# D1.14 NGI research topic analysis II

| | |
|---|---|
| **Work package** | **WP1: Topic Identification** |
| **Task** | **1.7 NGI Topics Filtering & deep dives** |
| **Due date** | **30/04/2021** |
| **Submission date** | **30/04/2021** |
| **Deliverable lead** | **DATALAB, Aarhus University** |
| **Dissemination level** | **Public** |
| **Nature** | **Report** |
| **Authors** | **Mathias Holm Sørensen, Ida Anthonj Nissen, Anja Bechmann** |
| **Version** | **1** |
| **Reviewers** | **Katja Bego, Kristóf Gyódi, Markus Droemann, Alberto Cottica** |
| **Status** | **Final** |



**Acknowledgement**: This Report is part of a project that has received funding from the **European Union's Horizon 2020 research and innovation programme under grant agreement N°825652**

**1.0 Introduction** **3**

1.1 Purpose & scope 3

**2.0 Methodology** **4**

2.1 Venue 4

2.2 Participants, survey & quizzes 4

2.3 Structure 6

**3.0 Challenges and policy solutions** **8**

3.1 Lacking or unstable Internet access 8

3.2 Discriminatory algorithmic decision-making 9

3.3 Facial Recognition and Surveillance 10

3.4 Implementing technology without proper deliberation and transparency 12

3.5 Internet shutdowns 13

3.6 Discrimination and hate speech 15

3.7 Risk of data leaks 17

3.8 Challenges and policy solutions — Overview 18

**4.0 Prioritization and grouping of the challenges** **20**

**5.0 Conclusions and next steps** **26**

**6.0 Literature** **27**

**Annex 1: Survey responses** **32**

**Annex 2: Quiz 1 & 2 questions and responses** **36**

Quiz 1 36

Quiz 2 43

# 1.0 Introduction

In recent years we have seen many examples of the ways in which internet-related technologies can impact our lives — often in ways which do adhere with our principles of democracy and the idea of the internet being a tool to improve people's lives. These examples include, but are not limited to, censorship, discrimination, Internet shut downs and data-driven decision making.

The Internet has shifted from being a luxury for the few to a necessity for the masses in order to realize democratic values and human rights (Reglitz, 2019). In concurrence with a larger interconnectedness between the Internet and everyday life, questions of human rights and democratic values in our digital life shoots to the forefront of both the discussions of legislators and researchers. The question of how to secure and expand the Universal Declaration of Human Rights (The United Nations, 1948) to fit this new reality becomes increasingly important.

In 2016, the United Nations adopted a goal of promoting and protecting Human Rights on the Internet, but the question of whether Human Rights offline naturally apply to online ones is a present one (Reglitz, 2019). To better identify the nature of the challenges on the Internet as well as their potential policy solutions, interdisciplinary collaboration between experts is needed.

This deliverable describes a workshop held as part of the annual Association of Internet Researchers (AoIR) conference, which is the largest conference purely focused on Internet research. The workshop had as its purpose to derive qualitative input on the negative effects Internet-related technology can have on our lives and society, and what potential policy solutions researchers within the field see that could address these challenges.

## 1.1 Purpose & scope

In this deliverable, we will report on the findings from the second of three expert workshops conducted by Aarhus University as part of Work Package 1: Topic identification in the NGI Forward project. The aim of the three workshops is to bring new insights into how to support a more human-centric course for the Internet. The methodology and outcomes from this first workshop can be found in *D1.13 Value-driven future Internet: A social science perspective I* (Møller & Bechmann, 2020). The qualitative results derived from the first workshop was along with quantitative data from D1.2: Visualizations of key emerging technologies and

social issues (Gyódi et al., 2019) used in the first formal selection of first eight key NGI topics, as described in D1.9: NGI Topic guides and evaluation report I (Møller et al., 2020).

The purpose of the second workshop was to identify and discuss potential challenges and policy solutions through a more case-specific point of departure than the first workshop to gain more specific and actionable output. The workshop centered around questions of how to secure a future Internet more in line with the principles of democracy — such as but not limited to upward control, political equality and majority rule (Kimber, 1989; Dahl, 1989) and the human-centered values such as Universal Declaration of Human Rights (The United Nations, 1948).

# 2.0 Methodology

## 2.1 Venue

As with the first workshop, this workshop took place as part of the annual Association of Internet Researchers (AoIR) conference held from 27-31 October, 2020. The conference is typically held as a physical conference, but as was the case for a lot of events during 2020, the event was converted to being exclusively online. The workshop was titled *Value-driven Next Generation Internet: A future Internet in support of people's lives and global sustainability,* and was one of four pre-conference workshops that the attending Internet researchers were invited to attend.

AoIR was once again chosen as the venue for the workshop as it is one of the largest organizations in the world focused on Internet research, which provided unique access to a large number of academic experts. As mentioned in the first workshop report, D1.13, AoIR prides itself in taking a leading role in advocating ethical and socially responsible approaches to Internet research, and therefore, the topic of human and democratic rights on the Internet seemed a fitting topic in the program.

Even though AoIR focuses on a specific field within research, the attending researchers come from a large number of different academic disciplines conducting research on social, cultural, political, economic, and aesthetic aspects of the Internet.

## 2.2 Participants, survey & quizzes

The participants of the workshop consisted of Internet researchers who attended the 2020 iteration of the AoIR conference and chose to register and take part in this workshop. Six

researchers from Aarhus University attended to act as workshop-tutors, framing the discussions in the breakout groups and taking notes. All participants of the workshop are researchers, but as this deliverable also includes academic literature the researchers attending the workshop will be referred to as “participants”, and authors of academic literature will be referred to as “researchers”.

The workshop had a registration survey that the participants had to fill out prior to attending the workshop (see annex 1). This was on the one hand to gain an overview of the number as well as background of participants, but also to get their initial thoughts on the topic before being influenced by other participants. The survey and quizzes were done individually by the attendants and consisted of free text questions and multiple choices with a free text option. 61 people registered in this survey — excluding the workshop tutors from Aarhus University but including the co-organizers — and 52 different universities and research organizations were represented. The research fields represented were Journalism, Information Studies, Media & Communication Studies, Sociology, Education Science, Digital Design, Social Science, Health, Digital Humanities, Computer Science, Law, Geography, Game Design and language studies. Throughout the online workshop the number of participants fluctuated between 60 and 40 people.

As was the case for the first workshop (described in D1.13), the survey consisted of questions on academic background and field as well as one qualitative question asking participants for their initial reflections on the topic. To combat repetition between the identified topics in the survey from the first and second workshop, we listed some of the identified topics from the first workshop in the survey question (See annex 1 for question and answers).

Furthermore, the workshop participants were encouraged to fill out two quizzes during the two breaks in the workshop (See Annex 2 for questions and answers). The questions of these quizzes varied from broader questions such as “Which internet-related technology or technologies will be predominant in our daily life in 2030?” to more specific ones such as “Which business models and technologies do we need to ensure these values stay a central part of the future internet?”. Where the purpose of the introductory survey, among others, was to establish the general theme of the workshop, the purpose of the quizzes was to establish the themes of the specific sections of the workshop. Additionally, the survey and quizzes helped highlight topics that would otherwise be overshadowed in the discussions between the attendants. Some attendants might feel that a topic is too narrow, obvious or

under-researched to be a suitable topic for discussion, and therefore this initial survey provides potentially valuable output for later research. It is important to note that it was not the purpose of the survey and quizzes to derive quantitative insights, but rather to broaden out the qualitative input from the workshop to further inform the upcoming selection of the next round of NGI Topics.

## 2.3 Structure

The workshop was separated into three sections (see figure 1). The purpose of the first section was to identify examples from the past two years of how technology can negatively affect human-centered values. This was done in breakout rooms and the participants were urged to come up with potential policy solutions to the identified challenges. The second part of the workshop had the purpose of prioritizing the challenges from the first part of the workshop to identify the most important points of attention when creating a human-centric, democratic and sustainable Internet for 2030. Finally, the last section of the workshop consisted of four lightning talks by the co-organizers Katrin Tiidenberg, Nancy Baym, Andra Siibak and Michael Zimmer. These lightning talks centered around topics related to the overall theme of the workshop and were implemented to attract participants.

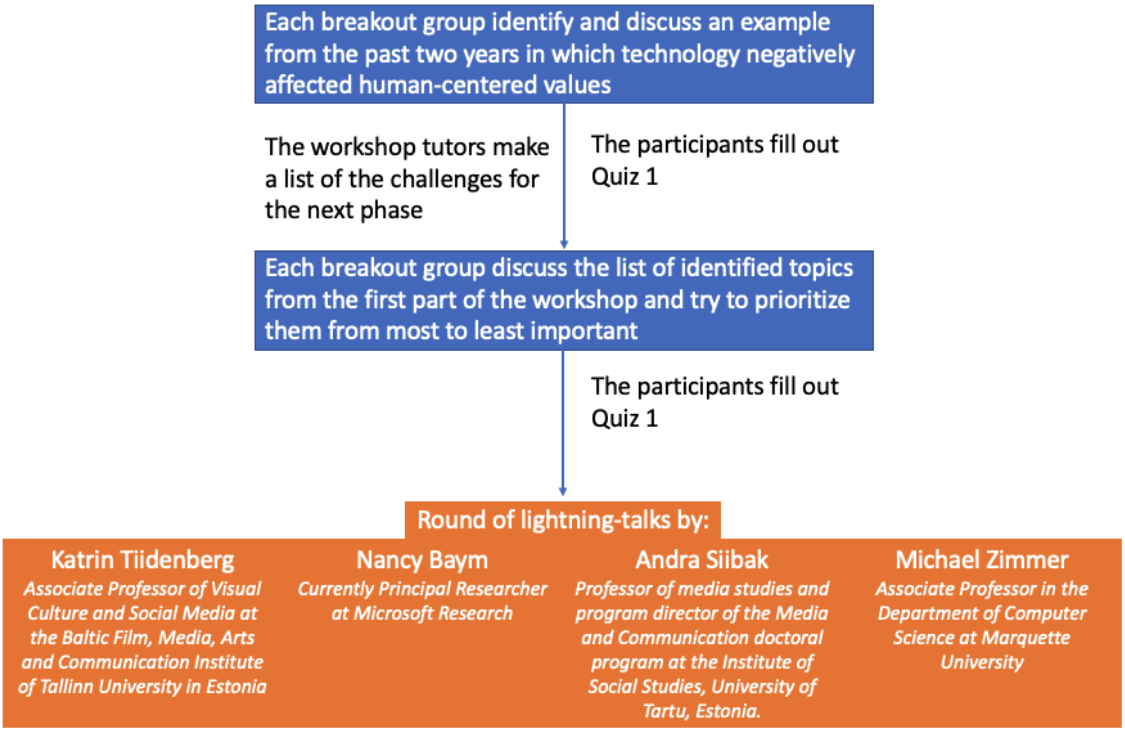


Figure 1: Visualization of the structure of the workshop.

