THE DANISH INSTITUTE FOR HUMAN RIGHTS

PHASE 3: ANALYSING IMPACTS

GUIDANCE ON HRIA OF DIGITAL ACTIVITIES

Acknowledgments: This 2020 version of the Guidance was written by Emil Lindblad Kernell and Cathrine Bloch Veiberg, with research assistance from Claire Jacquot. We would also like to thank Eva Grambye, Elin Wrzoncki, Tulika Bansal and Ioana Tuta for their input and support. The Guidance has been developed on the basis of the HRIA Guidance and Toolbox. We also received invaluable input from several individuals and organisations who contributed their expertise, reflections and time on a voluntary basis, for which we are deeply thankful. We wish to extend our sincere thanks to: Rikke Frank Jørgensen from the Danish Institute for Human Rights; Richard Wingfield from Global Partners Digital; Jan Rydzak from Ranking Digital Rights; Jason Pielemeier and David Sullivan from Global Networking Initiative (GNI); Molly Land from University of Connecticut School of Law; Alex Warofka from Facebook; Nicole Karlebach from Verizon; Alexandria Walden from Google; Michael Karimian from Microsoft; Patrik Hiselius from Telia; Dunstan Allison-Hope from BSR; Margaret Wachenfeld from Institute for Human Rights and Business (IHRB); Mark Hodge and Lene Wendland from OHCHR and the B-Tech project; Isabel Ebert, University of St. Gallen, on behalf of the German Institute for Human Rights; Ephraim Percy Kenyanito from ARTICLE 19; Louise Kjær from Bluetown; and Elias Aboujaoude, Professor of Clinical Psychiatry at the Stanford University School of Medicine. In addition, the DIHR would like to recognise the collaboration with Lorna McGregor and Sabrina Rau from the Human Rights and Big Data Project (HRBDT) at Essex University, as DIHR's academic partner in the project, with a particular focus on Data Privacy Impact Assessments.

The contribution of expert reviewers does not represent their endorsement of the content.

Wilders Plads 8K
DK-1403 Copenhagen K
Phone +45 3269 8888
www.humanrights.dk

At DIHR we aim to make our publications as accessible as possible. We use large font size, short (hyphen-free) lines, left-aligned text and strong contrast for maximum legibility. For further information about accessibility please click www.humanrights.dk/accessibility

CONTENT

This document contains the Phase 3: Analysing Impacts section of the Guidance on Human Rights Impact Assessment of Digital Activities (the Guidance).

You can access the full version of the Guidance at: https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities

A NOTE ON THIS VERSION

This first version of the Guidance on Human Rights Impact Assessment (HRIA) of Digital Activities (the Guidance) is based on DIHR materials and experiences, input from expert reviewers and practitioners, the UN Guiding Principles on Business and Human Rights and international human rights instruments, as well as public domain sources on impact assessment.

The preparation of this Guidance included a workshop in Denmark in November 2019, during which 20 expert reviewers participated in a discussion on human rights impact assessment of digital activities i.e. digital projects, products and services.

It is anticipated that in 2020-2021, a Phase II of the project will focus on applying the Guidance in practice, the gathering and sharing of learning, and subsequently updating the Guidance based on experiences from practice.

As HRIA of digital activities is an emerging practice, this Guidance seeks to provide support to those working with HRIA of digital projects, products and services, but also to contribute to a platform for dialogue about HRIA practice and standards in the 'digital' business and human rights field. In this context, we welcome comments from stakeholders on the Guidance and on experiences with using it.

Please send comments, questions and suggestions to:

Emil Lindblad Kernell emke@humanrights.dk and Cathrine Bloch Veiberg cph@humanrights.dk

Funding

Creation and publication of this guidance has been made possible by general operating funds received from the Danish Ministry of Foreign Affairs.

PHASE 3

ANALYSING IMPACTS

WHAT HAPPENS IN PHASE 3?

Phase three involves analysing the data that has been collected during scoping and data collection in order to identify actual or potential business-related impacts and assess their severity. This will involve drawing on the normative content of international human rights standards and principles, comparative projects, findings from stakeholder engagement and so forth. In practice, some of this analysis will occur during data collection itself, but it is nevertheless important to allocate time and space specifically for impact analysis.

