Consultation Report
Access to Remedy in the Technology Sector

23 – 24 SEPTEMBER, 2021

In resolution 44/15, the Human Rights Council requested OHCHR to convene a consultation to discuss challenges, good practices and lessons learned in enhancing access to remedy for victims of business-related human rights abuse. In the context of that resolution, as well as the work undertaken on remedy through the Accountability and Remedy Project (ARP) and the B-Tech Project, OHCHR organized a two-day consultation to provide an opportunity for States, experts, civil society and other stakeholders to discuss the challenges involved in seeking and delivering remedies for harms connected to the technology sector, and practical ways to address them.

The consultation took place in the Palais Des Nations and also online, over two-days. The event was organized into the following four thematic sessions:

- Session One: Remedying adverse human rights impacts of technology companies through the courts. [Page 3 / Link to session recording]
- Session Two: State-based non-judicial mechanisms and their contribution to access to remedy in cases of tech-related human rights abuses. [Page 7/ Link to session recording]
- Session Three: Understanding the needs and perspectives of affected stakeholders when attempting to seek remedies. [Page 10/ Link to session recording]
- Session Four: The role of technology companies in remedying human rights harms connected to their products and services. [Page 14/ Link to session recording]

This report provides an overview of key themes, and contributions from panelists and participants, for each session. The deliberations will inform ongoing work through ARP and the B-Tech Project, and ideally all stakeholder groups seeking to advance remedy for victims of human rights harm associated with new digital technologies.

Please see the consultation concept note for the full agenda including list of speakers.

About the Accountability and Remedy Project

The Accountability and Remedy Project (ARP) aims to strengthen implementation of the Access to Remedy pillar of the UNGPs. Since its official launch in 2014, three substantive phases have been completed, with each phase producing recommendations for enhancing the effectiveness of one of the three different categories of grievance mechanisms referred to in that pillar (background on ARP).

About the B-Tech Project

Through the B-Tech project, OHCHR seeks to ensure respect for human rights in the development, deployment and use of digital technologies through the uptake and implementation of the UNGPs by digital technology companies. The project's vision is to have the UNGPs promoted and applied – by companies, States, investors, and civil society – so that respect for human rights and dignity for all are at the heart of the 21st Century digital economy (background on B-Tech).

Foundational Paper Series

The UNGPs offer States, technology companies, investors and advocacy organizations a robust and credible framework for preventing and remedying human rights harms resulting from the use of technologies. In the context of OHCHR's work on accountability and remedy and tech, four foundational papers have been released on access to remedy in the technology sector.

- Basic concepts and principles
- A "remedy ecosystem" approach
- Designing and implementing effective company-based grievance mechanisms
- Understanding the perspectives and needs of affected people and groups

Session One: Remedying adverse human rights impacts of technology companies through the courts

This session explored the extent to which courts are used as a way of obtaining remedies for human rights harms arising from or connected with the activities of technology companies. Beginning with a discussion of how courts are used at present, what recent data tells us about current trends and barriers to accessing justice, the session heard directly from legal practitioners about their practical experiences in litigating human rights-related cases in different jurisdictions.

The insights gathered from Session One will be used by ARP and the B-Tech Project as the platform for a more forward-looking discussion. This will focus on the challenges that domestic courts may face in keeping pace with and responding to technological developments with potentially global impacts. Furthermore, there will be a focus on areas where further legal development and cooperation may be needed to ensure that courts can play their part as a source of *effective* remedies in cases where people's human rights are adversely affected by the development and application of these new technologies.

Part I. Remedying adverse human rights impacts arising from digital technologies: What roles do courts currently plan?