To ensure as little overlap in the discussed topics as possible, the tutors had a document where they could list identified topics. When one topic was identified, the other tutors could

try to steer discussions in other directions. It was in our interest to limit the overlap between the identified challenges as much as possible in the first part of the workshop, to provide an as diverse output as possible. This succeeded to some extent. As it will become apparent in the following analysis, there is some overlap between the topics discussed in the different groups. However, even though this was the case, the six breakout groups ended up identifying seven separate challenges as one group ended up discussing two separate challenges. When there was overlap in the identified challenges the discussions provided diverse policy suggestions. What will later be argued is that ignoring the overlap between different Internet-related challenges would be more damaging than beneficial.

The seven identified challenges were:
1) lacking or unstable Internet access;
2) discriminatory algorithmic decision-making;
3) facial recognition and surveillance;
4) implementing technology without proper deliberation and transparency;
5) shutdowns of Internet by governments to suppress protests or movements;
6) discrimination and hate speech aimed at minorities; and
7) risk of data leaks.

## 3.0 Challenges and policy solutions

The following analysis presents the discussions of the six different breakout groups, based on notes and recordings made by the workshop tutors, which have been contextualized with related academic findings.

### 3.1 Lacking or unstable Internet access

In the first group, two different challenges were discussed. First, the group discussed the challenge of *unstable and lacking Internet access*. The participants discussed how the Internet has become so instrumental to accessing information that instability and lack of connectivity can be a fundamental challenge to democracy. They identified "freedom to be curious" and the possibility of accessing information freely on the Internet as fundamental criteria for a human-centric Internet. "Access" was discussed in general terms to both include infrastructural lack of access as well as politically imposed barriers.

The notion that instability and lack of Internet access can be a fundamental challenge to democracy is by no means novel, but rather a point that has previously been made in academic literature (Reglitz, 2019), where it has further been argued that access to the Internet is a prerequisite for governmental transparency (Tejedo-Romero & Araujo, 2020). In general, transparency within a governance context can be said to describe the availability and accessibility of information (Chen & Han, 2019; Harrison & Sayogo, 2014; Piña & Avellaneda, 2019; Piotrowski & Van Ryzin, 2007; Roberts, 2006) and some researchers have argued that Internet access "is an institutional factor that influences the pattern of citizens' demand for information and pressures for information disclosure and transparency" (Tejedo-Romero & Araujo, 2020). As for the discussed criterium of "freedom to be curious" and the possibility of accessing information freely, the formulation of "freedom of curiosity" as a human right might be novel but both points still directly relate to Article 19 in the UDHR describing freedom of expression, opinion and access to information (The United Nations, 1948).

As a policy solution this group suggested a more decentralized power structure on the Internet, as opposed to the current structure which participants felt gives a limited number of stakeholders the ability to control citizens' access to the Internet. As discussed in one of the other groups, this can be especially problematic when that power is centralized within the government, as there have been examples of Internet shutdowns conducted by national authorities in an attempt to suppress protests or movements that challenge their power.

Examples of this have been seen in countries such as Bangladesh, the Democratic Republic of Congo, Egypt, India, Indonesia, Iran, Iraq, Sudan, Myanmar and Zimbabwe (Roth, 2020).

### 3.2 Discriminatory algorithmic decision-making

The second topic that the first group discussed was *discriminatory algorithmic decision-making.* The group argued that this issue challenges multiple human values and rights that should be at the forefront of a human-centric Internet. Among these challenged values and rights were freedom of opportunities, individual autonomy, the right to be invisible/anonymous as well as the right to be the person they want to be. An example of discriminatory decision-making by algorithms is the 2020 scandal around the university-level entrance (A-level) grading system recently implemented in the UK.

Because of the Covid-19 pandemic, a lot of students worldwide have not been able to physically attend exams. In the UK it was decided that an algorithmic grading system using mock-exams and track-records of the students should be used to give the pupils a fair grading, free from the potential inflation of grades that would potentially happen if the grading was left to the teachers (Shead, 21/08-2020). This case was also discussed in group 3 and will be further uncovered in section 3.4.

When discussing a topic like algorithmic decision-making, the first question should of course be whether the decisions made by the algorithms are fair, which is already a big topic of discussion within academia. Another topic that is only now getting some traction is the *perception* of fairness in algorithmic decision-making as opposed to the *actual* fairness (Wang, Harper and Zhu, 2020, p. 1). Algorithms are already making decisions that have a significant influence on people's lives, such as public safety matters, job hiring, college admissions and loan approvals (Wang, Harper and Zhu, 2020, p. 1) and a lot of documentation of algorithms' capacity for more reliable decision-making already exists (e.g. Cowgill, 2018; Erel et. al., 2018; Kleinberg et. al., 2017; Miller, 2018). The perceived fairness however is another matter, as different stakeholders have different notions of what is fair and what is unfair (Kyung Lee, Tae Kim, & Lizarondo, 2017). One study shows that people's perceived fairness is very dependent on whether they receive a positive or negative outcome themselves (Wang, Harper and Zhu, 2020, p. 1).

As for potential policy solutions for discriminatory algorithmic decision-making, a suggestion derived from academic literature could be to focus on how the argument of the final decision is constructed to try to also comply with the perceived fairness and not only

striving towards fairness in the actual decision-making. A way to heighten the trust in these decisions was by the participants of this group suggested to be to enforce the right to data portability, and that it should be a liability for the data handler when not working. Even though already a part of the GDPR (article 20), participants agreed that they would like to see it enforced more effectively and that people should be made more aware of the possibility of being provided the information that was taken into account in a given algorithmically made decision. Furthermore, in the analysis of the two following group's discussions, we will highlight how their policy suggestions could also be relevant to combat this challenge.

### 3.3 Facial Recognition and Surveillance

The second group discussed a topic that can be said to be under the umbrella of privacy. In general terms, the group discussed video *surveillance, and more specifically the challenges with the use of facial recognition technology*.

The group identified the challenges of facial recognition as being two-fold: 1) technology works best for some demographic groups and 2) technology is developed with too little focus on ethics.

The first of these two challenges relate to another topic discussed in many of the breakout groups: discrimination. How facial recognition relates to discrimination can be exemplified by looking at an experiment run by researchers at American Civil Liberties Union (ACLU). Here, the researchers used Amazon's facial recognition tool, "Rekognition", to find facial matches between members of congress and a database containing photos of convicted felons. In this test, the tool incorrectly identified 28 members of Congress as people who had been arrested for a crime. These identified members were predominantly people of color (Snow, 2018).

The concern of the influence of facial recognition technology is something arising from the still growing integration of machine learning in everyday life, "which in turn raises questions of topics related to bias, fairness, and the formalization of ML (machine learning) standards attract more attention" (Robinson et al., 2020, p. 1). One reason for these biases can be due to the nature of the data and methodology where specific demographics that are at the majority of the test set are favored. This skew in performance of particular demographics can be identified as a bias of the algorithm (ibid.).

In extension of the previous challenge, the other challenge of facial recognition that was

discussed in this group was a reflection on the ethical considerations made when developing facial recognition solutions. The critique was here, that one thing is the discussions of ethical use of the tool, another is the inherent ethics of developing the tools themselves. The group therefore discussed the possibility of banning the technology and putting it on hold while establishing the ethical guidelines of the technology but conceded that even if this was the right approach from an ethical standpoint, it would be close to impossible enforce globally.

Instead of banning the technology, one policy solution could be to enforce more balanced [data] test sets, which could, in turn, combat the aforementioned skew favoring the majority demographic. This could be done by implementing a system of proving fairness before the technology is implemented. It is, however, still a thoroughly complicated matter, as identifiers such as race and gender are not only things that are currently a big topic of discussion, but also something that can make developing functioning facial recognition tools challenging, as definitions vary greatly from source to source (Robinson et al., 2020, p. 2). For example, some preliminary research criticizes the oversimplified label of male and female from an instrumental point of view, as they argue, that rather than a binary input it should be a value between zero and one to improve accuracy, so that gender is viewed as existing on a spectrum rather than being perceived as either one or the other (Merler et. al., 2019, s. 16).

Another solution, which was suggested by this breakout group, is to regulate the diversity at the top levels of both engineers and policymakers to highlight biases and discrimination inherent to the tools.

The third and final suggestion is to include ethics as a more prominent part of the curriculum of computer science-educations. This third suggestion was also argued to entail greater interdisciplinary collaborations between computer scientists and more human-centered fields of research to move the focus away from exclusively math and algorithmics research into more research on human implications. This suggestion from the group would also be a relevant suggestion to combat the aforementioned challenges of unfair algorithmic decision-making.

The discussions of the challenges of facial recognition are something that one member of the group found severely lacking in a European context whereas the US is far more focused on the problem. A reason for this was suggested to be that there have not been any high-

level scandals in Europe to make the general public aware of the technology, its possibilities and especially its challenges. So, another priority should be to highlight the challenges of the technology and encourage further public deliberation on the subject.