It is important to include not only the impacts that seem the most 'immediate' but to consider all impacts that the business has caused and contributed to, or may cause or contribute to, as well as impacts that are directly linked to digital projects, products and services. Impact analysis should also involve assessing impact 'severity', including by considering the scope, scale and irremediability of the impacts. This requires considering impacts from the perspectives of those who are experiencing them or who may experience them.

Lastly, to contribute to business respect for human rights, HRIA of digital activities should first and foremost focus on identifying and addressing adverse human rights impacts. Therefore, whilst positive effects may be noted, the identification of 'positive' human rights impacts is not the primary objective and should not detract from identifying and addressing adverse impacts.

?

KEY QUESTIONS ADDRESSED IN THIS SECTION:

- **What are the different types of impacts to be considered—i.e. actual, potential, caused by the business, contributed to by the business, and directly linked to business operations, products and services through business relationships?**

- **What does the 'digital ecosystem' imply for the assessment of company involvement in impacts?**
- **How can the severity of human rights impacts be assessed?**
- **Why do the UN Guiding Principles focus on 'adverse' impacts and what does this mean for the inclusion of project-, product- or service-related benefits in HRIA?**

1.1 TYPES OF HUMAN RIGHTS IMPACTS TO BE CONSIDERED

An adverse human rights impact occurs when an action or omission limits in whole or in part the ability of an individual and/or a group to enjoy their human rights. Individuals and/or groups may be affected by human rights impacts differently based on their gender identity, ethnicity or other characteristic. This impact can be both direct and indirect.

The perceptions of the affected individuals may or may not correlate with what constitutes a human rights abuse under international human rights law. Thus, individual and group perceptions of impact should be taken into account but should not be considered determinative.

Individuals and/or groups may perceive that they are negatively impacted in a certain way even when that impact does not amount to a negative human rights impact.

For example, individuals or groups might claim that their content posted on a social media is being 'demoted', and that their freedom of expression has therefore been negatively impacted. However, the evidence suggests this has not happened and it simply was not a post that garnered a lot of interactions and therefore did not spread or 'go viral'.

Conversely, individuals and/or groups may perceive that they are not negatively impacted when other data and expert analysis suggest that their rights have been impacted, or the impacted individuals may simply not know that their rights have been or could be impacted even when they have. In other words, it can be an issue of knowledge rather than perception.

For example, an individual's right to privacy can be negatively impacted if data is collected by a digital platform the individual is using. The individual feels safe because the platform clearly states that it anonymises all data it collects. However, if the data anonymisation is flawed, the data can be reidentified and

sensitive data related to the individual might be accessed by third parties. In this case the individual is likely to not know that the impact is occurring.

Assessment teams should consider all input while ensuring that their analysis draws from international human rights standards and principles.

1.1.1 ACTUAL AND POTENTIAL HUMAN RIGHTS IMPACTS

Principle 18 of the UNGPs states that companies should *"identify and assess any actual or potential adverse human rights impacts with which they may be involved either through their own activities or as a result of their business relationships"*. As such, **HRIAs must consider both impacts that have occurred or are occurring but also impacts that may occur in the future**. Box 1, below, provide examples of actual and potential impacts.

BOX 1: EXAMPLES OF ACTUAL AND POTENTIAL IMPACTS

Actual impacts occurred or are occurring. Examples:

- Facial recognition (e.g. facial identification) technology developed by a company and sold to a local police force has proven to produce higher numbers of false positives for ethnic minorities than for the majority in a given country, leading to an increase in wrongful arrests of ethnic minorities.
- A social media platform company found to have contributed to severe violations of the right to privacy as result of preventable data breaches failed to provide remedies to impacted rightsholders.
- A company that provides a search engine, has actively participated in the cyber-censorship policy of a government, contributing to serious breaches of the right to access to information and freedom of expression.
- A telecommunications company sells data to a data broker who in turns sells it to an entity that helps customers target specific individuals for personalised advertising. The digital service is then used to harass a customer's former partner and thereby leading to impacts on the right to privacy as well as the right to security of person.[1]
- An algorithm is used to predict university entrance exam results, using school's past track record on general exams to provide "fairer" results, which ends up disproportionately affecting students attending school in poorer areas by downgrading their predicted exam results. The predicted grades are used by universities in their admissions processes, barring some students from entering university, thereby leading to actual impacts on the right to equality and non-discrimination, among other rights.[2]