Unevenness in availability and comparability of data on court activity (i.e. at domestic level, and from jurisdiction to jurisdiction) makes it difficult to build up a comprehensive picture of the responsiveness of courts to tech-related human rights harms. However, from a high level review of cases referred to judicial mechanisms in recent years, it is possible to observe a number of general features and trends including:

- the importance of providing options for **private enforcement** of legal standards (i.e. additionally to, or in place of, public enforcement by regulatory or law enforcement bodies);
- the importance of **bespoke statutory causes of action** (rather than general legal theories relating to liability for harm) as a basis of legal claims;
- related to the two points immediately above, the **numerical dominance of cases concerned with the right to privacy**;
- the **apparent relative under-utilisation of criminal proceedings and processes**;
- the **diversity of jurisdictions** in which cases arising from allegations of tech-related harms are appearing;
- the **diversity of remedies sought** by claimants, and the high level of emphasis (relatively speaking) placed by complainants on **preventative remedies** (i.e. forward-looking remedies aimed at future prevention of harm); and
- the vital role of **civil society organisations** as a source of **advice and support** and, increasingly, as **representatives of affected groups** in legal cases.

Using these data and findings as a springboard for discussions, participants reflected on the "**patchiness" of coverage** of different types of human rights in domestic legal regimes relating to the technology sector. While a limited set of rights received enhanced protection under bespoke domestic regimes (notably privacy), many rights are only partially covered, not vigorously enforced by the authorities, or overlooked altogether. Several participants described the challenges that practitioners can face in **identifying a cause of action** that mapped sufficiently well onto the type of human rights harms that had been suffered as a result of the use of digital technologies, or the manner in which they had been designed or developed.

In some cases, **creative lawyering** could help to overcome the problem of gaps in legal regimes or "patchiness" of legal coverage; but, in other cases, the **lack of causes of action that are both easy to understand and apply and which properly express the nature of the harms suffered** mean that cases risk early dismissal either because judges have found arguments unpersuasive (in light of the prevailing legal tests) or because strict legal criteria relating to the "**standing**" of the claimant to commence proceedings or the "**materiality**" of the harm have not been satisfied.

Examples of attempts in different jurisdictions to seek remedies for adverse impacts on **freedom of thought** associated with the activities or products of technology companies were discussed in this light. While in some jurisdictions there may be a constitutional route to remedy for these (and similar) types of human rights harms (and judges may be reasonably well-disposed to hearing legal arguments on this basis), the **novelty of claims** based on "under-used" or less well understood human rights, and the **lack of clear underpinnings in domestic legal regimes**, were proving a barrier to remedy in others.

It was furthermore noted that **legal theories and causes of action that focus on harms to individuals may not be easily adapted to deal with instances of "collective" and "societal" harm** arising from the way that technologies have been designed, used or deployed, or with **systemic issues.** Examples of "collective" or "societal" harm associated with the use of digital technologies might include the impacts on **freedom of thought** or the **discriminatory effects** within a population that could result from manipulation or removal of on-line content, which could lead to **reducing awareness of opportunities, choice and personal autonomy,** and, in extreme cases, **undermining of civil and political rights**.

While judges have shown themselves to be receptive to **new legal arguments** in some cases (e.g. relating to the correct interpretation of laws regulating the technology sector in light of international human rights standards), there are limits to which **judicial creativity** alone can address many of these emerging challenges. Fundamentally, **the legal obligations of technology companies to identify, prevent, mitigate and address human rights risks need to be more clearly articulated in domestic legal regimes**. In the process, **closer attention needs to be paid to rights and/or adverse impacts that are "collective" in nature, and rights that may presently be "under-used" in this context because their scope, content and practical**

implications (for digital technologies and social media companies in particular) are not yet well understood.

Part II. Defending human rights in the courts: Two case studies

Gaps and inconsistencies in the domestic legal regimes relied on by affected people and communities can create or exacerbate **barriers to remedy** in a number of ways. Participants highlighted the **additional procedural steps** that often became necessary where the law was unclear, adding to **legal costs and delays**. The **technical complexity of domestic law regimes** relating to the regulation of the technology sector was noted (owing to the technical complexity of the subject matter), with the **extraterritorial scope of many regimes** (needed to respond to the cross-border nature of business activities and their impacts) complicating the legal picture yet further.