### 3.4 Implementing technology without proper deliberation and transparency

The discussions in this group had a similar starting point as the group described in 3.2, as they also discussed discriminating algorithmic decision-making with the British algorithmic grading system at the basis of the discussion. However, where the first group saw this as a concrete example related to algorithmic decision-making, this group saw it as a broader example of how *implementing technology without proper deliberation and transparency* can lead to societal and social challenges.

The British algorithmic grading scandal was understandably a topic discussed in multiple groups, as it captures some of the fundamental challenges in the tension field between human rights, democratic values and technology. In this group, the participants pointed to freedom from discrimination, rule of the majority, political equality and right to education as human rights that were challenged by the scandal.

The group discussed how the scandal did not seem to be an example of malintended national authorities actively trying to actively discriminate against students. The well-meaning intentions but problematic results of the implementation of the technology highlights the importance of the challenge that this group discussed. The group saw this event as an example of when technology is implemented too fast, without proper public deliberation and transparency.

Therefore their suggestion for combatting cases such as this was to call for more deliberation and slowing down the discussions of implementing new technology that can affect citizens to the extent that was the case for the UK grading system, where students' future opportunities  of pursuing higher education were potentially influenced by a skewed grading-algorithm. The group suggested having requirements of public debates, transparency and testing to act as a road bump before implementing technology. As with the previous group's policy suggestions, this suggestion would also be valuable when discussing the topic of biased algorithmic decision making, as discussed by the first breakout group.

## 3.5 Internet shutdowns

The question of decentralizing versus centralizing the power of the Internet is interestingly portrayed in the discussions of this group. Because, whereas one of the topics chosen as the first set of key NGI topics was "Decentralizing the power on the Internet" — which was also discussed in connection with the challenge of limited access to the Internet — this group discussed centralizing the point of control to an international, neutral level.

*Internet shutdowns* can take different forms, but in general, the term describes a means of disrupting citizens' access to information by blocking access to the Internet or platforms (Parks & Thompson, 2020, p. 4288). Thus, the group argued that Internet shutdowns challenge multiple human rights such as freedom of expression, freedom of information, freedom of opinion and the right to assemble.

The group specifically discussed Internet shutdowns in African countries, which is interesting as it is an under-researched area compared to the shutdowns in the likes of China, Iran, and Turkey (Parks & Thompson, 2020, p. 4289). This is even though Internet shutdowns occurred in 13 African countries in 2018 alone (Taye, 2019). One reason that could potentially explain the limited focus on the Internet shutdowns in Africa compared to other countries is that the shutdowns are not always the typical short-term technical shutdowns that the term *Internet shutdown* typically describes (Parks & Thompson, 2020, p. 4288). In for example Tanzania, a different type of Internet shutdown has by Parks and Thompson been called a *slow shutdown* (ibid.). This shutdown is not a case of a temporary short-lived shutdown — as the technical shutdowns — but rather a gradual suppression of the citizens' means of communication and communication channels over an extended period of time. These shutdowns are done legislatively and have gradually intensified during the last decade, as the Internet and social media has been accessible for a larger number of citizens in the aforementioned African countries (Ayalew, 2019, p. 208; Parks & Thompson, 2020, p. 4289). The participant who initiated the discussion of this topic is affiliated with the University of the Witwatersrand in Johannesburg, and specifically mentioned the Internet shutdowns in Cameroon, Ethiopia and Egypt as cases he had followed closely.

During the discussion, the shutdowns in African countries were described as "governments adopting softer ways of suppressing free opinion and information". The aforementioned participant described how Kenyan bloggers are shut down by the government, and in some cases — depending on how critical they are towards the government - these bloggers are even arrested and tried for the likes of hate speech or defamation. According to the

participant, this has resulted in a situation where all the most prominent bloggers in Kenya have pending legal cases with either private companies or the government.

Another example of these regulations is the social media taxes implemented in Uganda in 2018. These taxes have been criticized for being a means of silencing free speech (Akumu, 2018). Furthermore, there have been examples of surveillance cameras being installed in Internet cafes as well as an implementation of a license requirement to run a blog in Tanzania which provides the government with means of controlling who is allowed to express their opinion online (World Politics Review, 2018). These gradual shutdowns typically intensify around elections where technical shutdowns are also used to prevent organizing protests or reporting election fraud (Freyburg & Garbe, 2018, p. 3896 f.).

The primary policy suggestion that the group came up with was to combat the challenge of Internet shutdowns performed by national authorities by centralizing the power of the Internet at an international and neutral place. This would remove the responsibility of Internet access from the individual ISPs (Internet service providers), which could remove some of the power that some governments hold over these ISPs. This is a solution supported by academic literature, where there has been found a correlation between the Internet shutdowns in sub-Saharan African countries and ISPs with majority ownership by authoritarian states (Freyburg & Gabe, 2018, p. 3896). This study points towards the importance of varied ownership of ISPs that cannot be controlled by the government (Ibid.). Centralizing the point of power would however only solve the problem of the temporary technical shutdowns and not the slow shutdowns done through legislation. To combat this gradual suppression of the citizens' access to the Internet, the group discussed the possibility of international legislation to respect people's right to freedom of expression, freedom of information, freedom of opinion and right to assemble. Furthermore, the group suggested altering the technical design of the Internet by using encryption of data to make it harder for governments to identify specific actors.

In *D1.9: NGI Topic guides and evaluation report I* it was argued that decentralizing the power of the Internet was an important priority in securing a more human-centered Internet, because the Internet today is controlled by a handful of giant companies that act like gatekeepers (e.g. Zuboff, 2019, Møller et. al. 2020). This is an interesting point when contrasted to the discussions of this group, who instead of decentralizing actually suggested centralizing the power. Furthermore, the discussions of limited access to the Internet in the first group also concluded with a policy suggestion of decentralizing the

power of the Internet. So, discussions in two groups that relate to very similar topics ended up with very different policy suggestions, which exemplifies the importance of taking different starting points when discussing potential policy solutions, as it can result in vastly different solutions to similar challenges. The two policy suggestions can however be said to be two sides of the same coin, as both are based on a wish to minimize the misuse of power by specific actors — be it governments or the private sector.

### 3.6 Discrimination and hate speech

The fifth group discussed *discrimination and hate speech*. The initial discussions centered around the violence and hate speech against Muslim minorities in Myanmar. However, the discussions were quite expansive in this group and provided insides on both power on the Internet, private actors and trustworthy information flow.

To understand the different points of discussion in this group, some background-knowledge is needed as some points might not seem related otherwise. Myanmar was under authoritative rule until 2010, which meant restrictions on media, cell phone access and Internet use to minimize the possibility of outside information and anti-regime organizing[1]. However, in 2010 a new semi-elected government gained the power and new legislation was implemented allowing freedom of speech, association and assembly — though still with fundamental restrictions (Fink, 2018, p. 44). At the same time, the government opened up for foreign telecommunication companies which meant cheaper sim-cards and a surge in the availability of telephones and Internet access for the public. Due to the fact that these phones typically came preloaded with Facebook installed and that time spent on Facebook was not counted in the mobile phone plan's, Facebook became a huge part of the new digital reality of the citizens of Myanmar. While this has offered the citizens of Myanmar a possibility of expressing themselves and obtaining information, it has also contributed to a rising amount of hate speech and general disdain towards the Muslim minority in the country, which in turn has led to violence (ibid.; Stevenson, 2018). Facebook has taken some responsibility in the matter and in a report, they detail how, they "unwittingly entered a country new to the digital era and still emerging from decades of censorship, all the while plagued by political and social divisions" (Stevenson, 2018). However, the platform has been criticized for not doing enough to identify and minimize a vast amount of posts and misinformation that fueled what has been called a modern ethnic cleansing in Myanmar

[1] Since the workshop a there has been a military coup in Myanmar, and the elected leaders have been detained: https://www.bbc.com/news/world-asia-55882489

(ibid.).

With basis in this case three fundamental challenges were discussed in relation to hate speech. The first of these challenges is the need for digital literacy. One of the identified points, which was argued to have a fundamental influence on the rise in hate speech and violence against the Muslim minority in Myanmar, is the lack of general knowledge about the use of the Internet among the citizens. The ability to separate true and false information is something that has proved challenging even in countries where the citizens are more used to using the Internet, and the group, therefore, suggested actively pursuing digital literacy in both countries new to the Internet and in countries more familiar with it. One of the participants in the group highlighted how this lack of digital literacy was especially problematic because the phones came with Facebook pre-installed as this made Facebook the primary news outlet to a large number of citizens, which allowed for a rampant spread of mis-, dis- and malinformation. Having a social media as the primary news source can be problematic as the amount of user-provided content and the ease of sharing news-content can aggregate citizens around shared worldviews and narratives (Pourghomi et. al., 2017).

The next challenge that the group discussed related to the Myanmar case was the power and responsibility of private actors, which relates directly to the topic of securing trustworthy information flows. In Myanmar it was seen how a minority of Buddhist ultranationalists used Facebook to spread a narrative of how Muslims posed a threat to both individual people and to the Buddhist majority nation (Fink, 2018, p. 44). To combat this, one participant highlighted the need for effective content moderation on the platforms. However, it was also agreed upon that the practicalities of this pose some not so minor challenges if the content is to be reviewed manually by people, which is still the most common means of testing the trustworthiness of information on social media platforms (Walter, Sørensen & Bechmann, 2020). The group discussed the possibility of AI technology to both combat hate speech and to provide faster fact-checking than the manual method allows.

Finally, the discussion of this group also relates to the challenges of totalitarian political systems, because even though some legislation was made to allow freedom of speech, association and assembly, there were still fundamental restrictions and problems in how the situation was handled by the government in Myanmar. For example, a law passed in order to authorize fines and prison sentences to people proven guilty of causing undue influence and “threatening any person using a telecommunication network” (The telecommunication law,

2013) was used to charge both journalists and individuals who were critical towards political leaders online (Fink, 2018, p. 47). Furthermore, the government has been criticized for not explicitly condemning narratives promoted by Buddhist ultranationalists and for benefitting from these narratives (ibid.).

