Human Rights in a Digital Age

24 May 2018
Geneva
Housed at Essex University’s Human Rights Centre with partners worldwide, the Human Rights, Big Data and Technology Project considers the challenges and opportunities presented by big data and associated technology from a human rights perspective.

Our aim is to map and analyse the challenges and opportunities of the use of big data and associated technology from a human rights perspective, to consider whether fundamental human rights concepts and approaches need to be updated and adapted to meet the new realities of the digital age, and to develop good practice guidelines and propose regulatory responses and remedies from a rights-based perspective.

The Project addresses issues ranging from the use of data-driven technologies by police forces to the use of big data to hold duty-bearers to account, considering a spectrum of rights implications, regulation and remedies. Our team is comprised of interdisciplinary researchers and specialists, enabling the Project to draw on a unique breadth and depth of experience in addressing the protection and promotion of human rights in an era of big data.
OPENING REMARKS AND BRIEFING ON THE HUMAN RIGHTS, BIG DATA AND TECHNOLOGY PROJECT ................................................................................................................................. 4
KEYNOTE: PEGGY HICKS ........................................................................................................................................................................... 6
PANEL ADVANCING HUMAN RIGHTS IN THE DIGITAL AGE ........................................... 7
C H R I S E A R N E Y .............................................................................................................................................................................. 8
P H I L I P P E S T O L L ............................................................................................................................................................................. 9
D E L P H I N E V A N S O L I N G E ................................................................................................................................................................. 10
D I S C U S S I O N ..................................................................................................................................................................................... 10
RISKS AND CHALLENGES TO HUMAN RIGHTS IN THE DIGITAL AGE ......................... 13
B A R B O R A B U K O V S K A ................................................................................................................................................................. 14
T O M A S O F A L C H E T T A ................................................................................................................................................................. 15
D A V I D R E I C H E L ........................................................................................................................................................................... 16
D I S C U S S I O N ..................................................................................................................................................................................... 17
RESPONDING TO RISKS AND CHALLENGES: HUMAN RIGHTS FRAMEWORKS IN THE DIGITAL AGE....................................................................................................................... 20
J E A N - Y V E S A R T .............................................................................................................................................................................. 20
N I G H A T D A D .................................................................................................................................................................................... 21
D R . H A N N A H R A U ........................................................................................................................................................................... 23
G R A H A M W E B B E R ........................................................................................................................................................................... 24
D I S C U S S I O N ..................................................................................................................................................................................... 25
CLOSING REMARKS .................................................................................................................................................................................. 28
Opening Remarks and Briefing on the Human Rights, Big Data and Technology Project

Robert Roth, Director of the Geneva Academy of International Humanitarian Law and Human Rights and co-host to the conference, welcomed the participants and opened the conference.

Lorna McGregor, co-director of the Human Rights, Big Data and Technology (HRBDT) project, introduced the project by explaining that the project was set up in 2015 with a £6 million funding by the UK Economic and Social Research Council and the University of Essex. The team includes 37 researchers across seven disciplines: computer science, sociology, criminology, economy, law, philosophy and political sciences. The project is based at the University of Essex, with a number of researchers based externally at the Geneva Academy, the University of Cambridge, Queen Mary University of London and Eyewitness Media Hub.

The research focuses around two key questions:

1. What are the opportunities, and risks, for human rights generated by big data, artificial intelligence and smart technologies?
2. What are the effective responses to protecting against the risks and enabling the opportunities of big data, artificial intelligence and smart technologies?

The consistent message of the HRBDT project is that the international human rights framework must be at the heart of shaping those responses. The first step is to research and document the risks caused by big data, artificial intelligence and smart technologies to human rights. The project is based on empirical research, but also includes engagement with law enforcement agencies and businesses working with big data and technologies at the operational level. It looks at the practice of businesses, the relationship between the state and businesses and inter-state relationships.

When assessing risks to human rights, the right to privacy is key. Nevertheless, all human rights are being looked at, as the HRBDT project has shown that all rights are at risk, whether big data, artificial intelligence and smart technologies are being used for good, bad or neutral purposes. Opportunities for human rights generated by big data and technologies are also being studied. The HRBDT research team rejects the idea of trade-offs between rights, and is working closely with UN agencies, states and civil society to look at ways in which big data and technologies may offer opportunities.

Apart from looking at risks and opportunities in general, the research project looks in detail in three areas of work.
1. How to use big data and technologies to document human rights violations;
3. How to use big data and technologies to enhance humanitarian responses to forced displacements; and
4. How to use big data and technologies to protect the right to the highest attainable standard of health.

The project makes the case for the value of the human rights-based approach to these issues. The research undertaken also interrogates the underpinning concepts of human rights and aims at reframing these concepts (e.g. consent, identity, democracy) to further ensure the protection of human rights. It looks closely at how to operationalise the right to a remedy; it also focuses on regulation to ensure that human rights are protected both in law and in practice.

The project hopes to give practical resonance to our research and to support states, UN agencies and civil society in their work. The prime target for engagement is the UN space, because the international institutions in Geneva are the focus point for human rights at the global level. The Universal Periodic Review process also allows an entry point for engagement at the national level.

The HRBDT project has had the opportunity to engage with many actors, through submissions, participations in UN events, side-events and expert-meetings, such as the UN Business and Human Rights Annual Forum. It extends its work outside the UN space where doing so can add value to the work undertaken. One example is its engagement with national actors on the UK.

Lorna McGregor concluded the presentation of the HRBDT project by saying that this conference will be an opportunity to engage further with different actors, learn from them through panels and discussions, and will maybe lead to future collaboration with some of the actors present at the conference.
Keynote: Peggy Hicks

Peggy Hicks invited the audience to see technology as a drug with life-saving properties that can however turn dangerous. She divided her intervention in two parts, addressing first a selection of substantive key challenges, while emphasizing that there were manifold other risks that needed to be discussed.

The three baskets of key challenges are portrayed in the table below.