Participants drew attention to the way in which these uncertainties tend to **exacerbate the effects of already existing power and resources imbalances** between companies, on the one hand, and affected individuals on the other. Shifting the focus from legal to financial and practical barriers, participants explored the way in which "**information gaps**" between individuals and technology companies can be particularly acute as regards the workings of **algorithmic decision-making tools and processes** and the different ways in which **personal data** is being used. This lack of transparency adds substantially to the **financial and other risks** of resorting to judicial processes to enforce human rights standards and obtain redress for human rights harms.

Turning to the role of courts in interpreting and enforcing public law standards (as distinct from their role in handling claims made be affected people directly), concerns were expressed, (drawing from first-hand experiences in a number of cases) about the **role of regulators and law enforcement bodies**; specifically, **the gulf that can exist between "law on paper" and the manner in which it is implemented inpractice.** Participants provided examples of cases and settings in which **prioritisation by regulators of vested interests risked undermining human rights protections**. Of particular concern to some participants was an apparent trend in favour of allowing governments to access personal data more freely (increasingly enabled by the terms of domestic legal regimes), to ends that may not be aligned with human rights standards and protections. Participants also drew attention to the difficulties that can be experienced by affected people and their representatives in persuading relevant regulators (e.g. those with mandates covering privacy and/or freedom of expression, as well as specialist appointees) to recognise that their human rights had been adversely impacted and to take swift action.

Part III. Courst and tech

Finally, participants were asked to consider and comment on the **different factors that may constrain the ability of courts (and individual members of the judiciary) to robustly interrogate and respond to allegations of tech-related harms** that are brought before them, whether by

private individuals or by regulatory bodies. It was noted that, while the **gaps in understanding by judges of technical aspects of certain digital tools and products** could create challenges and inefficiencies, these were narrowing as judges become more familiar with digital technologies, because of the ubiquity of these in daily life, but more specifically (i.e. for judges) the **growing use of information and communication technologies and automated decision-making tools to help streamline court processes**. The positive impacts of different **training and awareness raising activities** were noted, though **greater investment and support is needed in jurisdictions where the judges continue to face a chronic shortage of resources**.

A more complicated structural issue to address, related **to judicial confidence**, is the extent to which the **regulatory architecture for the technology sector** seems to be developing in a way that is both normalising and entrenching **outsourcing of certain regulatory and security functions to technology companies**. This, it was argued, may **affect the way that courts weigh up their options to intervene in future**, likely causing them to **favour more conservative options** because of the desire not to unravel or create lacunae in what will be regarded by many as **essential (cross-border) infrastructure**. A further consideration that may weigh against courts ordering far-reaching reforms may be the probability that, given the level of reliance by society on digital technologies and their supporting infrastructure, such interventions may have human rights implications of their own.

Questions concerning the role of courts in remedying tech-related human rights harms (and their effectiveness in doing so) are intricately bound up with questions of the effectiveness of domestic legal regimes regulating the technology sector at large, both in terms of the design and implementation of those regimes. This is because of the constitutional role of courts to interpret, apply and enforce the domestic laws that already exist. While scope for "judicial creativity" often exists, **the ability of courts to devise bespoke solutions to the human rights-related problems that are brought before them is never unlimited and is usually tightly constrained**.

It is for this reason **that incomplete, poorly designed or incoherent regulatory regimes, which do not adequately respond to the human rights risks that may be posed by the business activities in question, were identified in the High Commissioner's report at the conclusion of the first phase of the Accountability and Remedy Project as among the most fundamental and intractable barriers to judicial remedies**.

That report included, among its recommended actions, that States conduct regular reviews of domestic law regimes to ensure that they continue to "provide the necessary coverage" and adopt "the appropriate range of approaches with respect to business-related human rights impacts in the light of evolving circumstances and [States'] obligations under international human rights treaties" and that States take "the necessary legislative and/or policy steps to correct any deficiencies in coverage or approach.". See UN Doc. A/HRC/32/19, Annex, 1.9.