Maybe the most important point in the discussion was the need for shifting the focus of research to a more global south perspective. One researcher argued that the challenges of the Internet are often looked at through a global north perspective, but that it would be just as — if not more — fruitful to focus research on the global south instead as the challenges are often magnified in these countries. Because, where the US elections of 2016 and 2020 were seen to have a large amount of hate speech, polarization and misinformation, these tendencies could be seen just as clearly in Myanmar. For example, there are clear parallels between the way Buddhist ultranationalist movements in Myanmar have used common fears to build a community and the polarizing language used during the 2020 US election. Furthermore, the critique of the government in Myanmar for not condemning the Buddhist ultranationalists seems similar to the critique President Trump met when he did not condemn white supremacy explicitly (Shear, Broadwater, Cooper & Cochrane, 2020).

### 3.7 Risk of data leaks

The sixth and final group discussed the *risk of data leaks*.

There are many examples of data leaks, and as more communication channels and institutional data such as health, economic and educational data is digitized and stored on different platforms, controlled by different governmental and private actors, the need for data security as well as transparency becomes increasingly important. As argued in *D1.9: NGI Topic guides and evaluation report I* high-level data breaches such as the infamous Cambridge Analytica scandal have highlighted just how little control we have over our own data.

Much of the discussion in this group centered around online platforms' handling of data and the group pointed not only at privacy but also at topics such as access to information, technology, rights to govern own data and transparency as necessary focus-points when fighting the mishandling of our data. Furthermore, it was argued that privacy in itself could not be the topic of the discussion, as this would entail privacy being a fixed and clear concept - which it was argued not to be. This discussion led to the specific topic of data leaks from the platforms. When referring to this topic the group discussed how coming up

with a specific event where this had happened seemed almost trivial, as the occurrence seemed so frequent. Instead, the group discussed different potential policy solutions to combat the mishandling of the data instead of discussing one event in particular.

The first policy suggestion was to establish more transparency of who specifically controls data, and in extension thereof, who is accountable for when the mishandling or breaches actually happen. In extension of this point, the group discussed the possibility of implementing more accountability mechanisms at different levels of the process such as the business model, the collection, the storage and the processing.

The second suggestion and the most dividing one within the group was breaking up the data to make it harder to deanonymize. This was the most divisive suggestion because this would make the work of researchers way harder. As social media has become one of the most – if not the most – important facilitator of communication and sharing of information (Stieglitz et al., 2018), social media has become an important source of empirical data for researchers in a lot of different academic disciplines (Batrinca & Treleaven, 2015). In addition to the reduced access to the data due to several privacy breaches, the anonymization of the data challenges research because anonymizing the data fully, challenges the validity of the results (Dwork, 2008). Instead, different solutions such as social media data safe spaces for researchers have been suggested (Møller, Walter & Bechmann, 2020).

The third and final suggestion that the group came up with was legislatively forcing a slowdown of the collection of our data. The group discussed that one of the biggest challenges with data collection is that it is hard to control it due to the pace at which data is collected.

## 3.8 Challenges and policy solutions – Overview

Below is an overview of all the challenges and their accompanying policy solution from previous analysis.

| **Challenges** | **Policy solutions** |
|---|---|
| Lacking or unstable Internet access | - Decentralizing the power structure on the Internet. |
| Discriminatory algorithmic decision-making | - Focusing on the perceived fairness |

| | |
|---|---|
| | of algorithmic decision-making (derived from literature review)<br>- Enforcing t the right to data portability |
| Facial recognition and surveillance | - Enforcing more balanced test sets, to combat the skew favouring the majority demographic (derived from literature review)<br>- Regulating the diversity at the top levels of engineers and policymakers to highlight biases and discrimination inherent to the tools<br>- Including ethics as a greater part of the curriculum of computer science-educations |
| Implementing technology without proper discussions and transparency | - Implementing public scrutiny, transparency and testing to act as a “road-hump” before implementing technology |
| Internet shutdowns | - Centralizing the point of control for internet access at an international and neutral place<br>- Implementing international legislation to respect peoples’ right to freedom of expression, freedom of information, freedom of opinion and right to assemble<br>- Altering the technical design of the Internet by using encryption of data to make it harder for governments to identify specific actors |
| Discrimination and hate speech | - Implementing digital literacy<br>- Implementing effective content moderation on the platforms (need for the development of automated solutions)<br>- Initiating research focused more on the global south |
| Risk of data leaks | - Establishing more transparency over who is controlling the data<br>- Establishing accountability for when the mishandling or breaches actually happen<br>- Scrambling the data to make it harder to deanonymize (not good for research)<br>- Legislatively forcing a slowdown of the collection of our data |

## 4.0 Prioritization and grouping of the challenges

In this section of the report, we will provide an overview of the previously described discussions including the discussions that the participants had in the second part of the workshop, where they were asked to prioritize the seven challenges from the first part of the workshop. This second part of the workshop proved that many of the discussed challenges are intertwined in ways that make it hard to prioritize one over the other. This was however to be expected as the challenges were never meant to be a comprehensive list of all challenges related to the Internet, but rather discussions around how the Internet and Internet-technology has, and can, negatively affect human-centered values. The intended outcome of the prioritization exercise was therefore not to provide a simple ranked list of Internet-related challenges, but rather to further the discussions with a different point of departure to the first part of the workshop.

Only one group ended up prioritizing the challenges. In the other groups, there was a higher degree of grouping and comparing the different challenges instead of actually organizing them from most to least important. The group that did end up prioritizing the challenges prioritized them as follows:

| **Priority** | **Internet-related issues** |
|---|---|
| Very high | Internet shutdowns |
| Very high | Facial recognition technology |
| High | Discrimination of minorities |
| High | Risk of data leaks |
| Medium | Discriminating algorithms |
| Medium | Lacking or unstable Internet access |
| Lower | Implementing technology without proper deliberation |

The first point made in this group before prioritizing the challenges was related to the suggestion of taking a more global south perspective in research. Namely, one participant framed the discussion by pointing out the importance of looking at these challenges through a global lens rather than evaluating them purely based on the participants' own contexts. This same participant started by referring to the challenge of "Internet shutdowns" as potentially the most extreme of the challenges — however, still concurring that this

evaluation depends on the way you view the different challenges compared to each other as they are all important. One of the other participants pointed towards the challenges linked to facial technology as another high priority challenge, as it is a very prominent part of the direction that society is moving while being a challenge that affects a lot of different societies. This participant argued that the fact that facial recognition will potentially influence a larger number of people negatively than the number of people affected by Internet shutdowns, is a reason to say that facial recognition is an even more important point of attention. The question left by this part of the discussion is whether the amount of people affected by the challenge or the severity of the challenge holds precedence over the other.

On the opposite side of the spectrum, the challenge that was prioritized the lowest by the group was “Implementing technology without proper discussion”. The justification for this was that even though this is critical, it happens all the time and the outcome is varying depending on the specific technology and context in which the technology is implemented. Furthermore, the challenge in itself was deemed too vaguely formulated with unknowns such as: “Discussions between who?” “Transparency from who to whom?” Focusing too much on this challenge from a policy standpoint could therefore result in not concrete and less valuable outcomes and solutions, according to this group.

In another group, however, it was argued that the challenge of implementing technological, algorithmic and digital solutions without proper discussion in many ways contains the other challenges and should therefore be prioritized highly. It was further argued that implementing these suggested deliberative road bumps could be a way of challenging the tendency of asking for forgiveness rather than asking for permission both in governmental and corporate decision-making. Furthermore, the need for public deliberation before implementation would shift what can in some instances be very opaque processes to be more transparent by making the discussions prior to implementation publicly accessible. One participant in this group also drew a parallel between this challenge of lack of deliberation and a need for restructuring the power of governmental and private actors on the Internet. This question of the power on the Internet is a topic that is highly relevant in all of the discussed challenges in the workshop and is something that should be of high priority in policymaking and legislation.

Regarding the question of an increased amount of transparency, one group discussed the possibility of providing more of a choice when it comes to personalization. This could for

example be a choice between being presented with a neutral newsfeed on Facebook compared to a personalized feed. In relation a higher degree of control over one's own data was discussed, which also relates to not only facial recognition data but also biometric data in general.

These discussions also led one group to discuss the underlying challenge of actually implementing the suggested solutions. Here, it was discussed how globally embedded the Internet is, and how you would even go about implementing it if an alternate design was to be developed. This discussion led to the conclusion that it might be easier to restructure the current Internet as opposed to starting from scratch. From here, it was derived that the global regulatory environment is fragmented and that the closest thing to a universally accepted framework would be the Universal Declaration of Human Rights. These would however have to in some way be made Internet-specific in order to use it as some kind of enforcement mechanism - a point mirroring the critique that the United Nations met when they promoted the protection of Human Rights on the Internet, as this was deemed to universal to actually combat some of the unique challenges of the Internet (Reglitz, 2019). The participants of this group however agreed that the lack of an Internet specific framework is not the problem, as such frameworks do exist. One example of a more internet-centered set of human rights is the Internet Rights & Principles Coalition (IRPC), based at the UN Internet Governance Forum called *Charter of Human Rights and Internet Principles for the Internet* (https://internetrightsandprinciples.org/campaign/):

1. Universality and equality
2. Rights and social justice
3. Accessibility
4. Expression and association
5. Privacy and data protection
6. Life, liberty and security
7. Diversity
8. Network equality
9. Standards and regulation
10. Governance

The problem is on the contrary the frameworks such as the Charter of Human Rights and Internet Principles are not systematically used by legislators.