Potential impacts have not occurred yet but may occur in the future. Examples:

- Algorithms are used by justice systems to assist in sentencing decisions by calculating flight and recidivism risks, leading to a potential risk to the right to due process and a fair trial when risk assessments cannot be appealed.
- A company is developing a digital service which facilitates the assessments of social media platform users' sentiments concerning companies. The technology may also be used to identify protesters and human rights defenders.
- A telecommunications company 'zero-rates' (i.e. provides access to a subset of digital services at no financial cost) its own platforms and other digital services, thereby incentivising users to favour those services over others, and allowing the company to better track individual users' activity, while also serving the users very targeted ads. This may lead to the limitation of information available to internet users, which may in turn lead to future impacts on freedom of information and even on the right to participate in public affairs.[3]

It may often be easier to identify current and past harms, than to identify potential harms that have not yet taken place. Further, while it may be relatively straightforward to identify future impacts in relation to projects where recurring issues are known (e.g. automated decision-making systems in judicial processes without a 'human in the loop'), it may be **difficult for HRIA teams to identify impacts related to new and emerging digital products and services** that have not yet been tested or launched. In such cases, there are different methodologies that can be considered. See Box 2, below, for one alternative.

BOX 2: ASSESSING POTENTIAL IMPACTS THROUGH 'FUTURES THINKING' METHODOLOGY

Contribution by Dustan Allison-Hope, BSR.

Anticipating the future is difficult. The world is changing at a rapid pace, with disruptive technologies, shifting social norms, and turbulent politics transforming the human rights context. Blind spots and group think can prevent companies and those conducting HRIAs from seeing future possibilities, while tendencies to "predict" one version of the future obscures the very wide range of different futures that are possible.

Futures thinking, also known as **strategic foresight**, is a structured process that BSR uses for exploring the future, engaging with uncertainty, and considering unanticipated consequences—in order to act more responsible in

the present. Futures thinking and strategic foresight methodologies can therefore be used together with other **human rights due diligence (HRDD) activities**, including HRIA.

Futures thinking may be **most helpful in relation to two different aspects** of human rights impact assessments:

1. broadening horizons to consider a longer list of potential adverse human rights impacts, and
2. becoming more creative in defining actions to address this wider range of potential impacts.

As an example, the ubiquitous deployment of autonomous vehicles could lead to the emergence of private zones where driverless cars are unable or not allowed to travel, or to the identification of "wanted persons" who become trapped in their car while the police are called. Impacts on human rights might include freedom of movement, locational privacy, or arbitrary arrest. Considering this potential future scenario may allow companies to put in place a range of measures to avoid, prevent, or mitigate these potential future impacts.

In practice, the **following steps would be included as part of the futures methodology**, to identify potential impacts:

1. **Identify a plausible future development** relevant for the human rights impact assessment underway.
2. **Identify potential social, technological, economic, environmental, and political implications** ("first-order affects") arising from this plausible future development.
3. **Identify second- and third-order affects**.
4. **Compare all first-, second-, and third-order affects against a list of potential human rights impacts** derived from international human rights instruments—and identify the impacted rights.
5. **Brainstorm potential actions** the company can take, alone or in collaboration with others, to avoid, prevent, or mitigate these adverse human rights impacts (see Phase 4).

It is important to note that this exercise is not a substitute for a human rights impact assessment, but rather is intended to be one relevant and possible approach to contribute to HRIAs or other HRDD activities by anticipating plausible, important, and non-obvious future adverse human rights impacts.

Based on publications from BSR's Sustainable Futures Lab.

1.1.2 INVOLVEMENT IN IMPACTS

According to the UNGPs, businesses are required to consider potential and actual human rights impacts which are: **caused** by the business; impacts that the business **contributes** to; and impacts that are **directly linked** to a company's operations, products or services through business relationships, including both contractual and non-contractual relationships.[4] This implies that **the full digital ecosystem must be considered when impacts are assessed**, in order to be able to assess an individual company's involvement in human rights impacts.

