware that digital technology is required to protect data. On the other hand, they see new technology as a threat to the security of their data. It is not about *good* and *bad* technology but the *same* technology can be used in both ways. The insight is that **we need technology to cope with the dangers of technology**. However, users need support to keep up in the race for safety excellence.

**Video 2 - Organisational Level** (length 12.5 min.): The future scenario in this video starts with a job interview, in which the recruiter has access to personal information about the female applicant gleaned from social media during the interview (e.g. her wish to have children or her political opinion). On the basis of the provided data, she is rejected. Discrimination against the applicant is the central theme of the video. It seems that the students identify themselves with the female victim: they declare the issue of discrimination to be a major future problem, which is also associated with the digital divide in society. Although an explicit expression of trust or distrust in data capitalism or technology is not mentioned, people realise that they have to deal with it in some way. The proposed solution is a virtual assistant that suggests with whom to share data or which personal data should be deleted. It remains unclear who runs the data platform, the state or private companies. Further scenes show how the virtual assistant makes recommendations. For example, the woman should not eat chocolate because she is pregnant, she should not smoke because that might make her health insurance premiums rise, she should not drink beer because that might deteriorate her social ranking. It looks like she accepts the advice unconditionally and uncritically. The conclusion is that the individual must decide to be *socially* compliant or non-compliant. Cf. to Table IV for scene descriptions.

In the video of Group 2 (Table IV), we see the following contradictions: (1) "Use of personal data is in users' interest" (Time Stamp 03.09-03.24) *vs.* "Use of personal data is in the interest of companies" (health insurance) (Time Stamp 02.48-02.58), (2) "Users can control data-based discrimination" (deleting personal data) (Time Stamp Time Stamp 12.25-12.38) *vs.* "Users become victims of data-based discrimination" (training bias in data that are not their own) (Time Stamp 04.06-05.14). The contradiction (1) is related to the purposes for which person-related data are used. Intelligent assistants can either recommend suitable solutions to users' problems based on their available profiles or they serve other parties' interests to the harm of the users. In connection with the problem of trust in intelligent assistants, there is the additional

 ISBN: 978-1-68558-078-0 

TABLE IV. DATA PROTECTION AND PRIVACY—ORGANISATIONAL LEVEL.

| Scenes of Group 2's Video |
|---|
| **Time Stamp 01.50-02.04**<br>The future scenario starts with a job interview in which the interviewer uses personal background information about the applicant (e.g. desire to have children, political orientation), which leads to a rejection. |
| **Time Stamp 02.34-02.48**<br>The same person wants to buy chocolate and asks her voice assistant for the nearest kiosk. The voice assistant answers that the protagonist should not eat chocolate because she is pregnant. |
| **Time Stamp 02.48-02.58**<br>The question whether one should rather smoke instead of chocolate is answered in the negative. The reason given is health and possible increases in health insurance premiums. |
| **Time Stamp 02.59-03.08**<br>When asking for a beer, the assistant points out the negative effects in the social ranking. |
| **Time Stamp 03.09-03.24**<br>The request for a holiday with the order to book a flight to Hawaii is refused because the account balance is too low. |
| **Time Stamp 03.24-03.35**<br>It is noted that this is an aspect of discrimination. |
| **Time Stamp 03.36-04.05**<br>In further analysis, further future scenarios are developed with the result that discrimination will be a major problem in 2023. |
| **Time Stamp 04.06-05.14**<br>Examples of discrimination through digitalisation are listed. This affects women in application processes, as the algorithm tries to match the company and the applicant, while the training data contain a bias. |
| **Time Stamp 07.00-09.47**<br>In three interviews, the interviewees are asked about the dangers and opportunities of data mining by large companies. |
| **Time Stamp 09.48-11.52**<br>Possible solutions for 2037: a label to guarantee privacy, people themselves determining the algorithms, educational offers in terms of prevention, research projects in the field of data protection, customers who can control access to their data at any time. |
| **Time Stamp 11.59-12.23**<br>Discrimination in the job interview can be prevented by avoided by a deliberate decision which data are shared. |
| **Time Stamp 12.25-12.38**<br>A personal intelligent voice assistent gets the order to delete certain personal data. |

question of the extent to which users should bow to the supposedly *optimal* advice of intelligent assistants. Users may feel they have to bow to the applications, mostly overlooking the limitations of such technologies. This raises the question of **privacy in relation to intelligent applications**. It raises the question to which extent we transfer responsibilities to technical applications. The contradiction (2) reflects the desire to influence the impact of data use, while at the same time it is clear that such data use must be transparent to be controllable—users can hardly control a bias in training data. The central theme behind this contradiction is the wish to **understand and control the use of data in digital applications**. Such control requires transparency and explainability, which has already been identified as a key research topic in artificial intelligence research [37].