One participant tried summing up the identified challenges as fitting into two separate overarching challenges; transparency and privacy. While this can be deemed true for four of the seven challenges it is also a simplification of the nuances that each of the challenges contain. Furthermore, three of the seven challenges would have to be altered fundamentally to neatly fit into these two overarching topics. As made clear by the model below, the challenges of "Unstable and no Internet access", "Internet shutdowns by governments" and "Discrimination and unequal access" do not easily fit into the categories of neither transparency nor privacy. Of course, the *slow shutdowns* could be said to relate to privacy in that the government can find and prosecute regime-critical bloggers and journalists but to fit the challenge into the umbrella of privacy a lot of the nuances concerning power would be lost.

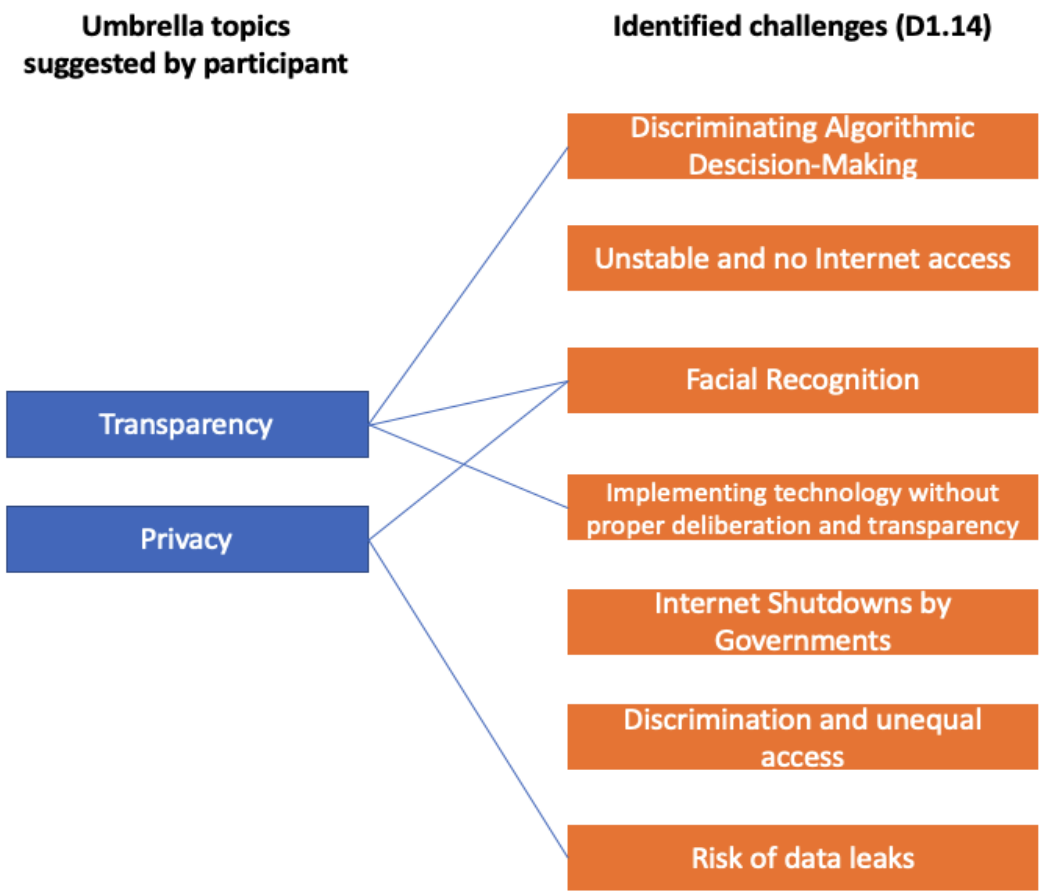


Figure 2: Relationship between umbrella topics of transparency & privacy and challenges identified in workshop (D1.14)

In general, it would be more natural to compare the challenges discussed in this workshop to the 8 initial NGI topics, as this portrays the multifaceted nature of the challenges as well as the overlaps. When comparing the seven challenges with the NGI topics identified in D1.9

it becomes clear that the NGI topics are general enough to also include the challenges identified in the workshop, but also that there is a vast overlap between the topics and the challenges, making it clear just how intertwined the current and future challenges of the Internet are. Furthermore, while the topics identified in the first workshop (D1.13) and in the following identification of key topics in D1.9 provided a general overview of challenges, the aim of this and the final expert workshop will be to discuss more specific challenges to gain more actionable policy solutions.

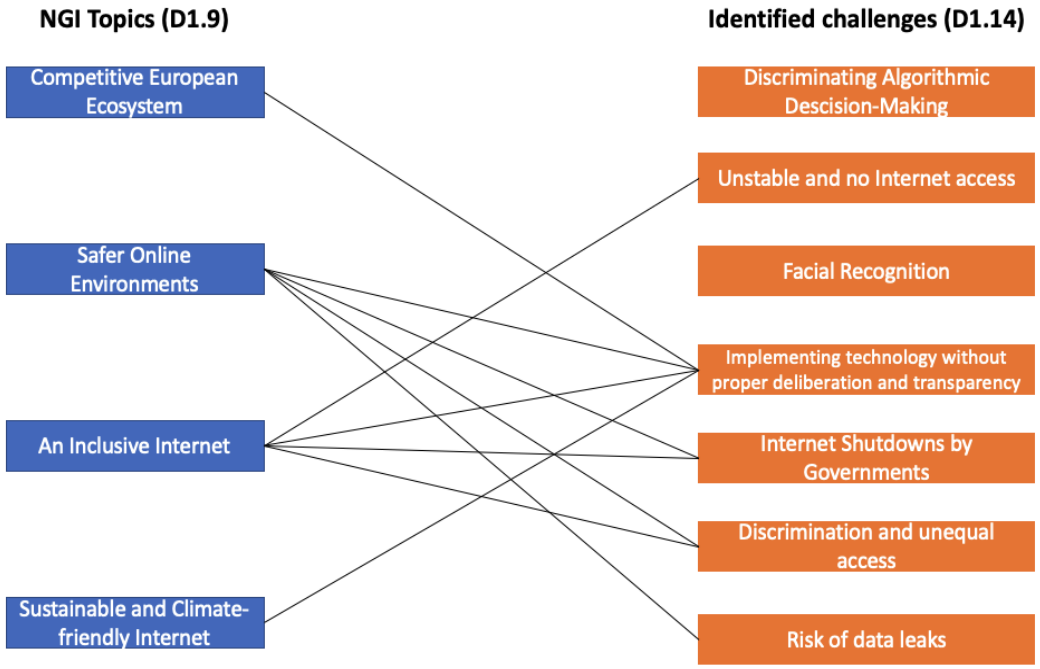


Figure 3.1: Relationship between initial NGI Topics (D1.9) and challenges identified in workshop (D1.14).

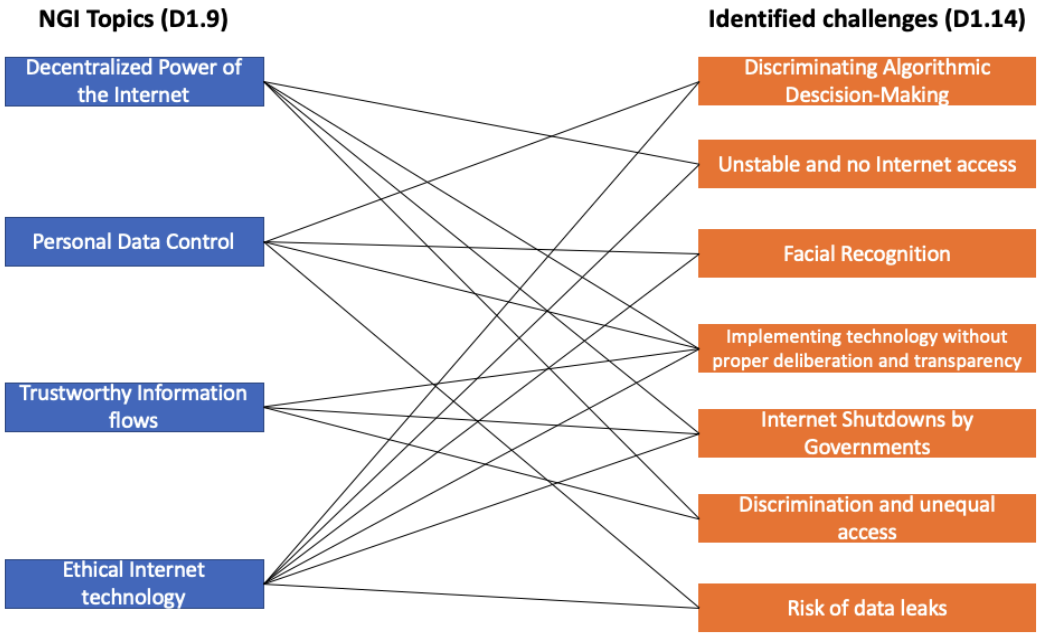


Figure 3.2.

While there is some truth in the statement made by one participant, that all of these topics either fit in the category of transparency or the category of privacy, it is also a synthetization of the topics which overlooks the nuances. Topics such as deliberation and questions of power were very clearly portrayed in the discussions in the different groups but would be reduced to a side note if the challenges were reduced to just concern privacy and transparency.

The case-specific approach that we took in this workshop resulted in more specific, narrower topics that in turn gave a more policy-oriented output than the first workshop. So even though most of the topics discussed in this second workshop in one way or another fit into the umbrella of the first NGI topics (D1.9), the discussions both provided new challenges and new solutions. As an example, the possibility of centralizing the control of internet access at an international and neutral point of control gave new input to the discussion of how to regulate the misuse of power by single actors — both governmental and private. While there are some correlations between the different topics of discussion in this workshop and the 8 NGI topics, the identification of challenges provided a new output which more clearly portrays the connections between the different topics and challenges.

One thing that can be derived from both the previous analysis of the initial discussions in the breakout groups, the aforementioned relationship between the NGI topics and the challenges from this workshop and finally the apparent difficulty of not being able to prioritize the different challenges, is the interconnectedness of many of the internet-related challenges we face globally both currently and in the future. This interconnectedness is very likely the reason that a lot of groups found it easier to find similarities between the different challenges and umbrella-challenges rather than prioritizing them compared to each other. This could be an argument to actively pursue holistic solutions.