<table>
<thead>
<tr>
<th>Basket</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to Privacy</td>
<td>Key concerns and questions are:</td>
</tr>
<tr>
<td></td>
<td>- What is the place of privacy in data and information systems?</td>
</tr>
<tr>
<td></td>
<td>- How do we view privacy?</td>
</tr>
<tr>
<td></td>
<td>- We must think of the severe impacts not only on individual users but also the impacts on civil society and human rights defenders particularly</td>
</tr>
<tr>
<td>Freedom of expression</td>
<td>- Hate speech can be lethal, and messages of incitement and hate speech are excessive online, but regulators can be too quick to &quot;use the sledgehammer&quot; (e.g. German Network Enforcement Act)</td>
</tr>
<tr>
<td></td>
<td>- The &quot;sledgehammer approach&quot; however incentivises businesses to over-block consent and therefore limits freedom of expression. We must maintain the fundamental protections for protected speech.</td>
</tr>
<tr>
<td></td>
<td>- Authoritarian regimes could use the cloak of speech restricting measured to block information from opposing ideologies as opposed to responding to threats of terrorism of incitement to violence.</td>
</tr>
<tr>
<td>Right to equality and non discrimination</td>
<td>- Algorithmic bias is not only under-regulated but also insufficiently understood. The impacts of AI and big data may be long term and can have serious consequences on human rights. Because of the fast paced nature of technology development we must ensure that they are not discriminatory</td>
</tr>
<tr>
<td></td>
<td>- Toronto declaration- set of principles that will protect the principles for non-discrimination and guide companies looking forward. risks of discrimination must be detected and responded to as early as possible.</td>
</tr>
</tbody>
</table>


Ms. Hicks dedicated the second part of her talk to the gaps, some of which may amount to critical failures, in the processes needed to address these challenges.

She identified the role of the private sector as the “driver of the digital age” noting that one of the great advances in human rights of the past decade has been to address the role of businesses in respecting human rights: the UN Guiding Principles on Business and Human Rights (“UN Guiding Principles”) have been crucial to providing the global standards to create greater accountability. Applying these principles in the digital age alongside new guidance tools for tech related sectors is a way to balance responsibilities and ensure human rights are respected.

Ms. Hicks also pointed to three challenges for regulating the digital space:

1. Regulation by States can be too slow
2. Approaches to regulation are insufficiently flexible
3. More expertise is needed

In this context, she referred to the need to develop alternative models of regulation. While there are efforts at better regulation greater understanding of the problems is needed in order to develop adequate regulation. This year, being the 70th anniversary of the Universal Declaration on Human Rights, can remind us that we do have the basic tools and principles upon which to build regulatory responses. Human rights can provide the foundation for addressing a host of complex issues and can be adapted to multiple situations and contexts. However, to support this we must have cross sector knowledge exchanges to break down barriers and create cooperation which ensure everyone is on the same page. We must target those who are not yet included in the discussion with particular focus on the global south. Some stress that multilateralism is no longer a solution, but discussion of the breakdown of multilateralism could not come at a worse time for the big data and new technology related issues. We need to find a way to address these issues across platforms and jurisdictions.

Peggy Hicks concluded by saying that we may be at a tipping point. If we fail to engage quickly, to both understand and build up our ability to address the challenges posed by new technology we could see real regression. At the same time, if we can manage to harness technology to protect rights, to demand equality and to end discrimination, our digital advances could be what we need for building better societies.

Panel Advancing Human Rights in the Digital Age

This panel on “Advancing Human Rights in the Digital Age” was moderated by Sonia Bhalotra, Work Stream Deputy on health and human rights in the HRBDT Project. Bhalotra spoke about her work in the project looking at econometric techniques to
examine policies related to universal health coverage. She proceeded to introduce the speakers on the panel and invited them to give their interventions.

Chris Earney

Chris Earney, head of Innovation Service at the United Nations High Commissioner for Refugees (UNHCR), began his presentation by introducing the UNHCR innovation service and their work around competency and culture building around innovation. He emphasized that strong messaging on diversity and inclusion must underpin innovation. UNHCR supportfield operations through innovative practices while being conscious of the differences between innovation and technology, as these do not necessarily converge. UNHCR very much looks at the future to understand what a future in terms of protection of displaced population means and how to prepare for that future. Human Rights in the digital age presents risks, questions, opportunities and requires dialogue with a range of different partners to understand the implications of new technologies on the people UNHCR is interested in supporting.

Earney emphasized four main points: firstly that new technologies do not change the importance of privacy. The people they are working for, and with, are extremely vulnerable and privacy must remain central. The question of how to apply their rights in a digital setting however remains a challenge.

Secondly, he demonstrated the opportunities that technology presents in humanitarian contexts by predicting displacement with high levels of accuracy. This opportunity however brings with it new questions if this information changes obligations of a variety of actors in regard to the local context. New technologies and survey data also allow UNHCR to understand sentiments of host communities such as in Greece, France and Germany into which displaced communities are moving. This additionally demonstrates the wide scope of opportunities that new technologies present in the present and also for the future. Earney stated that UNHCRs approach entails "preparing for that future by using the tools presented in the digital space".

Thirdly, Chris Earney emphasized that data protection must remain central to our endeavours in the digital age. Data breaches are still too common and the GDPR it is an opportunity to drive up organization standards to further secure data. Earney mentioned that he believes recognition of weaknesses to be an aspect that requires
improvement in the humanitarian sphere. It is insufficient to just develop innovative systems. They must be secure and must have taken into account potential risks.

Finally, Earney warned of the danger of binary conversation of human rights in the digital space which distinguishes on one hand between benefits for humanity but on the other detriments to humanity. We must understand both sides and understand the potential and risks associated with new technologies and the digital age and find ways to use the digital for good.

He concluded his presentation by stating that “we need to be humble but also bold in our actions.” We need to engage with a wide variety of actors and we must make sure the future of technology is one that has continued inclusion and involves end users in the creation, policing, and iteration of those technologies.”

**Philippe Stoll**

Philippe Stoll, Head of the Communication Policy and Support Unit at the International Committee of the Red Cross (ICRC), began by presenting ICRCs thinking around how to improve the capacity to engage with affected people through technology. New technology tools can be enablers of new types of engagement and communication and they can sometimes push affected people to ask and to answer questions thus empowering them. ICRC’s work is not about imposing technology on communities. It is host communities that are already using new technology and online mediums to reach out to them. This sometimes has much to do with how comfortable people are in some online spaces and can be more open to giving testimonials in some contexts.

New tech also enables new tools for transparency and accountability and activities can easily be put under scrutiny. New tools also aid their services and efficiency such as Google Open Street map developed for people to see where water would be distributed so people can come directly to pick up locations. This illustrates how one can raise awareness so that the use of data is optimised through new technologies. This offers enormous opportunities for reaching out to new communities and ensuring transparency and accountability.
Delphine van Solinge

Delphine van Solinge, a protection advisor for digital risks for populations in armed conflict for the ICRC, followed Philippe Soll’s presentation emphasizing the risks that new technologies present. Digital technologies are neutral things whose positive or negative connotation is determined by who uses it and for what purpose. As Stoll indicated for ICRC digital connectivity and access to information has made their organisation and the beneficiaries better connected and they bring many advantages in the delivery of humanitarian services and assistance.