**Video 3 - Societal Level** (length 15 min.): The future scenario describes a social principle of "digital first" or "digital only", i.e., you must be online or you are excluded from society. The question is raised whether social life can or should only take place online. Social media play a central role in society, but they are organised in a decentralised way in the sense of communities (not in the sense of big tech). It is also difficult to distinguish between true and untrue information. Various solutions for dealing with misinformation are proposed. One is that users categorise posts as fact, opinion or scientifically verified statement. Other solutions include a traffic light system based on a central assessment and a point system which involves sanctions for misbehaviour by spreading misinformation. Two people from two opposing political parties are asked about the problem: one person wants a solution controlled by the state, while the other person wants as little state influence as possible and insists on freedom of expression. Finally, the importance of this issue for democracy is highlighted. Cf. to Table V for scene descriptions.

In the video of Group 3 (Table V), we see the following contradictions: (1) "Credibility criteria for information are objective" (Time Stamp 08.30-10.00) *vs.* "Credibility criteria for information are subjective" (Time Stamp 08.30-10.00), (2) "Information shared in social media is democratic" (liberal view) (Time Stamp 03.52-05.16) *vs.* "Information shared in social media in manipulative" (Time Stamp 06.40-08.10). Regarding contradiction (1), the solution to the problem of fake news proposed by the students primarily suggests that there is a clear distinction between objective *truths* and subjective *opinions*. At the same time, this categorization is conducted by individual users and is therefore subjective, which raises the question of clear criteria for such a categorization. More likely, it is a social issue rather than one that can be based on technical means or individual opinion. Thus, we need **social processes to ensure the trustworthiness of content**. We must learn how to establish such processes. Contradiction (2), on the one hand, refers to the fact that anyone can contribute to social media, while, on the other hand, it is becoming increasingly apparent that such possibilities open the doors for various kinds of manipulation (example: filter bubble). The problem is similar to the one in contradiction (1), but its focus is rather on the mechanisms in social media than on the assessment of content quality. Some social media groups are more like conspiracy circles than fora for public discourse. This raises the question whether such groups increase or weaken users' autonomy as responsible members of the society. It must be ensured that there are mechanisms that **enhance users' autonomy**, for example, by resolving information fragmentation and support open exchange since openness appears to be an essential precondition for better user control.

## V. DISCUSSION

The videos describe issues that the students perceive as most urgent today or expect to become critical challenges in 2037. The students have dealt extensively with the subject matter in their preparation, so that we do not assume that the occurring contradictions were merely inaccuracies. Instead, we assume more fundamental issues behind these contradictions. That this assumption is not unfounded is illustrated by the so-called privacy paradox; it describes that people express concerns about the violation of their privacy by big digital

 ISBN: 978-1-68558-078-0 

TABLE V. DATA PROTECTION AND PRIVACY—SOCIETAL LEVEL.