## 5.0 Conclusions and next steps

During the workshop the participants were asked to find and discuss a current challenge in the tension field between human rights, democratic values and the Internet. In the first part of the workshop the participating researchers were separated into six different breakout groups and came up with seven separate challenges and seventeen potential policy solutions to combat these challenges, while two additional policy solutions were derived from academic literature (for overview see section 3.8).

In the second part of the workshop it became apparent that pursuing holistic solutions rather than focusing on single challenges, as well as focusing on global challenges rather than exclusively focusing on the global north, could be a way to achieve the best results, as the different challenges and policy solutions are intertwined in numerous ways. This interconnectedness became further exemplified by looking at the connections between the initial NGI topics and the identified challenges in this workshop.

To secure this holistic approach to the current and future Internet-related challenges it was suggested to have a set of human rights that are Internet-specific. The participants however conceded that this lack of a framework is not due to the framework not existing, but rather that these existing frameworks are not consistently used as the basis of legislation, regulation and policy making in general.

The results from this and the final workshop will along with quantitative data from additional work done in *WP1: Topic Identification* be used to select the final set of 8-10 NGI Topics that should be the primary points of attention in support of a more human-centric evaluation of the Internet.

## 6.0 Literature


Akumu, P. (2018). “Uganda introduces social media tax despite criticism”. Latest retrieved 31-03-2021 from: https://www.aljazeera.com/economy/2018/7/1/uganda-introduces-social-media-tax-despite-criticism

Charter of Human Rights and Internet Principles for the Internet. “Internet Rights & Principles Coalition (IRPC)” Latest retrieved 31-03-2021 from: http://internetrightsandprinciples.org/site/campaign

Chen, C. , & Han, Y. (2019). Following the money: The political determinants of E-fiscal transparency in US states. Public Management Review , 21(5), pp. 732–754. doi:10.1080/14719037.2018.1523451

Cowgill, B. (2018). “Bias and Productivity in Humans and Algorithms: Theory and Evidence from Résumé Screening”.

Dahl, R., A. (1989) *Democracy and its critics*, New Haven: Yale University Press.

Dwork, C. (2008). “Differential Privacy: A Survey of Results”. In M. Agrawal, D. Du, Z. Duan, & A. Li (Eds.), Theory and Applications of Models of Computation, pp. 1–19. Switzerland: Springer. doi: https://doi.org/10.1007/978-3-540-79228-4_1

Erel, I., Stern L., H., Tan, C., and Weisbach, M., S. (2018). “Could Machine Learning Help Companies Select Better Board Directors?” In Harvard Business Review. https://hbr.org/2018/04/research-could-machine-learning-help-companies-select-better-board-directors

Fink, C. (2018). “Dangerous Speech, Anti-Muslim Violence, and Facebook in Myanmar”. In: Journal of International Affairs, 71(1.5), pp. 43-52: https://www.jstor.org/stable/26508117?casa_token=piHQ2EnzhkMAAAAA%3AR_7wiQSOO0O5lDKWG0VcsJopJFtz1woGBWeDl8NHpuFlw7ViV0MJ5bthHo-WM9N7P-tOlGTnPz9nz2velhPl-nAq1raH1D6wXaa2mdxlpfiYziNNxCA&seq=1#metadata_info_tab_contents

Freyburg, T., & Garbe, L. (2018). “Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa”. In: International Journal of Communication,

12, pp. 3896-3916.: https://ijoc.org/index.php/ijoc/article/view/8546

Gyódi, K., Nawaro, Ł., Paliński, M., & Wilamowski, M. (2019). D1.2: "Visualisations of key emerging technologies and social issues." The European Commision.

Harrison, T. M. , & Sayogo, D. S. (2014). "Transparency, participation, and accountability practices in open government: A comparative study." *Government Information Quarterly* , 31(4), pp. 513–525. doi:10.1016/j.giq.2014.08.002

Head, J. (1/02/2021). "Myanmar coup: Aung San Suu Kyi detained as military seizes control": https://www.bbc.com/news/world-asia-55882489

Kimber, R. (1989). "On Democracy" In: Scandinavian Political Studies 12(3), pp. 199-219.

Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J. and Mullainathan, S. (2017). "Human decisions and machine predictions" In: The quarterly journal of economics 133(1), pp. 237–293.

Lee, M., K., Kim, J., T. and Lizarondo, L. (2017). "A human-centered approach to algorithmic services: Considerations for fair and motivating smart community service management that allocates donations to non-profit organizations". In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 3365–3376. doi: https://doi.org/10.1145/3025453.3025884

Matfess, H., & Smith, J. (2018). "Africa's attack on Internet freedom. Foreign Policy." Latest retrieved 31-03-2021 from https://foreignpolicy.com/2018/07/13/africas-attack-on-internet-freedom-uganda-tanzaniaethiopia-museveni-protests/

Merler, M., Ratha, N., Feris, R., & Smith, J., R., (2019). "Diversity in Faces", *arXiv:1901.10436v6:* https://arxiv.org/pdf/1901.10436.pdf

Miller, A., P. (2018). "Want Less-Biased Decisions? Use Algorithms" In: Harvard Business Review: https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms

Møller, L. A., & Bechmann, A. (2019). D1.13: Value-driven future internet: A social scienceperspective I. The European Commission.

Møller, L., A., Bechmann, A., Gyódi, K., Paliński, M., Nawaro, L. (2020). “D1.9: NGI Topic guides and evaluation report I”. The European Commission.

Møller, L. A., Walter, J. & Bechmann, A. (2020). “D2.1: Evaluating Safe space solution including data management and processing setups”. The European Commission, SOMA [825469].

Parks, L., & Thompson, R. (2020). “Internet Shutdown in Africa| The Slow Shutdown: Information and Internet Regulation in Tanzania From 2010 to 2018 and Impacts on Online Content Creators”. In: International Journal Of Communication, 14, 21.: https://ijoc.org/index.php/ijoc/article/view/11498/3186

Piña, G. , & Avellaneda, C. (2019). Central government strategies to promote local governments’ transparency: Guidance or enforcement? In: *Public Performance & Management Review* , 42(2), pp. 357–382. doi:10.1080/15309576.2018.1462215

Piotrowski, S. J. , & Van Ryzin, G. G. (2007). Citizen attitudes toward transparency in local government. *The American Review of Public Administration*, 37, pp. 306–323. doi:10.1177/0275074006296777

Pourghomi, P., Safieddine, F., Masri, W. and Dordevic, M. (2017). "How to stop spread of misinformation on social media: Facebook plans vs. right-click authenticate approach," In: *2017 International Conference on Engineering & MIS (ICEMIS)*, doi:10.1109/ICEMIS.2017.8272957.

Reglitz, M. (2020). “The Human Right to Free Internet Access”. In: Journal of Applied Philosophy, 37(2), pp. 314-331 : https://onlinelibrary.wiley.com/doi/full/10.1111/japp.12395?casa_token=aMQKnZj3U6YAAAAA%3ARxlH85nDw2cv4CxTGKzFYAu792AxFayPlyPnez2qhP-UMFXnG2FQsD_CJoU8ZkG-vA1gsK2717pr9g

Roberts, A. (2006). *Blacked out: Government secrecy in the information age* . New York, USA: Cambridge University Press.

Robinson, J., P., Livitz, G., Henon, Y., Qin, C., Fu, Y. & Timoner, S. (2020). "Face Recognition: Too Bias, or Not Too Bias?" *CVPR 2020 Workshop paper:* https://openaccess.thecvf.com/content_CVPRW_2020/papers/w1/Robinson_Face_Recognition_Too_Bias_or_Not_Too_Bias_CVPRW_2020_paper.pdf

Schneier, B., (2020). "We're BanningFacial Recognition. We're Missing the Point." Latest retrieved 31-03-2021 from https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html

Shead, S. L. (2020). "How a computer algorithm caused a grading crisis in British schools". Latest retrieved 31-03-2021 from: https://www.cnbc.com/2020/08/21/computer-algorithm-caused-a-grading-crisis-in-british-schools.html

Snow, J. (2018). "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots". Latest retrieved 31-03-2021 from: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Stevenson, A. (2018). "Facebook Admits It Was Used to Incite Violence in Myanmar". Latest retrieved 31-03-2021 from: https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html

Taye, B. (2019). "The state of Internet shutdowns around the world: The 2018 #KeepItOn report." Latest retrieved 31-03-2021 from: https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018- Report.pdf

Tejedo-Romero, F. & Araujo, J., F., F., E. (2020). "E-government-enabled transparency: The effect of electoral aspects and citizen's access to Internet on information disclosure", In: Journal of Information Technology & Politics, 17(3), pp. 268-290, doi: 10.1080/19331681.2020.1713958

The Editors. (2018). "How Tanzania's Government Is Trying to Dismantle a Free Press 'Piece by Piece'". Latest retrieved 31-03-2021 from: https://www.worldpoliticsreview.com/trend-lines/24595/how-tanzania-s-government-is-trying-to-dismantle-a-free-press-piece-by-piece

The Telecommunications Law (2013), “The 4th Waxing Day of Thadingyut, 1375 M.E., 8 October 2013”. Latest retrieved 31-03-2021 from: http://www.burmalibrary.org/docs23/2013-10-08-Telecommunications_Law-en.pdf.

The United Nations. (1948). *Universal Declaration of Human Rights*.

Walter, J., Sørensen, M., H. & Bechmann, A. (2020). “D2.3: Outlier (disinformation) detection solution”. The European Commission, SOMA [825469].

Wang, R., Harper, F., M. & Zhu, H. (2020). “Factors Influencing Perceived Fairness in Algorithmic Decision-Making: Algorithm Outcomes, Development Procedures, and Individual Differences”. *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems:* https://dl.acm.org/doi/pdf/10.1145/3313831.3376813

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 edition). New York: PublicAffairs.