While there are many benefits, the risks must also be considered. The use of technologies by parties to the conflict for different purposes needs better analysis and understanding. Parties to a conflict can track individuals, they can allow or promote the spread of disinformation or hate speech leading to adverse consequences for individuals and/or communities caught in violent environment. Considering the two extreme purposes that technology can fulfill, both positive and negative, Delphine van Solinge stated that understanding of technologies and their possible use is needed to ensure mitigating potential no harm against civilian populations in armed conflict or other situations of violence. She added that it’s also important to understand the role and responsibilities of different actors in relation to this.

The ICRC has for two years been working on a handbook on data protection in humanitarian action. This is being done in collaboration with humanitarian organisations and companies working on technology. Additionally they are working to optimise securing their information. When carrying its humanitarian mandate, the ICRC is collecting information on very vulnerable groups of people with the sole objective to better protect and assist them. Securing their personal information is key to ensuring no adverse effects will be felt by them.

Discussion

After the presentations the moderator, Sonia Bhalotra, opened the floor for questions.

One attendee expressed concerns about the use of criminal law for and criminalisation of certain types of conduct such as drug use, sex work or HIV transmission. In certain areas, the application of criminal law can be inappropriate, and decriminalisation should be promoted. The use of surveillance for criminal law
enforcement can have an impact on the right to health in cases of criminalisation of these conducts. The panel remarked that criminalisation of some conducts inevitably leads to pushing it underground, as has been observed around 1980 and 1990 with HIV/AIDS. Criminalisation by some countries of certain conducts is inconsistent with human rights law for these reasons. It was then asked whether big data could help capture the deleterious impact of that criminalisation in those countries by better tracking the damaging impact of such criminalisation.

A second concern raised related to the discovery that for a journalist in Switzerland it is difficult to obtain information and statistics about any issue pertaining to justice and court cases. As a result, it is difficult to be informed about pressing issues related to the judiciary system. The attendee made the point that it affects many aspects of civil life, and yet conferences rarely touch on these issues. In response, the panel observed that whereas there are very specific problems in Switzerland in access to information on case-law, at least there is an existing system in place where these cases are dealt with. There is a procedure by which one can raise a concern and get it processed. In many crisis situations around the world, these mechanisms do not exist. In some cases, there is no mechanism by which to challenge the way your personal data is being used, after a person has handed over personal data as prerequisite to be granted proper protection. For example, the UN and governments share information including personal data as part of the Global Compact on Refugees, but there is no recourse for individuals whose personal data are being shared. In the example given about Switzerland, individuals have an avenue to protest. In many contexts addressed by the panel, such avenues are non-existent.

Attendees then brought up the idea of ‘do no harm’ in relation to data collection and analysis. How does it work in practice? The panel made clear that when dealing with data, the first concern is to not add vulnerabilities to the ones already existing. The first thing before beginning to collect data is to make sure that the system in place to collect them is adequate with how people functions and how they will access the services. This means that the digital divide and digital literacy of the targeted group must be taken into account when designing services.

The high confidentiality of the International Committee of the Red Cross (ICRC) with data is unlike many other organisations because of its core principle of confidentiality. Despite the necessity in humanitarian work to interact with other actors, sharing information and data remains a sensitive issue for humanitarian organisations, because confidentiality is one of the very fundamental foundations of their work, to gain the trust of the people it works with. To avoid sharing information that could be harmful, the question in mind when sharing data is whether doing so has an added value for the beneficiary. Nevertheless, the humanitarian sector faces an increasing necessity to work in more collaborative manners. So is the pulling together of resources, knowledge and processes, within limits. In that sense, the privileged position enjoyed by the ICRC in the humanitarian field must be maintained, for confidentiality to be sustained.
When working with data it is important to remember why this data is being collected and what will and can be done with it. The organisation must have a clear idea of how the data is going to be collected, managed, secured, stored and how it will give the person to whom the personal data belongs the possibility to have a say on what use is made of the data. One important question is who owns the data. The ICRC has developed a handbook on data protection, which provides guidance for NGOs working in the humanitarian sector to avoid doing further harm. It is important to always think one step ahead, but this is proving difficult given the rapid pace of technological advances in comparison to the slow pace of the humanitarian sector.

Another comment concerned how different sectors apply the question of big data and proportionality in very different ways to law enforcement. From this remark came two questions: how do institutions make decisions around the proportionality of privacy intrusion in conflict with the good outcome arising from the use of data? And is there any independent oversight of the quality of these decisions to use data?

One panellist expressed that the actors in the humanitarian field should constantly question themselves about their collection of data. In terms of oversight, the more organisations have external friends, partners, and colleagues interrogating the collection of data by the organisation the better. Once again, the process of data collection and processing must be clear especially to the person providing the data. An organisation must not impose a decision on the individual. There are also cases where the person consented to their data being used but the organisation, in assessing the risks associated, decides against it because the consequences to the individual would be too risky. It must also be noted that there are different levels of transmissibility of data according to the source providing it, whether it is a community or an individual.

A further comment coming from the panel noted that UN agencies may be afraid that using the language of human rights will lead to them being assimilated to accountability mechanisms, thereby deteriorating their relations with some actors. In reality, UN agencies use human rights to shape their policies and give advice on policies but without becoming accountability mechanisms. Policies will be better shaped if populated by human rights. There is no actual worry to have on this question. The panel made another remark about accountability, saying that if humanitarian organisations and UN agencies do not address the questions around big data themselves, other actors will step in. This can have the effect of further blurring the process of accountability and create more misunderstandings among the persons the humanitarian organisations are supposed to help.

One attendee wondered about ownership of data and the consent for using and sharing by the person whose personal data it is. The HRBDT project, for example, uses data from Brazil for academic research. How do individuals consent to such use of their data? How do the different actors deal with similar issues? Empowerment
and ownership go together. If there is an objection to Facebook sharing its data with Cambridge Analytica, shouldn’t there be a similar objection to academic institutions using data without the consent of individuals who provided it?

The panel responded by saying that the data used in the research about Brazil was available for use and is anonymised. Their use in the research in question leads to benefits in terms of evaluating the programmes implemented by the government and allow for better targeting.