| **Scenes of Group 3's Video** |
|---|
| **Time Stamp 0.08-01.06**<br>Scenario in the year 2037: A reporter wants to interview randomly selected people on the above topic. The person interviewed (a group member) answers reluctantly. The person expresses that he or she distrusts the truthfulness of the news and has difficulties understanding topics, that classic media (e.g. books) are no longer used. |
| **Time Stamp 01.12-01.33**<br>Description of a utopian vision of the future in which life takes place only in digital space. |
| **Time Stamp 01.51-02.14**<br>The task and, in part, the methodological procedure are explained. |
| **Time Stamp 02.30-02.50**<br>Five thematic areas are defined: (1) Addiction/Internet, (2) Invasion of privacy/sensitive data, (3) Misinformation/Consumption,<br>(4) Influence/economy (advertising), (5) Misinformation/State/Politics, from which the topic misinformation is selected. |
| **Time Stamp 02.51-02.58**<br>Question: How can society curb misinformation on social media? |
| **Time Stamp 03.25-03.50**<br>Future scenario in 2037: reality<br>and the internet are merging more and more, you can't escape it. You can no longer be offline. Social media are increasingly dominated by communities, it is no longer clear what is true or false. |
| **Time Stamp 03.52-05.16**<br>Interview with two male politicians on the subject of misinformation in 2037: (1) older politician: the state must bear responsibility. (for what remains unclear); (2) younger politician: liberal thoughts are important. Filters mean a bit of censorship. Providers should set as few filters as possible. |
| **Time Stamp 05.30-06.20**<br>Future scenario 2037: The blending of internet and reality leads to social division; certain interest groups turn away from others; money is replaced by collected data; data in social media feeds rating system; social media become more and more personalised. |
| **Time Stamp 06.40-08.10**<br>Five main problems in future scenarios: (1) Power shift to social media and loss of control over the distribution of information; (2) Dependence on social media and more and more time spent using social media and electronic devices (danger of filter bubbles); (3) Societal change through digitalisation depends on more and more population groups; (4) Division of society through digitalisation; (5) Misinformation that can no longer be controlled. Misinformation is seen as the biggest problem. |
| **Time Stamp 08.30-10.00**<br>Approaches to the issue of social media and misinformation:<br>(1) Self-tagging of social media posts: This distinguishes fact, opinion and scientifically verified statement; (2) Traffic light system distinguishes the truth content of posts; (3) Point system after repeated publication of fake news blocks the responsible persons; (4) The state punishes misinformation more severely (deterrence). |
| **Time Stamp 10.02-10.55**<br>Interviews on possible solution: very time-consuming (time, staff); traffic light system is a good idea, clearly visible. |
| **Time Stamp 11.02-13.00**<br>Conclusion: Relation to democracy is important Main finding: Flexibility/adaptability is required, new inventions, one has to be open as a human being so that society can move forward. Cooperation between organisations is important. |
| **Time Stamp 13.00-14.00**<br>Retrospective: View to 2027 is limited, we have to look further ahead. |
| **Time Stamp 14.00-14.53**<br>Supplementary information. |

service providers but don't show a corresponding reaction in their behaviour [38]. Group 1's contradiction (2) is related to it. In the analysis of the paradox, Solove explained that users practically have no other choice than to surrender to circumstances that are perceived as a threat to their privacy [5]. This is one example of how contradictions can point to broader problems.

In order to check the generalisability of the results we compared them to results of previous studies that we had conducted with another group of users, who were more diverse (e.g., between the ages of 17 and over 70, lower as well as higher affinity to technology)—for more details refer to [2]. In this study, we identified the following connections (The numbering of contradictions follows Table VI):

**C1.1:** Ambivalence towards data retention and the role of the state corresponds to recent studies that found that the Swiss population tends to trust their government (due to their effort in the COVID-19 crisis) [39]. On the other hand, there is a fundamental distrust in general particularly in terms of surveillance [40]. Both views were also reflected in our studies of attitudes towards voice assistants.

**C1.2:** The ambiguous attitudes towards the dangers of digital technology as friend or foe correspond to our previous studies of voice assistants. Some people had developed an almost personal relationship to their voice assistant whereas others remained suspicious of them—some even stopped using them at all. Since users did not consider these voice assistants as essential for their daily life stopping the use was easy. This does not apply to more important digital applications, where the conflict persists.

**C2.2:** The conflict regarding control also appeared in the use of voice assistants, where some users switched them off if they wanted to make sure that their utterances remain private. Some participants completely banned voice assistants from certain rooms, e.g., bedroom or bathroom. Apart from switching off the device they were never completely sure what happened to their conversations, that is, they did not have the feeling to control the use of their data.

TABLE VI. CONTRADICTIONS IN THE VIDEOS.

| |
|---|
| **C1.1:** "Central storage, data must be controlled by the state" *vs.* "Distributed storage, data must not be controlled by a single institution"<br>**C1.2:** "Technology is a threat to the user (quantum computing)" *vs.* "Technology is a friend of the user" |
| **C2.1:** "Use of personal data is in users' interest" *vs.* "Use of personal data in in the interest of companies"<br>**C2.2:** "Users can control data-based discrimination" *vs.* "Users become victims of data-based discrimination " |
| **C3.1:** "Credibility criteria for information are objective" *vs.* "Credibility criteria for information are subjective"<br>**C3.2:** "Information sharing in social media is democratic" *vs.* "Information sharing in social media in manipulative" |

Connections to other contradictions were less obvious, which was generally due to the limited intelligence and performance of current voice assistants. For example, participants did not think that the assistants would harm their autonomy due to manipulation, although they recorded enough data to produce a very detailed personal profile. Equal access to

 ISBN: 978-1-68558-078-0

information was no problem either since most information sources on voice assistants were free. Similarly, the content was not regarded as a problem since a considerable part of the information provided came from Wikipedia or other well-known sources. However, we can imagine these three aspects might become problematic once voice assistants are misused by parties with a polarising agenda and content of unclear origin or if users only get high-value information if they pay for it.