The three different categories of involvement illustrate the many ways in which companies can be involved in negative human rights impacts, and that companies have a responsibility to prevent, mitigate and/or remediate those impacts. While determining how a company is involved with an impact (i.e. whether the company caused, contributed to, or is directly linked to an impact through its product or services) can support determining how to address it, these categories exist on a continuum of involvement and might require context-specific interpretations. In dynamic and fast-changing scenarios, it is important that an over-emphasis on determining the exact involvement of the company with the impact should not inadvertently delay action to address the issue. That other duty-bearers (i.e. states, companies, investors and others) may be more closely involved in an identified impact does not imply that companies that are further removed from the impact are free from responsibility. What responsibility a company has in terms of specific actions and activities will, however, differ depending on the type of involvement.

Limits of the responsibility: The boundaries that the UNGPs set for a company's responsibilities also means that companies are not expected to address all adverse human rights impacts that take place within their sectors, value-chain or ecosystem.

Company involvement depends on context: It is important to note that a company's responsibility in relation to the same activity may change over time, depending on the context, the company's own actions or omissions.[5] **As an example**, if a company is aware that it is directly linked to a negative impact through a business relationship, and fails to take steps to address the impacts, it may be seen to be contributing to the impact since the omissions facilitate the occurrence of the impact.

Table A, below, presents some illustrative examples of the three categories: caused, contributed to, and directly linked to.

TABLE A: EXAMPLES OF DIFFERENT TYPES OF HUMAN RIGHTS IMPACTS		
Type of impact	**Examples**	**Examples of potentially impacted rights**
Caused, by the company's own activities (actions or omissions)	• **A real estate company** purchases and deploys algorithms in its hiring processes in order to rank candidates based on predicted success within the company. The predicted success is based on historical data provided by the company, and while the algorithm was developed to not categorise candidates based on the protected characteristics, the algorithm ends up only recommending male ethnic majority candidates.	Right to equality and non-discrimination
	• **A software developer** developing a 'smart' voice assistant is gathering large volumes of data from the entirety of its userbase in order to improve its products. This is done without adequate privacy protections and without fully informed consent. The product can only be used if users agree to share the data with undisclosed third parties, implying a lack of informed consent.	Right to privacy
	• **A data engineering company**, contracted by the government, has developed a contact tracing app for use during the COVID-19 pandemic, but did not consider the need for significant data encryption capacity to protect the sensitive information collected and processed.	Right to privacy

	• **A bank** operating in a country with wide unionization restrictions, purchases and applies new 'smart' human resources systems that are supposed to help improve worker satisfaction and retention rates. The new system uses natural language processing to analyse internal emails between staff in order to assess worker sentiments. Employees agree to allow access to their emails as part of their employment contracts. After the systems are introduced the unionisation rates within the company drop significantly, since there is a fear among employees that unionisation efforts can more easily be identified by the employer and may lead to negative impacts for the employees.	Right to freedom of association
	• **A telecommunications company** is asked by the government of a country to shut down the internet in a specific region in the country where there is a lot of opposition to the ruling government. There have been peaceful protests against the government, organized through social media platforms. The telecommunications company does not have a policy or process in place for these scenarios and adheres to the government's request without asking any further questions.	Freedom of expression; freedom of association and peaceful assembly
Contributed to, through the company's own activities (actions or omissions) or through a third	• **A software developer** develops a digital product that can 'scrape data' on public social media platforms for commercial purposes. The product is sold to and used by a third party to scrape data and provide information about internet users to a government	Right to privacy; right to security of person

party, including cumulative impacts	that uses the data for surveillance of political opponents. The software developer should have been aware of the potential use-case and the related risks.	
	• **An AI developer** develops an automated decision-making algorithm for 'efficient hiring' and markets it to business customers. The developer does not inform purchasers of the product of the potential human rights risks and how those can be avoided, even though it knew that discriminatory outcomes and impacts on the right to privacy were possible.	Right to privacy; right to equality and non-discrimination
	• **A tech company** providing a social media platform which has widespread use is not reviewing or moderating content posted on the platform before elections in a country with known risks of ethnic violence and conflict, which might be fuelled by the content posted on the platform. The company is not seeking knowledge of the type of content that is being spread on the platform and takes a 'hands off' approach.	Right to health; right to security of person; right to equality and non-discrimination
	• A supermarket chain enters a partnership with a **start-up software developer** that will help the chain optimise product placement in its stores to boost sales. To that end, the supermarket installs cameras in a number of stores. The facial characterization technology developed by the start-up can identify the emotional state of customers. The technology also allows it to link the facial characterization to customers in the supermarket chain's loyalty	Right privacy; right to equality and non-discrimination