Speaking from the perspective of an academic researcher, one attendee noted the advantages of administrative data, like those used in the research on Brazil for an academic researcher. It increases the possibility of accountability. One area where it is very difficult to undertake such a work is the judicial system. However, even courts decisions and litigants can benefit from administrative data. As shown by a recent decision by the U.K. Supreme Court, (The UNISON case) discrimination can be established by relying on administrative data. While there are risks associated, the benefits are very important.

The next question concerned developing countries where no data protection laws exist, and government has access to big data. In cases where the population does not give consent for the use of their data and has no available mechanisms to bring up grievances about data breaches, how do agencies working in developing countries operate and what is their accountability procedure?

That data protection frameworks vary between countries was noted: where there is a weak protection, institutions have a responsibility to strengthen the protection. However, lack of protection at the national level is a concern. One way to improve the processes at the level of international institutions is to engage with those people the institutions are trying to help. Engagement with civil society must be strengthened. Furthermore, biometric data gives an opportunity to better understand people, their needs and what the protection outcome can be. Now, a humanitarian organisation produces a mass of big data every day. Many of it is never used. If a more efficient way to use data was found, humanitarian organisations could have a more important positive impact on human rights.

On this note, Sonia Bhalotra closed the panel session and thanked the panellists and discussants for their presentations and the attendees for their questions.

Risks and Challenges to Human Rights in the Digital Age

Vivian Ng, Senior Research Officer of the HRBDT project, moderated the second panel on risks and challenges to Human Rights in the Digital Age. Before introducing the panel she reiterated the importance of understanding that the risks associated with new technologies to human rights are manifold. For this reason we need to understand not only the gaps but also the challenges we need to urgently respond to.
Barbora Bukovska

Barbora Bukovska, Senior Director, of Law and Policy at Article 19, spoke about three key challenges and highlighted one key risk. The first challenge she addressed was problems with the internet infrastructure. The majority of the internet infrastructure is operated by private companies and they are clearly politicised in the role they play. The internet infrastructure provider often function with regional monopolies with very little pressure on buyers, sellers and substitutes, which given them massive economic and political power.

The second area Article 19 sees as a problem is how AI and decision making influence the way in which people exercise their right to freedom of expression. One of the key impacts is on media pluralism and diversity, which are essential to promoting freedom of expression. There is a limited number of digital platforms acting as conduits for hosting content online and these are usually opaque when it comes to their AI usage and process behind blocking content. AI also impedes on civic space which is physical and legal place where individuals practice their rights, and this is increasingly impacts by AI, particularly in smart cities.

The third challenge is influence of AI on transparency and access to information. AI is increasingly used to moderate user content and companies employ these systems without transparency. Increasingly the decisions are driven by AI systems and they have the ability to exclude critical information that allow governments to deploy AI systems without transparency. The increased privatization on censoring content is also a challenge. When individuals use social media platforms they do this on terms of a service adopted by companies. These are however designed to create an imbalance of power and typically stipulate a jurisdiction other than that in which the users are based.

Freedom of expression standards are also usually much lower than is permitted under international law, which is problematic. Some companies justify limiting freedom of expression to create safer online environments, however when talking about dominant media platforms it is evident that social media platforms do not rely on the principles of necessity and proportionality but more on the basis of propriety. There is also clear lack of accountability and transparency regarding how the terms and conditions are applied. There is also lack of procedural safeguards and remedies for removal of content. Finally, public authorities circumvent the rule of law by cooperating with companies and not rectifying the blocking of legitimate content by the company.
Barbara Bukovska concluded by asking whether it is realistic to ask companies to comply with international standards when they are not required to change the business model under which they operate undermining the basis of democracy. This is a question where more discussion is needed.

**Tomaso Falchetta**

Tomaso Falchetta, Advocacy and Policy Team Lead at Privacy International, presented on the challenges in relation to the right to privacy. He first identified the issue of the blurring of the distinction between the private and public space and what that means for the protection of the right to privacy. Both private companies and public authorities are arguing that information in public domain is not protected, but the implications for the right to privacy are profound. An example of this is smart cities. A smart city is tech intensive with syncing sources everywhere. These include CCTV but are much more invasive in terms of privacy. Data gathering can occur through free wifi networks, microphones, environmental monitors and more. Much of this data is transmitted without the involvement of the individuals concerned and the individual has little way to prevent this collection of data.

The second challenge is the protection of personal data with regard to big data and the difficulty of distinguishing between anonymous data and personal data. Computers are able to make predictions about our political views and sexual orientation based on other data that was collected. The problem with this could be that personal identity and personal information can be easily identifiable through publicly available information. Predictions are becoming more and more accurate and produce data that is actionable by companies and governments. The privacy implications of profiling and using data is not limited to commercial purposes and targeting via profiling can have serious human rights implications such as those related to access to public services, insurance and credit services, education and a whole range of human rights.
David Reichel, Research Officer at the EU Agency for Fundamental Rights (FRA), works on fundamental rights implications of artificial intelligence and big data – with the EU Charter of Fundamental Rights being the basis of their work. One fundamental right that is impacted on by new technologies, involving big data and artificial intelligence is non-discrimination. FRA has published a paper that deals with this topic[1] and is currently developing a project on artificial intelligence and fundamental rights.[2] Additionally, FRA has published a handbook of European data protection law, including updates of the new data protection reforms.[3]

Data and algorithms are increasingly used in different areas including policing, advertising, recruitment and elsewhere. Discrimination can occur when big data analysis and algorithms are used. David Reichel reiterated Article 21 of the EU Charter on Fundamental Rights, which states that “any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.” He outlined that inclusion of information relating to any of the grounds of discrimination in a data set is very likely, which is why we must remember that – if not properly checked – algorithms might discriminate. In 2016, 10% of enterprises in the EU said they use some kind of big data analysis, and for large scale enterprises this increases to 25%. Almost half of those that use big data analysis use geo location data and social media data. This is important because it can relate to the grounds of discrimination.

Discrimination in algorithmic decision making can occur in different ways. One example is the use of biased data for training algorithms. In addition, data may not only be inaccurate but also may not accurately representative the group for which it is being used for prediction purposes. This can cause different groups to be treated differently. When you are aware that outcomes may be skewed, algorithms need to be looked at – with a view to potentially altering them – so as to avoid discrimination.