As can be seen from the discussions above, urgent improvements are needed to make domestic legal regimes more responsive to the kinds of human rights harms that stakeholders have identified in this consultation, and more broadly. Policy-makers and legislators need to pay much greater attention to the adverse human rights impacts occasioned by the collective and societal effects of the business activities of technology companies, which in many cases are not confined to domestic borders and may be global in reach. Without **substantial changes to regulatory models**, involving a **greater degree of international cooperation and coordination**, domestic courts may struggle to play more than a peripheral role in delivering effective remedies for tech-related human rights harms in practice; despite their being, in the words of the UN Guiding Principles on Business and Human Rights, "**at the core of ensuring access to remedy**" (see UNGP, 26, Commentary).

Session Two: State-based non-judicial mechanisms and their contribution to access to remedy in cases of tech-related human rights abuses

This session explored the role of non-judicial grievance mechanisms at the State level in complementing and supplementing judicial mechanisms in cases of technology-related human rights abuse. Such mechanisms may include regulators, ombudspersons, inspectorates, public complaints handling bodies, National Contacts Points under the OECD Guidelines for Multinational Enterprises and national human rights institutions. For further background, OHCHR's Accountability and Remedy Project has developed a detailed set of technical recommendations for improving the effectiveness of these mechanisms.

The discussion was divided in two parts. Part I centered on how to strengthen the competencies and capacities of National Human Rights Institutions (NHRIs) such that they can play a meaningful role in access to remedy fo abuses relating to tech company conduct, products and services. Part II provided reflections on a similar set of questions with regards to OECD National Contact Points for Multinational Enterprises.

Part I. The role and contributions of National Human Rights Institutions to access to remedy

A 2021 report by the UN Working Group on Business and Human Rights sets out the following three overarching ways in which NHRIs can contribute to Access to Remedy which provided a helpful framing to the discussions at the consultsation.

- **Foundational:** In the context of tech abuses, NHRIs can raising awareness, or for example work towards legal reform (legal regimes take time to respond), among others through making recommendations for legal reforms based on the context.
- **Indirect:** NHRIs can offer support to human rights defenders and people seeking access to remedy, e.g. through operational level grievance mechanisms. They can provide oversight and monitoring, or also provide legal assistance.

- **Direct:** If NHRIs have the mandate, they can themselves enable the delivery of o remedy, for example by accepting complaints, overseeing prompt payment of compensation or assisting with guarantee of non-repetition etc. This may take a range of remedial aspects.

Panelists reflrected that when it comes to tech-related human rights abuses, NHRIs can strengthen the efficiency of their work through building capacity internally and externally (e.g. workshops, peer learning about issues arising on the ground) and by facilitating transborder cooperation. Adding to this, engagement with companies is key to increase transparency and foster consultation with rightsholders when the technologies are created. With the goal to reduce opacity, NHRIs should inform processes in a proactive manner to create technologies that are compatible with international human rights.

The discussion showed that National Human Rights Institutions across different geographies recognize the necessity to take a closer look at human rights abuses in the technology sector and how access to remedy can be facilitated in such cases. The following key themes characterized the discussion:

Theme One: Initial awareness about the specific challenges in dealing with corporate human rights abuses in the tech sector - While there is a nascent existing awareness about the specific challenges posed by the conduct of tech companies towards human rights, precise coordinating action among NHRIs is yet to be seen. In particular, limited resources and/or capacity constraints have in the past hindered such efforts, but momentum and interest in addressing tech-related human rights impacts is growing, along with conversations about possible transborder cooperation.

Several NHRIs took the floor to present how they are increasingly working on tech and human rights. The NHRI of Australia conducted a human rights and technology project led by a former human rights commissioner over three years to identify and address the risks posed to human rights by AI. In consultation with the government, CSOs, academia and industry in Australia and worldwide, 38 recommendations to the government were formulated in a report. Among others, the NHRI called for an **AI safety Commissioner to be established** to promote safety and protect human rights in the use of AI in Australia, as an independent statutory office that works with and alongside regulators, to build capacity, monitor, and provide guidance to governments and private sector on how to comply with laws and ethical requirements.