The value of contradictions for design is that they provide insights into users' attitudes towards data-related issues. The contradictions in the proposed solutions reveal deeper-seated problems. It is important for the design of effective solutions that these are taken into account.

To provide better insight in the design targets that might tackle the problems we have derived general challenges from the contradictions und categorized them in various dimensions. One dimension refers to the different manifestations of information (as thing, as knowledge, as process) according to Buckland [41]—according to [42], we regard the knowledge dimension to be related to the application of information. The second dimension refers to the distinction between primarily individual or social concern. The results are compiled in Table VII. Moreover, we have included examples of design targets that address the challenges in the design of applications that use personal data.

TABLE VII. CATEGORISATION OF CHALLENGES

| | **Information-as-thing** | |
|---|---|---|
| | ***Individual*** | ***Social*** |
| ***Challenge*** | data ownership | equal access to technology |
| ***Design Target*** | user sovereignty over their data | infrastructure supporting technology updates |
| | **Information-as-knowledge** | |
| | ***Individual*** | ***Social*** |
| ***Challenge*** | control over data use | avoidance of discrimination |
| ***Design Target***t | transparency regarding data use | evidence of unbiased data |
| | **Information-as-process** | |
| | ***Individual*** | ***Social*** |
| ***Challenge*** | information reliability | information autonomy |
| ***Design Target*** | systematic reliability checks | control of ethical information usage |

Finally, we regard the suggested design targets in more detail to illustrate how the challenges might be addressed:

- **"User sovereignty over their data"**: Currently, the business models of most digital service providers take user data in exchange for their digital services. Thess business models are increasingly being distrusted due to privacy concerns [43]. The measures that have been suggested so far put the burden on the users, who on the whole cannot cope with it, e.g., GDPR [44]. The only effective measure seems to be that users retain full control over their data. For example, data trustee solutions have been suggested to supported users in protecting their data [45]. System designers should take the role of data trustees in digital applications into account.
- **"Infrastructure supporting technology security updates"**: Users cannot keep pace with the developments in cyber security, which appears to be a technological race between defenders and attackers of cyber security. Therefore, users need a system infrastructure that automatically installs all relevant system updates. Partially, systems already provide automatic updates but automatic technology updates should become mandatory and part of the infrastructure.
- **"Transparency regarding data use"**: Use of person-related data is necessary to individualise digital services, e.g., for recommendations. Users have to understand what this individualisation means and what their data are used for. System designers should take care of such transparency.
- **"Evidence of unbiased data"**: Bias in data-trained machine learning applications is well known, e.g., [47]. Measures have been suggested to avoid bias [48]. Data used to train algorithms should be checked for known biases and certified accordingly if necessary.
- **"Systematic reliability checks"**: To which degree information is trustworthy is often difficult to decide because even correct and validated information can be misleading if it is used in the wrong context. Designers must provide each user the opportunity to contribute to such checks and make the sources of information transparent. Systematic checking means that a procedure must be set in operation that ensures a high probability of detecting content of low quality.
- **"Control of ethical informational usage"**: Subliminal manipulation of users by data-based applications depends on the depth of available user profiles and the quality of algorithms. Protecting user data is already a decisive step for preventing manipulation but cannot prevent manipulation completely [14]. Protection also requires checks of the purposes, for which algorithms were trained. System designers should support users in conducting such checks. The purpose of data use should be made as transparent as possible.

The contradictions that we have identified reflect the participants' perceptions and attitudes with respect to their data and privacy protection requirements. The respective narratives helped them to express their views in a less restrictive way that show the tensions they experience. Thus, we were able to expand the insights we had gained in the earlier in-home studies. Nevertheless, further investigations of the multifaceted challenges are required. It is obvious that individual users cannot deal with these challenges on their own but need qualified institutions and suitable infrastructures that support them. The current study only had the aim to point at a first set of the existing issues of data-based applications. They are likely to represent a small spectrum of possible issues resulting from other scenarios. However, they already give an impression of the effort that is required to reconcile users' privacy interests and economic demands in the future.