There are possibilities for considering the ‘auditing’ of algorithms, which can be used to demonstrate the absence of discrimination. A difficulty in auditing algorithms, however, is the lack of transparency in creating these algorithms and the intellectual property rights involved. If the data or the algorithm is not accessible then effective auditing becomes a challenge. Not using any information on protected attributes is, however, not the “easy solution” as other ‘proxy’ information might be correlated with protected attributes. At the same time, information on protected groups – when looked at as aggregate data – might be needed to audit and potentially correct algorithms.

In sum, there is still much work to do in this field to understand and effectively respond to the potential for discrimination and the inaccurate use of data.

Discussion

After the panellists and discussants finished their presentation and comments, the moderator of the panel session, Vivian Ng, opened the floor to questions.

The first question to the panel brought up the idea of a licensing authority in the field of technology, similar to that for drugs and food. According to this idea, technological innovations and developments would be subjected to a social and human rights impact assessments and coupled with a licensing requirement of the product. The question remains as to whether such a mechanism is realistic. The panel began by reminding that at the moment, the human rights framework is the only existing tool, and that the data protection principles could be used to address many of the problems occurring in that field. The GDPR provides for specific cases the requirement of an impact assessment, with in mind the discrimination potential of a big data technology. Some of these data principles could be used for new technologies too. Also, there is an observable movement towards licensing and a regulatory framework.

What is missing at the human rights level is the development of the data protection aspect of privacy. The documents interpreting the right to privacy are too old and therefore do not do so, such as the General Comment of the Human Rights Committee on the right to privacy. Some initial steps have been taken, in the form of resolutions for example. Nevertheless, much is left to do, and it would help to have an assessment of technologies before their concrete application.

One question that arises in the hypothesis of a licensing authority is when in the process an impact assessment should take place? The difficulty is that the consequences of such technologies appear only at the stage of the concrete application of the technology. Some of these consequences are neither foreseeable, direct or intended. The question of temporality is central to the issue of testing the technology. The panel also stressed that the individual social location must also be
taken into account when establishing a process, because even if the process for data protection is fair, it may still reproduce the disadvantages already existing in the society.

The second comment to the panel concerned the use of the term ‘society’ in many of the presentations. What does ‘society’ mean? International human rights law is still stuck in the Westphalian paradigm, where only states have human rights obligations. Yet, technology does not care about this Westphalian paradigm. How can we deal with this model where the State is more or less irrelevant?

The panel responded by observing that data flows across borders and that the idea behind the GDPR was to have a focus on individuals irrespective on where the data was being processed, even if it was outside the European Union. Whether such a model can be applied universally is a massive question. What is certain is that there is recognition by States that data protection is an important topic. 120 countries around the world have introduced data protection legislation, even though these are not necessarily up to date or fully implemented. There are solutions to consider before concluding that states are not able to regulate around the question of big data.

The panel further insisted on the fact that States remain an important actor because they also carries positive obligations, which create a space of pluralism and diversity. They must foster an enabling environment where people are not limited to one source of information and one dominant actor. However, this does not mean that we cannot promote more flexibility in the way we approach regulation. Indeed, there is a dichotomy between, strong regulation from the State and voluntary compliance with human rights from companies. From the media perspective, the experience of independent self-regulation can also be highlighted. We can look at the different models in place and see how they contributed to human rights and also look at more creative regulations, fostering civil society engagement. The German model, for example, seems to have taken a step in that direction. Maybe some positive can come out of this model.

States should be the primary actors, according to the panel, because they also carry obligations to protect from third parties and other actors. International law is slow moving. It must speed up to finally acknowledge the massive role play of non-state actors and start attributing human rights obligations and responsibilities to these non-state actors. The system cannot work with a sole focus on States. The human rights framework is focused on individuals, but it also aims at protecting against abuse of authority. Therefore, international law needs a more nuanced approach to ensure this protection.

One attendee commented on the work of the Fundamental Rights Agency of the European Union (EU FRA) and expressed his opinion that the work of engagement by the EU FRA with other parts of the world should be more developed than it is at the time. By which the panel responded that EU FRA is an independent body, but
that it also must follow his mandate defined by law, according to which its role is to provide data and expertise in fundamental rights to the EU institutions and EU member states. The European Commission also works outside of the EU, but the disparities between the different regions and countries makes it difficult. Human rights in Europe are already at the very higher level, compared to many regions in the world. Opportunities for comparison are limited.

The last concern expressed in this panel session regarded cultural challenges in the field of big data and new technologies. Most panellists expressed the feeling that there were no real cultural challenges in terms of geographic differences. In any case, individuals as users have very limited choice, because of the dominance of some companies. The lack of possibility to use other companies’ services providing better protection of privacy gives a giant leverage to big companies such as Facebook and they can limit the choice of users with few consequences. If there was competition with other companies, human welfare and trust could become a concern of these nowadays monopolistic companies. The problem does not come from cultural differences, but from the imbalance of power between these companies and individuals. It is almost impossible for individuals to foster change effectively in this context.

The application of some of these technologies have expanded to settings where their use is completely unnecessary, such as biometrics data in schools for example. It creates and enhances an acceptance around these technologies by each and every one, with little resistance.

One challenge mentioned by the panel is the differences in approach by different disciplines, for example between computer scientists and statisticians. Interdisciplinarity and multidisciplinarity must therefore be fostered.

One member of the panel considered that there may be different sensitivities to technologies according to cultural differences. The most important elements to look at are the three following ones: (1) the visibility of harm; (2) the asymmetries between corporations and individuals in power and knowledge; and (3) the difference in impact at the generational level, with digital natives and younger generations being more affected by these technologies which affect how they socialise. The argument that people are willing to give up their rights and are not aware of these rights is wrong. The problem is rather that there is a dependence to these social media platforms for socialisation. Consent in such a situation is tricky.

Facebook is a very interesting example because it highlights the problem with the current framework. The onus should not be on the individual to manage their data. We must better look at the roles of the companies and states and at their responsibilities, because they are the ones properly capable of managing and protecting against harms. This focus on the individual, such as observed in the GDPR, is the fundamental flaw of the current approach. The idea of consent is
crucial, but every move on the internet translates into 25 to 30 decisions for the individual to make about personal data. It is an impossible task. This is why we must turn to corporations to enhance their responsibilities.

On this note, Vivian Ng closed the discussion and the panel session, stressing the need to work together in a multi- and interdisciplinary way. She finished by thanking the panellists and discussants for their very rich interventions and reflections.