The **NHRI of Morocco** framed the internet environment as an incubator of freedom, and hate and discrimination alike and pointed out its ongoing work on a report on tech and human rights, with an emphasis on the Moroccan election (fake news and lack of protection of personal data for voter targeting), online gathering to be included in the right of freedom of assembly and the effects of the pandemic triggering work on different themes, such as access to online education as well as the rights of defendants during remote court hearings.

Theme Two: Necessity to raise awareness about how to appeal and receive remedy from state-based non-judicial mechanisms and harmonize/broaden approach how to regulate and protect personal data. Data protection was a theme that was strongly mirrored in the intervention by the NHRI of Chile, which stressed that the country is the process of developing its own data protection agency. In Chile, the legal system is focused on standard judicial guarantees. The country has a set of quasi-judicial entities that could potentially have a mandate to open the way to better State-based non-judicial mechanisms which will allow access to proper remedy. Chile is going through three fundamental changes: development of its second National Action Plan on business and human rights, which will most likely also include tech; the development of an AI strategy and constitutional changes that will include human rights and environmental protection.

The NHRI of Chile called for the creation of an entity under the supervision of the presidency under the ministry of economy with an independent, technical nature and equipped with appropriate necessary resources.

Theme Three: Building capacity internally and externally, including facilitating transborder cooperation. With regard to building internal capacity, the Danish Institute for Human Rights sketched its internal process to create a strategy on Business and Human Rights in the tech space, mapping of opportunities and ideas for engagement to enter in the tech space and deciding to begin with developing a guidance on human rights impact assessments of digital activities. The institute also works on public procurement to enable policy makers and others to implement requirements for their suppliers to foster a good e-governance agenda and to ensure that there is a human rights based approach in the tech sector. The institute will be launching a report on automatic public administration and delivery, including assessing the development of AI in administrations with a human rights lens.

Moving towards external capacity building, panelists stressed the possibility of combining human rights expertise with data protection capacity to compensate for a lack of enforcement power - while many NHRIs lack enforcement power, teaming up with data protection authorities (DPAs) can assist them in enforcing privacy-related issues. The Berlin DPA stressed that it is worth looking into the GDPR framework and the specific powers vested in the national data protection authorities. The Berlin DPA can not only obtain an access to data being processed by state and non-state actors but also access the premises of the controllers. The core of GDPR relates to right to privacy. In the EU, it developed into a proper right for human rights protection. There are many ways to interlink the work between NHRIs and data protection authorities. In article 80 of the GDPR, the regulation opens up the representation of data subjects that have been violated in their privacy rights by non-profit organizations. It is sought to be a way of implementing class action and sample complaints cases. NHRIs can use the GDPR framework to represent underrepresented groups, for example refugees, which are under-represented and do not have enough means to file formal complaints withNHRIs. Although it is a very Euro-centric approach, the GDPR is expanding to other regions, like Northern America.

The NHRI panel demonstrated **the potential for mutual learning and exchange among NHRIs about how to best use mechanisms and parliamentary/advisory functions**. Ensuring policy coherence through discussing responses to tech regulation and incentives across geographies, including consistency between legal and executive branches of government, with specific roles, allowing for coordination so that both private and public entities can respect human rights in the tech sphere. The Global Alliance of National Human Rights Institutions (GANHRI) can act as important hub to exchange and align regarding developments across geographies

Part II. The challenges and opportunites OECD National Contact Points face in facilitating access to remedy

The discussion showed that OECD National Contact Points (NCPs) across different geographies are increasingly becoming a point of focus for cases involving the technology sector.

Panelists reflected on ample opportunities for different organizations or individuals to file a case, also regarding tech business conduct with NCPs. By way of background,NCPs are the implementing mechanism of the OECD guidelines. They promote the guidelines and act as an non-judicial grievance mechanism. Since their creation in 2000, NCPs have handled over 600 cases, in various countries and territories. With the growing importance of the tech sector, they have been handling more case in that sector. Regarding the issue of standing, NCPs may follow a broad definition. It can be an individual affected but also anyone who has an interest in the matter (consumer group, campaign organization etc.). In relation to the tech sector, it is not easy to identify the victim. Any organization that can show that they have an interest can file a case.