## Annex 1: Survey responses

| **Question: Based on the latest workshop as part of the Next Generation Internet initiative at AoIR19, several goals were chosen to inform the European Commission's future research agenda, such as Trustworthy Information Flows, Decentralised Power, Personal Data Control, and Sustainable Internet. According to you, what should be the next important topics to shape the vision of a more human-centric future internet? Please name and prioritize 3-8 topics below.** |
|---|
| 1. data and internet literacy 2. healthier environments from multiple perspectives (safer and more inclusive, climate-friendly, trustworthy information) 3. transparency in personal data management and algorithms implementation |
| 1. Tech for social good, 2. Trust in ai 3. Global tech, local values |
| 1) labour rights for platformed workers 2) algorithmic transparency 3) collectivised/deprivatised platforms |
| Calling out misinformation |
| 1) personal data control; 2) safety on platforms from abuse & hate; 3) more diversity at all levels of administration, design, deployment, and use; 4) bona fide broadband access for all involved in k-12 and higher education; 4) more diversity in service providers; 5) put and keep human rights & ethics in the forefront; |
| Linked data, open data, open science |
| Decentralised Power, Personal Data Control, Open protocols |
| data commons, community driven data initiatives, non-corporate models of data sharing |
| Different content-surfacing algorithms, trusted information channels, decentralised power. |
| Restructuring of Information Flows, Group Data Control, Competitive Digital Markets, Democracy Enhancing Digital Agency |
| Several structural, related, issues: 1) Rethink norms: A policy framework for a rights-based approach (cf. Zuboff 2019: epistemic rights); 2) Rethink governance: a structured, sustainable and impactful framework of multistakeholder governance; 3) Rethink decision-making: an approach to the Digital Welfare State that *prioritizes* the underserved (cf. UN 2019: A/74/48037) . |
| Digital public service; communities/community voices |
| I think that it should be said more about Sustainable Internet, Media and Information Ecology, Data Privacy Challenges. |
| public service objectives, trust, disintermediation |
| sustainable internet, trustworthy info flows |
| community ownership, pluralistic design epistemologies |
| Decentralized Power, Community owned networks, Sustainable Internet |
| Continuing lag in proficiency and skills (thinking about older adults, those with disability, etc); Better vision of social technologies to combat loneliness and social isolation; Stronger training in data ethics |
| sustainable Internet, especially mobile & Internet of Things<br>digital inclusion<br>alternative models of data governance for non-personal as well as personal data |
| Trustworthy Information Flows, Personal Data Control, Power Concentration |

| |
|---|
| 1. Why 'human centered' if there are already frameworks like human rights, that have also already been codified for the Internet (such as through the UN Guiding Principles for Human Rights, RFC8280, etc)<br>2. Protocols and human rights considerations, norms based Internet routing<br>3. How to embed structural human rights considerations in Internet governance and standards institutions |
| Availability<br>Transparency |
| 1) Research on representative organisations who can collectivise personal data in the interest of publics;<br><br>2) Infrastructural perspectives on interoperable data ecosystems and how companies open/close certain data points for exchange with personal data infrastructures<br><br>3) Moving from interoperability as a competition issue to how interoperability brings about changes of professional norms and practices |
| gender issues, different ways of appropriating digital technologies during the Covid19 pandemic, social and economic (in)equalities, |
| Measure of online participation inequalities, digital literacy, user engagement in design and policy framing |
| environmental impact of internet infrastructure (data centres), transparency and public accountability of emergent data infrastructure part of the internet backbone (again, data centres in particular) |
| 1. Public service algorithms 2.0<br>2. Publicism vs populism<br>3. The role of AI – biases, ethics and the battle of technologies<br>4. Consumer needs and demands in 2030<br>5. Who owns the data and who will own the platforms?<br>6. Robot journalism and CGC<br>7. Synthetic media |
| Sustainable Internet, anti-racism and gender equity online |
| Below in order of importance in my view:<br><br>Transparent Business Models,<br>Misinformation and Polarization,<br>Regulation,<br>Technology is only enabler (but is not the solution),<br>Role of innovative users,<br>Business value,<br>Role of social media technologies,<br>Sustainability |
| data protection, freedom of speech, consumer rights |
| Equal participation and creativity opportunities for all; Bottom-down and user-tailored design; Anti-commercialisation of technological tools, content and services. |
| Algorithmic transparency |

| |
|---|
| 1. Accountable infrastructures<br>2. Trustworthy governance<br>3. Everyday security for individuals, communities, and organisations<br>4. Understanding infrastructural power as a sociotechnical construct that will always accrue to institutions, as much as to "decentralised" communities |
| ethical data practices, algorithmic fairness, privacy by design, respect for vulnerable communities |
| Trustworthy Information Flows, Personal Data Control, Power Concentration |
| Data Justice, environmental sustainablity, demonopolization or breaking up of large overly powerful corporations like Facebook, appstores have way too much power and that is not OK |
| AdTech, alternative platform models, content moderation |
| targeted advertising, data portability, data ownership, facial recognition, telemetric recognition |
| dataveillance and privacy; algorithmic discrimination |
| Transparent Algorithms |
| Operationalising AI Ethics, AI/Tech and accountability, Alternative business models |
| Future of Intelligence; Accessibility; (Investigating) military uses of AI |
| Trustworthy Information Flows, Personal Data Control, Power Concentration |
| decentralized power, alternative business model, users' right to opt out for data surveillance, environmental impacts of data banks |
| Constraining the Power of Big Tech |
| Human-Technology Symbiosis; Human-Environment Interactions; Ethics, Privacy and Security; Well-being, Health and Eudaimonia; Accessibility and Universal Access; Learning and Creativity; and Social Organization and Democracy. |
| transnational surveillance regulation; strong ethics/legal frames; education |
| Personal Data Control |
| Sociality (social connectivity platforms, not social media?), Language and Accessibility, Governance and Decentralized Power |
| Trustworthy Information Flows, Personal Data Control, Power Concentration |
| Freedom of Information, Transparency, Reducing the Presence of False Actors (nots, etc) |
| I think that trustworthy information flows are important as well as fighting cyber criminality as these topics potentially harm societies. Furthermore it is important to me that I know where my personal data is stored and how it is processed. Also the issue of how to deal with reluctant information and dataflows or how to handle big data is important, also in terms of sustainability. Social inclusion is also an issue meaning that everyone should have the same access or access at all. |
| Teaching being critical about information, internet on green energy, going against shitstorms |
| anti-racism, intersectionality, feminism, solidarity |
| Ethics, Social Movements, public Participation |
| Personal data, deepfakes, decentralize power |

| |
|---|
| Ethics Ai |
| material redistribution of the resources accrued by social media mega corps |
| Internet as Public Utility, Ubiquitous Broadband, Decentralised Power, Platform Regulation |
| - Training in order for users to understand the functionality and closeness of internet most popular platforms; |
| Constraining Power of Big Tech |
| 1. limiting digitalization and computer mediation to areas where they are absolutely necessary (abandon techno-optimistic mindset and narratives, truly respect the choice to limit or avoid usage of ICT technologies) 2. supporting work and leisure routines rather than breaking them; 3. ensuring backwards-compatibility of software, services, and hardware to respect the underpriviliged 4. prioritizing software and hardware stability over never-ending upgrades (no planned obsolesence, limited subscription software licensing); 5. building intuitive no-nonsense interfaces; 6. maintaining transparency of services and algorithms. |
| Sustainable internet |
| 1. Empowering local distributed organisation<br>2. Clear guidelines for emotional and experiential design<br>3. Decoupling of tracking from use |
| Increased diversification of digital platforms to enable movement away from the current structure of platform oligopoly. |

# Annex 2: Quiz 1 & 2 questions and responses

## Quiz 1

| **Question: Which internet-related technology or technologies will be predominant in our daily life in 2030?** |
|---|
| live interaction related tech |
| blockchain |
| voice command, smartphones or handheld devices with small screens still used |
| AI-driven personal assistants |
| online communication channels of various types |
| algorithms |
| agile mobile reconfigurable personalized networks |
| Smart homes where most technologies will be integrated |
| Hard to predict a platform, but it will be mobile-oriented and probably focused on video |
| Internet of Things; we won't see what is predominant |
| XR- technologies |
| teleconference meetings |
| Cyber security |
| In which countries? For which groups of people? This is a difficult question. Perhaps: facial recognition, location tracking, an intensification of current privacy-violating trends. |
| hmm... more intense and integrated forms of social media |
| video calls, automatic translation tools, social chat bots |
| social media, various platforms for news and entertainment; as well as platforms for communicating. also I believe many additional technological changes will be brought forward to the education sector |
| Still mobile phones, because that's been a constant in the last decade. |
| Zoom, email, Google Hangouts, Twitter |
| email |
| comunicação |
| Augmented Reality |

| |
|---|
| Various forms of location-enabled mapping interfaces (google maps, but also Deliveroo, Uber, etc). |
| health tech, facial recognition |

| **Question: When I think of the direction in which internet-related technologies are going, I am afraid that in 2030…** |
|---|
| We are ever more balkanized |
| arbitrary rules |
| everything will be commercialized, and based on the US or Chinese cultural values |
| data surveillance will be even more normalized |
| a lot more will be commercialized and in the hands of a few dominant (US) companies |
| we will not know or understand how algorithms are shaping everyday decision-making |
| there will be no space for communication that is not monitored by government, law, advertisers, and other shady actors |
| Privacy will be a thing of the past |
| There will be more disinformation |
| We will have greater inequities and more frequent climate-related disasters and no privacy as we know it today |
| there will be social segregation based on your data and profile |
| more commercialized |
| Privacy will be eradicated. |
| See above. I worry that we will be increasingly individuated. |
| It will be even more commercialised than it is now |
| We will not focus on being present and listening |
| we still talk about the surveillance capitalism and privacy issues |
| EVERYTHING will be connected and there will be no opting out. |
| Large technology conpanies will strengthen their position, and limit any community based alternatives |
| we will lack basic privacy and the feeling of personal security |
| Se torne um meio de manipulação em massa, perdendo seu teor revolucionário |