Responding to Risks and Challenges: Human Rights Frameworks in the Digital Age

The final panel session welcomed experts representing different actors, from civil society to governments and corporations, for a discussion around the topic ‘Responding to Risks and Challenges: Human Rights Frameworks in the Digital Age’.

Sabrina Rau, Senior Research Officer in the HRBDT Project, began by reminding the participants that the previous panels had highlighted the opportunities and challenges raised by big data and associated technologies. She stressed the need for greater oversight, transparency and accountability and for a better understanding of the responsibilities of the different actors. She called for the present panel to discuss the solutions to these challenges, pointing out the three issues with traditional regulatory responses highlighted by Penny Hicks: these are too slow, they are not flexible and forward-looking enough, and they do not include sufficient expertise. The question of the distribution of responsibilities between the different actors is also a central one.

Jean-Yves Art
Jean-Yves Art, Senior Director of Strategic Partnerships at Microsoft, opened by alluding to recent press reports that Chinese authorities had used facial recognition technologies to arrest suspected criminals at the security gates of a popstar concert in China. Jean-Yves pointed out that the same technologies can be used to enable the arrest of political opponents but also help identify abducted children or reunite families in conflict zones. He observed how the same technology, depending on its use, can either have a very harmful impact on human rights or be helpful in upholding human rights. Tensions exist in relation to the use of these technologies.

He then talked us through the two sets of measures taken by Microsoft to address the human rights risks associated to the use of technologies. The first of these measures was the decision to ask the human rights consultancy ‘Article 1’ to conduct a human rights impact assessment of Microsoft’s artificial intelligence technologies at the conceptual level. The impact assessment was conducted in accordance with the UN Guiding Principles on Business and Human Rights. It aimed at identifying the human rights risks raised by artificial intelligence, and especially the causation element to see whether a link existed between Microsoft’s activities
and the human rights impact of these technologies. The impact assessment by ‘Article 1’ also made recommendations to address the risks associated with artificial intelligence.

The second measure taken by Microsoft was the implementation of the top recommendation made by the human rights consultancy impact assessment: set up inside Microsoft a Committee bringing together top executives of the business, engineering and legal departments. The role of this Committee is to review the technologies developed by Microsoft before they are put on the market to evaluate the human rights risks associated to these technologies. The Committee can look at questions of non-discrimination, safety, privacy, transparency, inclusiveness and accountability, among other considerations. The goal is to try to anticipate and consequently address the ethical risks. Jean-Yves Art concluded his presentation by offering a proposal to better anticipate human rights risks in developing technologies, namely to include some education/training in human rights law in the curricula of software engineers. This would give future engineers more sensitivity to those human rights and ethical risks in their work.

Nighat Dad

The third panellist of the session, Nighat Dad, Executive Director of the Digital Rights Foundation in Pakistan, began by noticing that developing countries offer no data protection and that the discussion is not very advanced compared to the discussion in this panel. For example, in Pakistan, the national database is said to have depository of biometric impressions of close to a hundred million individuals. The authorities in charge of keeping this data safe have been giving it away to internal and external institutions. The data is being sold for as low as $1 on Whatsapp and Facebook groups. This is an evidence of the level of insecurity of the national database servers and the human rights
implications of this insecurity have already started showing in Pakistan. The problem is the same with the data collected by any of the major telecom companies in the country. The absence of any data protection policies within companies and of national data protection laws foster this insecurity. A further problem comes from the Safe City Project, whereby thousands and thousands of surveillance cameras are deployed in cities without providing any standard operation procedure on how to keep safe the data collected.

How do civil society and NGOs respond to these challenges in a context of lack of narrative, policies and data protection around these issues? The Digital Rights Foundation uses both national and international mechanisms. First at the international level, the NGO submitted a report to the OHCHR for the Universal Periodic Review of Pakistan, revealing gender digital violence, violation of freedom of expression and of privacy, and more. The NGO also recently submitted a report to the UN Special Rapporteur on Violence against Women, showing once again the online violence faced by women and the surveillance against minorities, women human rights defenders and the journalist community. Another report was submitted to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, as part of the June 2018 Human Rights Council session.

At the national level, the NGO has pushed for incorporation of data protection policies. It has generated discourse, but it has not led to any success. Following the cybercrime legislation in 2016, the NGO has managed to push the government to start working on data protection. It submitted a policy brief to authorities making policy recommendations around the protection of journalists against surveillance and how law enforcement is treating citizens’ data. However, the government has not yet released the promised data protection draft. The State has also failed to prevent human rights violations in the online space. The NGO has responded to that challenge by creating a cyber-harassment hotline for women in 2016. It has received over 2,000 complaints since then from women, human rights defenders, journalists, whistle-blowers. The hotline helps identifying policy gaps and the effectiveness of the law enforcement mechanisms.

To finish, Nighat Dad mentioned artificial intelligence and how AI military systems have already made mistakes in cases of drone surveillance and attacks. The citizens are at the receiving end of the abuse and artificial intelligence and have no say in their development. One issue is that culture plays a role when it comes to privacy and that culture of privacy does not exist in Pakistan. Masses do not demand the right to privacy. As the State and companies see no demand for it, they do not comply with international standards.
Dr. Hannah Rau

Hannah Rau, First Secretary for Human Rights and Political Affairs at the Permanent Mission of the Federal Republic of Germany to the United Nations. Her presentation addressed the following question: How to strengthen the protection of human rights in the digital age? She stressed that the right to privacy was central to this question. Respect for the right to privacy enables the enjoyment of other human rights by creating a secure space online and offline. As both the Human Rights Council and the General Assembly have held, a comprehensive human rights framework exists that applies offline and online. However, the internet is increasingly shaping how we communicate, work and live. This entails opportunities, but also risks of controlling and limiting individual rights and civil society space. Given that human rights are increasingly exercised online today, more violations occur online, too.

There is a need to enhance the implementation of human rights online given that state-sponsored restrictions to human rights online are increasing. States, especially repressive regimes, use technologies as a convenient and effective tool to survey and control individuals, thereby restricting human rights and limiting civil society space. Discrimination and defamation can silence legitimate voices, infringe human dignity and undermine the democratic discourse necessary for a free and democratic society. Digital divides remain an acute problem. The security of online communications needs to be protected, also in the context of cybersecurity.

Unpacking the Human Rights framework to address these challenges requires an incremental approach: An ongoing process to keep up with rapid technological progress. A lot of work has already been done to unpack the existing human rights framework for online implementation. It is important to continue including all relevant actors in this process, especially civil society activists. Any solutions developed must bear in mind that the right to privacy is already protected, but faces growing challenges in the digital age.