	programme, in order to identify loyalty programme members shopping behaviour. There are signs in the stores about the existence of cameras and information is shared when customers sign up to the loyalty programme, but only a small percentage of in-store customers are aware of the technology applied.	
	• **An advertising technology ('adtech') company** that has collected large amounts of user data from across various social media platforms and publishers has developed tailored user profiles based on user interests, including sexual ones. The company promotes its ability to help advertisers target specific 'valuable audiences' and facilitates a third party's purchase of ad space that is used to target those with an 'interest in homosexuality' with hate speech. The online speech leads to offline threats and violence.	Right to equality and non-discrimination; right to privacy; right to security of person; right to health; right to life
Directly linked, to operations, products or services through business relationships, including both contractual and non-contractual relationships	• A **sensor company** has sold a range of sensors to a car company, which after installing the sensors decides to enter a new market with its 'smart car-sharing' application. For the purpose of billing, a number of data points need to be collected on each ride, which users agree to when they join the car-sharing programme. To optimise efficiency and learn more about user behaviour, the operator decides to collect and process data from the duration of every ride. By analysing the full range of data collected the car company is able to analyse and record driver behaviour. The government demands the	Right to freedom of association; right to privacy

	company hands over the data. Thanks to the driver behaviour data the government is able to identify individuals that have joined a meeting of the political opposition and persecute them.	
	• An **AI developer** has developed a body language recognition product that a law enforcement agency purchases 'off-the-shelf'. The law enforcement agency applies the product in order to identify criminal suspects. The use of the product is leading to increases in wrongful arrests of ethnic and racial minorities.	Right to equality and non-discrimination; freedom of movement; right to liberty and security
	• **A private equity fund** invests in a biotech company operating in a country without data protection laws. Following its due diligence, the fund recommends changes in the company´s data protection practices. However, upon an external audit it is found that the company retained excessive data without the users' knowledge.	Right to privacy

Some of these examples come from: OHCHR (2012), *"The Corporate Responsibility to Respect Human Rights: An Interpretive Guide":* https://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf [Accessed July 29, 2020]; B-Tech Project (forthcoming), *"Foundational Paper series",* OHCHR; The Markkula Center for Applied Ethics at Santa Clara University (2018), *"Ethics in Technology Practice, Toolkit":* https://www.scu.edu/media/ethics-center/technology-ethics/BestPracticesinTechFinal.pdf [Accessed July 29, 2020]; Ebert, Busch & Wettstein (2020, *"Business and Human Rights in the Data Economy: A Mapping and Research Study*", German Institute for Human Rights & University of St. Gallen.

1.1.3 APPLYING HUMAN RIGHTS STANDARDS AND PRINCIPLES IN IMPACT ANALYSIS

As seen above, an adverse human rights impact occurs when an action or omission limits in whole or in part the ability of an individual to enjoy her or his human rights. But how exactly can we determine whether a human rights impact has occurred in practice?

Table B, below, provides some illustrative examples of how specific human rights standards and principles might be considered in the analysis of human rights impacts.