Where should the case be filed? Where the impact takes place. If it takes place outside the OECD, it should be filed in the country where the company is headquartered. It can be in multiple countries. There is a broad range of possibilities. The OECD guidelines have embedded the UNGPs, which say that companies should not only prevent and mitigate adverse impacts that they cause and contribute to but also those that they are directly linked to through their products and services. It is sometimes through the products and services that a company is related to the adverse impacts. Thus, the OECD is a relevant forum to address these kinds of issues.

The importance of linkages between individual NCPs was also raised as an important avenue to advance remedy and accountability. Many of the mechanisms have distinctive and limited mandate and legal powers – for instance, some can file complaints but cannot investigate the case on their own, they can only offer a certain type of remedy etc. There is a lot of diversity regarding these mechanisms. The questions of whether these bodies have enough power to be able to fulfill the job assigned to them should be kept on constant review. To focus on the limitations may miss the wider point on how to respond to the reality that, in many cases, **progress is being made and NCPs have been responding to the challenges posed by the tech industry, though there is not a single mechanism that can remedy all rights at the same time.**

Session Three: Understanding the perspectives and needs of affected stakeholders when attempting to seek remedies

This session sought to surface the perspectives and needs of affected stakeholders when attempting to seek remedies for human rights harms arising from technology products and services. **The emphasis was placed on giving civil society actors, both at the global and regional level, the opportunity to share concrete cases and research, and to highlight specific difficulties to access remedies.**

The session was divided into two parts. In Part I, invited panelists from CSOs shared global and regional perspectives, showcasing specific trends, patterns and challenges. Part II, which was organized in cooperation with Global Partners Digital, involved a discsussion of three cases studies, providing an opportunity to workshop specific difficulties around access to remedy in the tech sector.

Part I. Global and regional perspectives, trends and patterns

Invited panelists presented key issues of concern in their regions/contexts linked to the use of digital technologies. In Latin America for example, the use of facial recognition and its deployment without proper human rights impact assessment on human rights and due diligence processes, had led to human rights violations including of the right to privacy, freedom of assembly and freedom of expression. In many instances, people had been falsely accused and imprisoned, and unable to initiate legal proceedings to ask for reparation. From the panelist's experience, the human rights risks linked to the use of such technology clearly outweighed the advantages. **Such risks included issues linked to a sense that the burden of proof was on victims (i.e., guilty until innocent), the hacking of databases, the precise surveillance of individuals, mass surveillance, and algorithmic discrimination including false positives in the context of policing and public safety.**

Another panelist exposed the human rights risks linked to a social protection system using government's databases to assess citizens' eligibility to receive a social benefit. These create challenges for different social groups, such as indigenous people who do not speak Portuguese or are digitally excluded. Besides, the system was outdated at the beginning of the pandemic and did not keep pace with the number of unemployed people. **This reinforced the idea that access to remedy should be an upfront concern in the conceptualization, development and design of such sytems.**

A panelist based in Asia presented the different legislative recourses available in case of a personal data breach, and formulated recommendations to strengthen access to remedy in such a case. **These included the need to clarify the remedy access in personal data protection bill, to amend the consumer protection law to explicate the implementation of remedy pillar of the UNGPs, to implement the ASEAN Strategic Plan on Consumers Protection 2025, particularly related to the ASEAN Agreement on Electronic Commerce**. Ultimately, more

clarity was needed to implement the remedy pillar in the National Strategy of Business and Human Rights.

A European panelist presented the case submitted by his organization against a facial recognition company, and highlighted the key concerns brought in this case deriving from the creation of biometric data, including the lack of anticipation of future risks; the fact that data can be used for new purposes and reveal more information from individuals already in situation of vulnerability, placing them at a higher risk (e.g., victims of sexual harassment, migrants). The fear of being identified might deter them from accessing services that they might need.

Bringing a global perspective from research conducted at the global level, a panelists shared some high level findings such as that the primary harms encountered include the violation of the right to privacy, the denial of freedom of expression, censorship, dissemination of harmful content and discrimination from algorithm biases (influencing hiring practices for example).