Not protection gaps but a lack of implementation of the right to privacy needs to be addressed. Together with like-minded countries Germany has been working to promote the understanding and protection of the right to privacy in the digital age,
In the Human Rights Council and the UN General Assembly. The understanding of the right to privacy has been developed through a panel discussion, an OHCHR report, substantive resolutions in Geneva and New York, the creation of the mandate of the Special Rapporteur on the Right to Privacy and an expert workshop. This has always been achieved by consensual resolutions. This work is also supported by joint statement, debates, side events and more. The Universal Periodic Review is an opportunity to give meaningful recommendations. The discussion is also advanced in other fora, such as the Freedom Online Coalition that is chaired by Germany in 2018.

In a nutshell, there is a great human rights framework, but it is facing new challenges in the digital age. Therefore, unpacking this framework to meet the challenges is an important cornerstone of the work of Germany in Geneva, New York and Berlin. Nevertheless, every actor in the field must do his or her share to give special attention to the topic of human rights in the digital age.

**Graham Webber**

The final speaker on the panel was Graham Webber, Interim Chief Executive of the Investigatory Powers Commissioner’s Office (IPCO). He explained the process for granting bulk investigatory powers to intelligence agencies under the UK's Investigatory Powers Act 2016. The four forms of non-targeted investigatory powers are bulk interception, bulk equipment interference, bulk acquisition of communications data and the retention of bulk personal data sets. The consideration for someone authorising the acquisition of the material is whether it is necessary to do so, having regard to the potential trade-off between the positive and negative impact of the acquisition.

The Investigatory Powers Act 2016 sets out the investigatory powers clearly and creates a new oversight body, formed of sixteen judges, a technology advisory panel, and about fifty officials. The Act provides two key powers for the oversight of the intelligence services. The first key power is the double-lock. This means that for any of the bulk powers to be granted, two steps are necessary: firstly, an application must be made to the Secretary of State; secondly, the decision of the Secretary of State is reviewed by one of the judges of the oversight body. Two specific considerations for the judicial review are set out in the legislation: privacy and the integrity of the communications system, in cases involving hacking. The second key power of the oversight body is the post-facto
oversight by officials and judges of conduct authorised under the legislation. The oversight body has complete freedom of access to the intelligence agencies to check their compliance with the law and the accuracy of the information provided in the warrant. Overall, the oversight body enjoys a wide range of powers.

The independent oversight of investigatory powers under the Act allows a debate which wouldn’t exist without this judicial review. One of the challenges faced by the oversight body is: how to judge proportionality in the context of bulk? There are a number of considerations, but three which are particularly relevant in the context of other discussions at the event. First, the negative impact of an interference must be assessed, balancing the benefits of holding the data with the impact on privacy. More research would be helpful to quantify this impact. Second, the positive impact on human rights of these bulk investigatory powers must be factored in. Third, foreseeability must be examined, looking at how the data will be used and how any internal authorisation works. To finish, Graham Webber observed that the Act is focused on authorising the collection of intelligence and does not give guidance regarding how analytical tools (such as artificial intelligence) could be applied data collected under the act. The oversight body must find its own way in that regard.

IPCO put out a request for people to send in ideas of questions which judges should consider when looking at bulk applications.

Discussion

Attendees to the conference were firstly concerned with which measures would ensure the implementation of the human rights framework resulting from the work at the UN level, as well as whether the UN is doing enough and what can be expected from it? The answer from the panel underlined the need for support from many states to make progress on a specific issue. The UPR in Geneva has led to some progress with the members of the Human Rights Council making recommendations to the country under review. However, for this to be translated into concrete steps by the government under review, civil society is key, and it is a more difficult task to push the State to act on these recommendations. Another course of action is naming and shaming, trying to draw public attention to specific cases of human rights violations. Treaty-bodies are also doing a lot in Concluding Observations, giving an idea of what a General Comment on the subject could contain. Nevertheless, it is also up to civil society and others to make an input and add critical voices to this process.

As an example, the panel indicated that in the UPR review of Pakistan there were no recommendations out of 168 accepted by Pakistan that related to digital rights. When civil society was resisting the Prevention of Electronic Crimes Act in Pakistan, the Special Rapporteur David Kaye sent several letters listing its concerns about the impact of the law on human rights, but there was no response from the Pakistani government to international enquiries on digital rights.

Another concern raised was whether the IPCO fits within the human rights framework, knowing that the various concerns and recommendations around the
Investigatory Powers Act (IPA) draft brought up by international and regional mechanisms were not addressed by the government. How can the human rights framework address these tendencies of States to ignore the right to privacy? Further, how transparent is the procedure? Is it transparent enough to allow people to understand the process and the basis on which the judge issues the warrant? The last concern expressed was about the level of details available to the judges of IPCO to make their decisions and the willingness of security services to provide information.

In trying to answer these questions, the panel began by noting the important role of an institution in ensuring the protection of human rights. It is not the role of the institution to unpick Parliament’s intention in passing legislation, but it is open to that institution to respond to criticism of or future legal challenge to that legislation, particularly where that impacts on the role of the institution. There is also hope that the work done by IPCO has enhanced engagement with civil society in the field of security and surveillance. In cases where the state is defeated in front of a tribunal, IPCO will need to be attentive to any human rights considerations raised in the case.

Regarding transparency, IPCO intends to publish as much as possible, but is limited in some ways by the legislation. What is authorised for publication is not a prerogative of IPCO, because national security is at stake. However, IPCO will publish as much as it can for the purpose of purposes of transparency. On the subject of the level of detail available to judges to make a decision, it has shown not to be a problem. Security services tend to show much information to the judges, and to do so easily. In case where the judge feels there is not enough information to make a decision, they can seek clarification or additional material. This is the first protection. The second protection is, when paperwork in the context of a post facto examination of the decision appears to take only the most optimistic spin of things, it could affect the level of trust between the security agency and IPCO and it could then become more difficult for the security agency to have authorisations granted.