| |
|---|
| That artificial will replace the real interactions, and we will not be able to recognize what's fake. |
| There will be no option to get "off the grid" rather than complete non-participation in public, social and economic life. |
| the internet will remain as centralized and commercialized as today. |

| **Question: I think in 10 years, the main problem around social media will be related to... (The options below are just some examples, we encourage you to come up with your own response)** |
|---|
| A lack of freedom of speech |
| digital-capitalism and enforced individualism |
| concentration of platform power, shaping of public discourse accordingly |
| data harvesting & privacy |
| Algorithmic manipulation, commercial interest of selected platform providers |
| insular communities, invisible profiling |
| lack of freedom of movement and inquiry because of surveillance chilling effects |
| Echo chambers and political polarisation |
| The spread of fake news |
| Hatespeech and discrimination |
| A lack of freedom of speech |
| The spread of fake news |
| The spread of fake news |
| Fragmentation of social media platforms |
| Greater inequalities in terms of who can be seen and who benefits from platforms (algorithmic bias) |
| Overflow of information |
| problems of data discrimination and datafication in general |
| Echo chambers and political polarisation |
| Hatespeech and discrimination |
| A lack of freedom of speech |

| |
|---|
| Hatespeech and discrimination |
| The spread of fake news |
| Attention harvesting, particularly in relation to labour and monetisation issues (e.g. content production and monetisation) |
| content moderation + AdTech |

| **Question: To combat mis- and disinformation, we should prioritise... (The options below are just some examples, we encourage you to come up with your own response)** |
|---|
| Counteract with accurate, factual information |
| break up big platforms |
| Counteract with accurate, factual information |
| Counteract with accurate, factual information |
| algorithms that prioritize values that are meaningful--not interactivity, popularity, or presence on the platform |
| better education in not just critical skills but also tolerating difference |
| A better understanding of why people share fake news |
| A better understanding of why people share fake news |
| A better understanding of why people share fake news |
| A better understanding of why people share fake news |
| A better understanding of why people share fake news |
| A better understanding of why people share fake news |
| Public education |
| All of the above! Plus a removal of (financial/career) incentives to gain visibility via sharing mis- and disinformation |
| Educate people to critically evaluate what they read |
| media literacy and general awareness in the public - deal with the issues in the society that are not directly related to fake news and polarisation |
| A better understanding of why people share fake news |
| Legislate social media giants the same way new oganizaitons are legislated |
| Counteract with accurate, factual information |

| |
|---|
| Development of fake news detection algorithms |
| Development of fake news detection algorithms |
| A better understanding of why people share fake news |

| **Question: When I think of the direction in which AI is going, I hope that by 2030... (The options below are just some examples, we encourage you to come up with your own response and add to 'other')** |
|---|
| Reduced inequalities globally |
| i don't think it will manage to do any of those things |
| Reduced inequalities globally |
| I guess by 2030 the progess in all these fields will still be rather little. But I''m hoping for less inequalities |
| Cured most diseases |
| we have excellent personalized medicine |
| Cured most diseases |
| we will have learned to understand and control AI! |
| We'll have managed to slow down/resolve climate change |
| We'll have managed to slow down/resolve climate change |
| Cured most diseases |
| Reduced inequalities globally |
| Reduced inequalities globally |
| Reduced inequalities globally |
| We'll have managed to slow down/resolve climate change |
| these three options are a bit too grand, i believe we can try to deal with all these things, but not managed to get rid of those problems entirerly - that would be too technologically deterministic view |
| We'll have managed to slow down/resolve climate change |
| Reduced inequalities globally |
| won't yet live in a police state |
| We'll have managed to slow down/resolve climate change |

| |
|---|
| We'll have managed to slow down/resolve climate change |
| We'll have managed to slow down/resolve climate change |
| Reduced inequalities globally |

| **Question: When cybersecurity and decentralisation of the internet come into conflict, I think we should prioritise…** |
|---|
| Decentralisation |
| Decentralisation |
| i don't know |
| Decentralisation |
| Decentralisation |
| strike a balance -- neither is a perfect model |
| mesolayers of community organization and governance |
| Decentralisation |
| Decentralisation |
| Decentralisation |
| Decentralisation |
| Cybersecurity |
| Decentralisation |
| This is a false dichotomy. There are always centers of power, the problem is how we hold them to account. |
| Decentralisation |
| Cybersecurity |
| Decentralisation |
| Decentralisation |
| Decentralisation |
| no answer |
| Cybersecurity |
| Cybersecurity |
| Decentralisation |

| |
|---|
| strike a balance |

| **Question: When data privacy and data sharing for social good come into conflict, I think we should prioritise…** |
|---|
| Data sharing |
| Data sharing |
| Data sharing |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Data sharing |
| Data sharing |
| Privacy |
| Privacy |
| Data sharing |
| Data sharing |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Privacy |
| Data sharing |
| Privacy |

## Quiz 2

| **Question: I think in 10 years, the main problem will be…** |
|---|
| algorithmic inequality, data colonialism, data capitalism |
| Large tech companies controlling more aspects of our lives, and becoming so essentialthat they are able to water down all regulations |
| Ubiquitous surveillance, unequal impacts of predictive analytics |
| Privacy issues and Decentralizing the Internet |
| Further monopolisation of infrastructures by private companies, and further fragmentation between different countries (i.e. USA/China) |
| Everything connected to the internet with little ability to opt out. |
| Privacy |
| even more unequal access to information on the Internet |
| Climate change-related environmental issues that exacerbate economic divides. The rich survive while the poor suffer. |
| that the automated media or subject (Andrejevic) will take over and end the democratic rights that we have had |
| Climate change (so, sustainable computing is a priority) |
| power imbalances due to data collection and aggregation |
| technology-induced psychological disorders stemming from increasing social isolation and computer mediation of everything - for the majority of less priviliged people |
| tailored suggestions for reading material / bying things / information that affect the freedom of choice by not displaying a neutral selection |

| **Question: Which values should we put at the core to ensure this scenario does not become a reality, ensuring a progressive and human-centric development and widespread introduction?** |
|---|
| more diversity in top tiers of decision making, more humanities, social theory and ethics education for computer scientists |
| Regulation of large tech |
| autonomy, dignity, human-flourishing |
| Legislation and Redesigning the internet |

| |
|---|
| Freedom of access, data privacy, anti-commercialism/privatisation |
| Transparency that allows informed human agency/choice |
| I feel that more than values we should teach people how to protect their privacy, and how to be aware of the consequence of sharing too much |
| transparancy (of data sources, of information sources, of algorithms), equal access opportunities (quite difficult across countries and their different regimes, though). |
| Equal rights of representation across national and economic barriers |
| rights to the access of information technology, rights to understand how it works, rights to the access to reliable information, rights to manage the information environment including your data, rights to personal privacy |
| Public deliberations on deployment of dangerous technologies. Include environmental costs in technological assessment. Parallel to that strive for more transparent and less personal-algorithms-mediated discursive sphere, where experts could present their views on developing issues of the days to a more civically engaged public |
| personal autonomy - which means the ability of individuals to see, correct and contest the data that is gathered about them |
| do not put all eggs in one basket' of digital technologies; ensure people have options to work and spend their free time with limited usage of digital technologies |
| freedom of choice, equality not only before the law but also before the internet |

| **Question: Which regulatory approaches and policies do we need to ensure these values stay a central part of the future internet?** |
|---|
| i don't know |
| Breakup of large tech due to monopolistic practices,<br>Regualtions need to be inclusive of anti-discriminaiton<br>The regulations have to have teeth and financial consequences |
| embedding and enforcing Universal Declaration of Human Rights (UDHR) within digital infrastructures |
| Having international laws on privacy and other internet issues that are ratified by different countries |
| Further regulation at the international level to control monopolisation and also abuses by governments |

| |
|---|
| Unsure - limits on big tech, but also not allowing governmental takeover of data & tech. |
| Educational policies |
| International agreements to free access to information |
| Access guarantees |
| We need regulation on the national and international level concerning the transparency and accountability of tech companies and regulation also on the transparency of governments and their actions in the field of security and surveillance |
| Decoupling of value from engagement built on outrage and emotion (for example, by penalising corporations on vertical integration of content, measurement and advertising). Antitrust legislation. "Green tax" on data processing. |
| stronger privacy regulatio s |
| it is difficult to say, but top-down approaches may not work here; one option would be to encourage the industry to drive this process. Currently, big companies seem to have recognized the need to let people track their usage of technology, and they may be more successful in this than governments or civil society organizations |
| Laws for clear ad / tailored suggestion labeling, an easy button to recline tailored suggestions |

| **Question: Which business models and technologies do we need to ensure these values stay a central part of the future internet?** |
|---|
| tax the giants, tax the rich, promote capitalism of sufficiency not capitalism of exponential growth |
| Need more community based technology development mercome network effect.<br>Peer to peer based social media platforms exts suchn as Aether https://getaether.net/, but the large social media platforms have hard to overcome<br>Similarly peer to peer Mesh networks for internet access exist. e.g. https://guifi.net/<br>Governments need to support more peer to peer technology business models, whether it is social media platforms of internet access models |
| decentralization, transparency, user-control |
| A human centred business approach on technologies |
| Open source, grassroots, community-owned |

| |
|---|
| Breaking up big tech as first step, but that leads to rise of new big tech companies. Permanent global competitiveness rules seem unattainable. End capitalism? I don't know. |
| Augmented Reality |
| main challenge is that currently often use of personal data is a business model, so I guess this needs to be resolved |
| Personal communication devices with access fees based on ability to pay, and minimal access available universally. |
| Philip Napoli: User data should be turned into a common resource |
| Hyper-local, decentralised federalised data repositories. Publicly funded (supra-)national platforms. |
| someone in our last session mentioned expanding the ability to choose between algorithms. this might be a good strategy |
| perhaps private companies should lead. |
| transparency of algorithms that are at work |