In term of key challenges and obstacles to access remedy, the identification of the harm, the scale of the harm, and the multiple links and processes in the tech sector make it hard to determine where responsibility lies, as well as to navigate the remedy ecosystem for individuals. Additionally, possible remedies may partially address the harm, processes are slow and subjected to delays, individuals seeking remedy may be afraid of retaliation. The lack of transparency from companies and the lack of them acknowledging their responsibility, by fear of legal claims, were also cited among the key challenges and obstacles, as well as individuals' lack of resources to seek remedy. On the way forward, there is a need for more clarity on what remedy is available and how to use them. **Processes need to be more centered on people using these mechanisms, they should be tailored to facilitate engagement with stakeholders and consider context and technologies.**

Speaking from the perspective of a CSO providing a digital security helpline to assist civil society and human rights defenders and the media, mostly located in the MENA region and in North and Latin America, a panelist provided an overview on the key threats to CSOs online, including account compromise, malware, censorship, DDoS and other attacks, harassment and communication surveillance. Among the key lessons to be drawn from the cases being handled by the digital security helpline, it was reported that **digital attacks are shrinking civil space, that companies do not understand the real impacts of their decisions on the most vulnerable groups, that mechanisms are not transparent, that there is a lack of understanding of specific contexts and that CSOs are under-resourced to address these harms.**

The **gender dimension** of the misuse and abuse of digital technology, in particular as it relates to cases of online and ICT-facilitated violence against women and girls, was brought up by two panelists, who exposed the plea of women victims of violence committed online. An example was provided of a country where national law sanctions violence committed on the internet, but women nevertheless were reported to face obstacles in accessing remedy

because of the existence of fake profiles; the length and costs of the proceedings, and the need for judges to evaluate justly and equitably the psychological consequences of these attacks on women. Another panelist was of the view that at the global level, technology-based violence is a concept that is still being grappling with.

In summary, the biggest concerns include the speed and reach of transmission, the difficulty in identifying the perpetrator, and the absence of territorial jurisdiction in case of online harm. Tech companies and the police also face challenges as there is no accepted definition of ICT, it is hard to identify the perpetrator and AI is not sophisticated enough to identify harmful content. **Panelists also noted that studies show that there is a lack of trust in the judicial process, and a persisting bias towards considering online violence as not being violence, fears of retaliation, of being charged by the police or stigma and taboo, financial and time costs.**

To improve the reporting process, it was recommended to adopt international standards, share protocols and information among intermediaries, police, and CSOs, make sure access to remedies is easy to understand and accessible, provide trainings about online violence, address privacy concerns and enhance the ability to trace IP addresses and photos, and to have more women in tech overall.

Part II. Case Studies

On the basis of three hypotheticals, discussants and participants shared their views regarding the difficulties associated with accessing remedies in case of human rights harms associated with the use of technology products and services. This part of the session was organized in cooperation with and moderated by Global Partners Digital.

- **On case study 1 (racial bias in AI and ADM systems used in the criminal justice system),** it was noted that affected groups should participate in the design and the use of algorithms to identify biases. There is a need to emphasize that structural inequalities put some individuals in a difficult position and make access to remedy more difficult for them. In every step of the product/service development process, companies should make sure that no human rights harm is involved. They should be conscious of gender and racial biases. Access to information is crucial when a company provides surveillance technology for the purpose of policing or criminal justice. There needs to be transparency about contracts between governments and companies, as well as about what companies want to get out of these partnerships.

- **On case study 2 (sensitive data exposure)**, it was commented that many nation-state actors infiltrate dating apps, leading to the arrest, detention and blackmail of LGBTIQ+ members. But harm can be generated by the app itself, with many dating apps sharing sensitive data to third party add brokers. What is considered as an effective remedy depends on the context, on the nature of the violation and on the type of actor. But grievance mechanisms need to be accessible to all users, be user-

friendly, and decisions should be transparent. Companies have to understand better the harms that their users are potentially facing, and the context in which they are operating.