Attendees then brought up an article in the Guardian reporting that law enforcement’s use of facial recognition had a 98% failure rate. The failure rate shows the extent of risks the human rights violations, yet is still being used. It has an important effect on the lives and dignity of these individuals, who have little or no recourse against it. The panel addressed the comment by acknowledging that the question of facial recognition is about the adequacy and sufficiency of the treatment of data with the facial recognition technology. The technology of facial recognition with an 98% failure rate is therefore obviously not complying with the ethical principles promoted by Microsoft in its development of technologies. At the industry level, there is a push to promote these ethical principles beyond simply Microsoft’s walls. The organisation ‘Partnership for AI’, gathering other companies such as Google, Apple or Amazon, is an example of this objective. However, there may be some concerns about the role of Microsoft with regard to the causation element of the UN Guiding Principles on Business and Human Rights, because Microsoft only produces some elements of AI, which then go to other industries that develop AI.
further and use these technologies. There are therefore some limitations to the work done by Microsoft regarding those ethical principles. The industry is aware of the risks and tries to do its best to address the concerns genuinely.

The panel further emphasised that the inaccuracy of facial recognition is not the main concern in terms of human rights. A worry of similar force should be raised about the implications of such a technology for the right to privacy. Information that you collect by ever better methods may still translate into serious human rights abuses. The floor of attendees noted that the biggest worry is about false-positive, that is to say flagging somebody completely innocent. When talking to the police, it seems that once someone is identified with this technology, the decision to stop-and-search is immediate. Yet, the process of decision-making around the data collected from AI is important. A real concern is actually the false-negative, which means that somebody in law enforcement knows the suspect and the machine fails to recognise that.

This response from the panel generated more questions. In particular, one attendee asked how it can be ensured that the ethical principles developed by Microsoft are universal ethical principles, especially with regard to the measures taken to make sure that the work of ‘Partnership in AI’ is not only a Western conversation. The panel explained that ‘Partnership for AI’ aims at broadening the recognition of the ethical principles used by companies like Microsoft and that there was a willingness within the organisation to be open and to work with other actors such as academics to address the issue of human rights in the best possible way. However, there is little geographic diversity. Most companies are U.S.-based. The panel further commented that it is important that not only governments and academia decide on the ethical criteria applicable and they shouldn’t be deciding on the behalf of the people in developing countries.

Then the question arose as to whether, from a civil society perspective, there are any positive contributions to take from these technologies? This question came after a comment noting how the tone around technologies has changed from all-positive to all-negative. Indeed, it must be highlighted that social media and online presence have given a new space for civil society. However, offline space and social media space has been shrinking, with the State making attempts to use malware technologies to track activists activities and silence them. So that there are opportunities coming out of new technologies, but some governments always find ways to shut down the opportunities and the online voices.

The remark was then made that Snowden’s revelations have shown that mass surveillance is not only the work of the State. Civil society in Pakistan raised this issue to politicians, but they appear unwilling to address the question or they have a lack of awareness around the subject. What is the position of the UK on this? The panel stressed that the UK is very clear about the standards that apply in different contexts, especially making a distinction between UK-based interceptions and interceptions outside of the UK. In cases of extraterritorial activities, there is no
requirement for the UK to get consent from the country which the data comes from. The more states are involved, the more chance there is for oversight, for a clearer judicial recourse and other protections. However, the State is also the one which individuals want to be protected from. This is the biggest paradox today.

Another question from attendees was concerning the ability of UN human rights mechanisms to be used more quickly and to stimulate a much larger discussion about human rights and big data, knowing the rapid pace of technological development. The panel recognised the importance of reacting quickly and to quickly identify and understand the human rights concerns linked to new technologies. To avoid unseen harm of online violations concrete tactics are key. All actors should push for implementation of the human rights framework online. Each country must develop national standards, relying on input from academia and civil society.

We have the ability to see the path technological development is following. With this information, we can also begin to work in advance on identifying the human rights concerns and conducting impact assessments. We can thereby future-proof, rather than address the concerns only once human rights violations have already occurred. To achieve this the different actors must raise awareness to states of the challenges of new technologies.

To conclude, two questions arose from this panel discussion: must we make some sacrifices in order to help avoid human rights damages? And if so, how much do we sacrifice?

Sabrina Rau closed the panel session by thanking all the panellists for their insightful and interesting presentations and the different interventions. She noted that the different actors need to work together across disciplines to “future-proof” legislation and technologies to protect fundamental human rights.

Closing Remarks

After the end of the final panel session, the co-director of the HRBdT project Maurice Sunkin delivered the closing comments to the conference. He hoped all had found the conference informative, invigorating and stimulating. He continued by expressing his gratitude on behalf of the entire HRBdT team to all those involved, who helped making the conference the success it was:

- To the panellists and speakers, in particular to Peggy Hicks for her keynote speech at the beginning of the conference.
- To the moderators and discussants, who managed in a very limited time to pick up on so many of the key issues addressed in the different panels.
- To all the attendees to the conference for their participation and their questions, which were important for building dialogue.
- To all those who helped organising the conference and with the logistics.
- To the Geneva Academy for hosting the event and helping with the organisation.

Maurice Sunkin continued his closing comments by noting that one of the greatest challenges faced in the area of new technologies is its dynamic nature and the pressure of change. Academics, unlike legislators, are usually accustomed to working at a fairly comfortable pace, almost a leisurely one. In that sense, the field of new technologies represents a real challenge because it is moving at an incredibly rapid pace. Therefore, we must pose some of the challenges that we are trying to confront, such as the problems around predicting the effect of new technologies or predicting the nature of these technologies. This is a moment in time when a very significant set of issues have to tackled.

Already in 1968, at the Teheran conference commemorating and reflecting upon the first 25 years of the Universal Declaration of Human Rights, the need was observed to address the challenges that new technologies were confronting to human rights. This is one of the greatest dilemma we are working for.

Our esteemed late colleague Nigel Rodley had already detected the potential of taking small steps in order to achieve significant change. The question however stays whether we can afford in an area such as technologies to take such small steps.

The last session panel it was noted that the different actors in the field of new technologies were confronted with the need for hard choices. But then, what are those choices? And how informed are those choices? A lot of concerns appear in relation to the need for anticipation of the consequences of these technologies. These remarks emphasize the role of a project such as the HRBDT in tackling the challenges faced by human rights because of new technologies.

Maurice Sunkin considers it a great privilege of being academic in the HRBDT team at the University of Essex. However, he asked what is the role of academics in an area like this? How can they contribute to the wider discussions that people working in practice around this topic have? Academics can work at carefully conceptualising what the issues are. It helps inform the discussion by careful thought and evidence. The HRBDT team hopes that through its research and through this conference, we are able to engage with different actors.

Maurice Sunkin concluded by expressing hope that the conference will have helped start a dialogue and that will continue in the future.