 ISBN: 978-1-68558-078-0 

## ACKNOWLEDGMENT

This study was funded by the Swiss National Science Foundation (SNF) project VA-PEPR, ref. no. CRSII5_189955.

## REFERENCES

[1] "VA-PEPR - How do we live in the omnipresence of voice assistants?" https://sites.hslu.ch/va-pepr/en/ [retrieved: March, 2023]

[2] E. Maier, M. Doerk, M. Muri, U. Reimer, and U. V. Riss, "What does privacy mean to users of voice assistants in their homes?" Proceedings of the ETHICOMP, pp. 300–314, 2022.

[3] B. Dembrow, "Investing in human futures: How big tech and social media giants abuse privacy and manipulate consumerism," University of Miami Business Law, vol. 30, no. 3, pp. 324–349, 2021.

[4] S. Zuboff, The age of surveillance capitalism. London, UK: Profile books Ltd, 2019.

[5] D. J. Solove, "The myth of the privacy paradox," George Washington Law Review, vol. 89, no.1, pp. 1-–51, 2021.

[6] N. Andalibi and J. Buss, "The human in emotion recognition on social media," Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–16, 2020.

[7] F. Lauf et al., "Linking data sovereignty and data economy," Wirtschaftsinformatik 2022 Proceedings, 19, 2022.

[8] M. Oates, Y. Ahmadullah, A. Marsh, C. Swoopes, S. Zhang, R. Balebako, and L. F. Cranor, "Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration," Proceedings on Privacy Enhancing Technologies, pp. 5–32, 2018.

[9] A. L. Allen, "Protecting one's own privacy in a big data economy," Harvard Law Review Forum, vol. 130, pp. 71–78, 2016.

[10] C. L. White and Boatwright, "Social media ethics in the data economy," Public Relations Review, vol. 46, no. 5, Article 101980, 2020.

[11] K. Löfgren and C. W. R. Webster, "The value of big data in government," Big Data & Society, vol. 7, no. 1, 2020.

[12] S. A. Elvy, "Paying for privacy and the personal data economy," Columbia Law Review, vol. 117, no. 6, pp. 1369–1459, 2017.

[13] K. Ward, "Social networks, the 2016 US presidential election, and Kantian ethics," Journal of media ethics, vol. 33, no. 3, pp.133–148, 2018.

[14] U. V. Riss, E. Maier, and M. Doerk, "Perceived risks of the data economy," Proceedings of the ETHICOMP, pp. 413–427, 2022.

[15] K. Vold and J. Whittlestone, "Privacy, autonomy, and personalised targeting," in Report on Data, Privacy, and the Individual in the Digital Age, by IE University's Center for the Governance of Change, Madrid, Spain: IE University, 2019.

[16] M. W. Skirpan, T. Yeh, and C. Fiesler, "What's at stake: Characterizing risk perceptions of emerging technologies," Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–12, 2018.

[17] A. Adams and M. Angela Sasse, "Privacy in multimedia communications," in People and computers XV—Interaction without frontiers. London, UK: Springer, pp. 49–64, 2001.

[18] M. M. Rantanen and J. Koskinen, "Humans of the European data economy ecosystem-what do they demand from a fair data economy?" Proceedings of IFIP International Conference on Human Choice and Computers. Springer, Cham, pp. 327–339, 2022.

[19] S. Knaapi-Junnila, M. M. Rantanen and J. Koskinen, "Are you talking to me?" Information Technology & People, vol. 35, no. 8, pp. 292–310, 2022.

[20] A. Cavoukian and J. Jonas, "Privacy by design in the age of big data," 2012. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf [retrieved: March, 2023]

[21] M. Colesky, J. H. Hoepman, and C. Hillen, "A critical analysis of privacy design strategies," Proceedings of IEEE security and privacy workshops (SPW), pp. 33–40, 2016.

[22] M. Alshammari and A. Simpson, "Towards a principled approach for engineering privacy by design," Privacy Technologies and Policy: 5th Annual Privacy Forum, APF 2017, Revised Selected Paper, pp. 161–177, 2017.

[23] S. Barth, D. Ionita, and P. Harte, "Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines," ACM Computing Surveys (CSUR), vol. 55, no. 3, pp. 1–37, 2022.