- **On case study 3 (online gender-based violence)**, panelists commented on the importance to remove the harmful content immediately, while reiterating the need to agree on a global understanding of freedom of expression. It was suggested to borrow from more developed areas, such as counter terrorism where content can be taken down quickly. It was noted that oftentimes, the law itself is not enough, and that there should be a political will to sanction online harm, as well as specific measures, and in particular preventive ones, and a budget allocated to these issues. Information about compensations and access to remedy should be made more easily accessible.

Session Four: The role of technology companies in remedying harms connected to their products and services

Where companies identify that they have caused or contributed to harm, their responsibility to respect human rights requires active engagement in remediation. Company-based grievance mechanisms can be one effective means of enabling remediation when they meet certain core criteria, and OHCHR's Accountability and Remedy Project has produced **technical guidance** on how to meet those criteria in practice.

With panelists comprising human rights leads from leading technology companies as well as experts from civil society and academia, the session focused on these responsibilities of tech companies under the UN Guiding Principles on Human Rights, opportunities and successful practices, and the challenges in meeting these responsibilities.

Perspectives from Academia and Civil Society

Academic experts reflected that while the technology sector has the same responsibilities as other sectors under Pillar II of the UNGPs, there are some "novel" aspects of harm in tech through its specialized and far-reaching products and services that require consideration when seeking to deliver remedy. The harms and impacts discussed affect *all* human rights, not only Freedom of Expression and Privacy. If anything, the complexity of the tech sector's relationship with remedy is due to this diversity of potential victims and of actors in the ecosystem.

Peers in civil society organizations focusing on business and human rights contributed to the conversation, noting that tech companies, when developing or working with their own internal grievance mechanisms, need to recognize whether they embody the characteristics of accessibility, transparency, and stakeholder engagement, in order to meet the expectations reflected in the UNGPs.

Perspectives from tech companies

Turning to representatives of tech companies, the conversation shifted to the ways that some companies have heeded recommendations in their approach to remedy. One company recognized that in any activity, a company should be required to ensure there is real human engagement in the loop, with effective channels for end users to raise grievances regarding harm stemming from an outcome of a product or service. Along with an ethics advisory board, related product/user principles and process assessments and trainings to put these principles into practice, the company believes it is in a better position to respond, rather than react, to user grievances. This proactive framework allows for a planned remedy response, rather than a knee-jerk or defensive one.

The second tech company participating in the discussion also noted a wide set of mechanisms to address complaints; both companies recognized that as tools and products mature and reach more users, and as new technologies enter the marketplace, the ecosystem of harms and remedies will only grow more complex. By preparing for remedy through various engagement processes, companies can be better prepared to respond beyond the ability of straightforward and traditional grievance mechanisms to address new issues.

In spite of all efforts to prepare for remedy, both corporate representatives acknowledged that at present there are no best practices for remedies in tech. It is helpful to look to other sectors for their lessons learned, while the global nature of tech products requires a likely broader set of interventions as well as understanding that users and potential victims also comprise a larger, and more diverse, global population.

Focusing on Preparing for Remedy

One speaker with extensive experience working on access to remedy outside of the technology industry noted the value of companies preparing for remedy – as against scrambling for solutions once negative impacts have occurred. The central notion is that good human rights due diligence (HRDD) does not mean that all negative impacts will be prevented in all cases. But HRDD should equip companies and their stakeholders to know what likely harms are going to be that will need to be remedied. Further, HRDD can help to build understanding of what the responsibility of different actors will be to provide remedy: using the UNGPs' cause, contribution and linkage framework.

In practice, as part of their human rights due diligence, companies should be addressing their preparedness for remedy for more severe harms, including capability of partners to deliver meaningful remedy. Companies can, and should, also build their leverage to encourage remedy – including via what is agreed upon in contracts or mutual commitments with partners, customers, and suppliers. When the moment comes, companies can then use this leverage.In short, companies should have a playbook about how to pursue remedy in relation to their most salient issues and high-risk partners.