[24] M. Doerk and W. Zenker, "(Inter)connected media-learning," in Problembasiertes Lernen, Projektorientierung, forschendes Lernen & beyond, J. Weißenböck, W. Gruber, C. F. Freisleben-Teutscher and J. Haag, Eds., pp. 127–139, 2018.

[25] H. Knoblauch, R. Tuma, and B. Schnettler, "Video analysis and videography," in The Sage Handbook of Qualitative Data Analysis, U. Flick, Ed., pp. 2—24, 2018.

[26] D. T. Markle, R. E. West, and P. J. Rich, " Beyond transcription: Technology, change, and refinement of method," in Qualitative Social Research, Vol. 12, No. 3, Article 21, 2011.

[27] G. Rose, Visual methodologies: An introduction to researching with visual materials. London, UK: SAGE.

[28] A. Nili, M. Tate, and A. Barros, "A Critical Analysis of Inter-Coder Reliability Methods in Information Systems Research," Proceedings of ACIS, no. 99, 2017.

[29] B. Sterling, "Cover story design fiction," interactions, vol. 16, no. 3, pp. 20–24, 2009.

[30] P. Coulton and J. G. Lindley, "More-than human centred design: Considering other things," The Design Journal, vol. 22, no.4, pp. 463–481, 2019.

[31] R. J. Boland Jr and R. V. Tenkasi, "Perspective making and perspective taking in communities of knowing," Organization Science, vol. 6, no.4, pp. 350–372, 1995.

[32] C. Booth, M. Rowlinson, P. Clark, A. Delahaye, and S. Procte, "Scenarios and counterfactuals as modal narratives," Futures, vol. 41, no. 2, pp. 87–95, 2009.

[33] G. Lively, "Narrative: Telling social futures," Routledge Handbook of Social Futures, London, UK: Routledge, pp. 224-232, 2021.

[34] Y. Engeström, Learning by expanding. Cambridge, UK: Cambridge University Press.

[35] S. Bødker and C. N. Klokmose, "The human–artifact model: An activity theoretical approach to artifact ecologies," Human–Computer Interaction, vol. 26, no. 4, pp. 315–371, 2011.

[36] P. Mogensen, "Towards a provotyping approach in systems development," Journal of Information Systems, vol. 4, no. 1, pp. 31–53, 1992.

[37] W. Brunotte, A. Specht, L. Chazette, and K. Schneider, "Privacy explanations–a means to end-user trust," Journal of Systems and Software, vol. 195, Article 111545, 2023.

[38] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," Journal of consumer affairs, vol. 41, no. 1, pp. 100–126, 2007.

[39] Y. Willi, G. Nischik, D. Braunschweiger, and M. Pütz, "Responding to the COVID-19 crisis," Tijdschrift voor economische en sociale geografie, vol. 111, no. 3, pp. 302–317, 2020.

[40] L. A. Viola and P. Laidler. Trust and Transparency in an Age of Surveillance. London, UK and New York, NY: Routledge, 2021.

[41] M. A. Buckland, "Information as thing," Journal of the American Society for Information Science, vol. 42, no. 5, pp. 351–360, 1991.

[42] D. J. Saab and U. V. Riss, "Information as ontologization," Journal of the American Society for Information Science and Technology, vol. 62, no. 11, pp. 2236–2246, 2011.

[43] N. Couldry and U. A. Mejias. "Data colonialism: Rethinking big data's relation to the contemporary subject," Television & New Media, vol. 20, no. 4, pp. 336–349, 2019.

[44] I. van Ooijen and H. U. Vrabec, "Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective," Journal of consumer policy, vol. 42, pp. 91–107, 2019.

[45] W. Kerber. " From (horizontal and sectoral) data access solutions towards data governance systems," SSRN Electronic Journal, 2020.

[46] R. Buch, D. Ganda, P. Kalola, and N. Borad, "World of cyber security and cybercrime," Recent Trends in Programming Languages, vol. 4, no. 2, pp. 18-–23, 2017.

[47] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A survey on bias and fairness in machine learning," ACM Computing Surveys (CSUR), vol. 54, no. 6, pp. 1–35, 2012.

[48] C. DeBrusk, "The risk of machine-learning bias (and how to prevent it)," MIT Sloan Management Review, 2018. https://sloanreview.mit.edu/article/the-risk-of-machine-learning-bias-and-how-to-prevent-it [retrieved: March, 2023]