TABLE B: EXAMPLES OF USING HUMAN RIGHTS STANDARDS AND PRINCIPLES IN IMPACT ANALYSIS

Example scenario	Examples of human rights standards and principles for analysis	Rights impacted and related human rights instruments
A company is providing a facial recognition technology that is later used together with thousands of cameras and extensive datasets including biometric information, in a country with weak rule of law where human rights defenders are persecuted.	If there is no user consent during data collection, the right to privacy is clearly impacted in this example, both in relation to the initial data needed to develop the facial technology as well as in relation to the data gathered and treated when the technology is applied. However, other human rights standards may also be affected. For example, this scenario might affect the rights to association and to freedom of expression. It is possible that individuals may no longer wish to join particular organisations or participate political rallies.	• Right to privacy: UDHR art. 12; ICCPR art. 17 • Freedom of association and the right to form and join trade unions: UDHR art. 20; ICCPR art. 22; ICESCR art. 8 • Freedom of expression and information: UDHR art. 19; ICCPR art. 19 • Right to a fair trial: UDHR art. 11; ICCPR art. 14 and 15

TABLE B: EXAMPLES OF USING HUMAN RIGHTS STANDARDS AND PRINCIPLES IN IMPACT ANALYSIS		
Example scenario	**Examples of human rights standards and principles for analysis**	**Rights impacted and related human rights instruments**
	This scenario may also affect the rights to due process and fair trial, if the data gathered from the facial recognition technology is used to arrest and detain individuals. The specific application of the facial recognition technology may also be based on biased data, and could be applied in a biased way, which could have negative impacts on the right to equality and non-discrimination.	• Non-discrimination: UDHR art. 7, art. 23; ICCPR art. 26; ICESCR art. 2
A tech company has developed AI tools for a law enforcement agency and the corresponding criminal justice system, which has the result that increasing amounts of religious and ethnic minorities are prosecuted and convicted for longer sentences than	The right to non-discrimination is a cornerstone of international human rights law. This includes considerations of both direct discrimination (i.e. addressing unjustified differential treatment, to promote 'formal' equality) and indirect discrimination (i.e. addressing conditions which, whilst neutral in appearance, disadvantage certain protected groups, to foster 'substantive' equality). For example, the non-discrimination provision in the European Convention on Human Rights (Article 14) is now understood to prohibit neutral measures where these adversely affect certain minority groups.[6] First and foremost, the company in the example would need to ensure that the data used to develop the AI tool is not biased or	• Non-discrimination: UDHR art. 7, art. 23; ICCPR art. 26; ICESCR art. 2 • Right to liberty and security of person (and freedom from arbitrary arrest): UDHR art. 3; ICCPR art. 9 • Right to health: UDHR art. 25; ICESCR art. 12 • Right to education: UDHR art. 26; ICESCR art. 13

TABLE B: EXAMPLES OF USING HUMAN RIGHTS STANDARDS AND PRINCIPLES IN IMPACT ANALYSIS		
Example scenario	**Examples of human rights standards and principles for analysis**	**Rights impacted and related human rights instruments**
previously. The decision to use the AI tools cannot be challenged by defendants.	discriminatory. It would also be important to consider the potential discriminatory application of the AI tool itself, and the capacity of law enforcement and judges to use the AI tool in a way that is not discriminatory. Further, while discrimination might be the initial concern, there are a series of human rights related to the discriminatory development and application of the AI tool that are perhaps equally relevant. It can for example adversely impact the freedom from arbitrary arrest or the right to equality before the law. If an individual is sentenced wrongfully, this can have far-reaching impacts on the right to health, right to education, right to family life, and so forth.	• Right to family life: UDHR art. 16; ICCPR art. 23
A social media company has developed products and services that have been reported to cause addiction among young people and children.	Health is a fundamental human right that is indispensable for the exercise of other human rights, and every individual is therefore entitled to the enjoyment of the highest attainable standard of health. This includes both physical and mental health.[7] Furthermore, children are a vulnerable group that needs special protection and their healthy development should be promoted. Addiction to social media has the potential to	• Right to health: UDHR art. 25; ICESCR art. 12 • Right of the child to health: Convention on the Rights of the Child (CRC) art. 24 • Right to education: UDHR art. 26; ICESCR art. 13

TABLE B: EXAMPLES OF USING HUMAN RIGHTS STANDARDS AND PRINCIPLES IN IMPACT ANALYSIS		
Example scenario	**Examples of human rights standards and principles for analysis**	**Rights impacted and related human rights instruments**
	severely impact the well-being of children and the right to mental health. In the present example, the company should take steps to redesign its products and services so that they do not cause addiction and corresponding health impacts. Furthermore, impacts on the right to mental health can have a series of related impacts on children's rights, including the right of the child to education—if due to the initial impacts the child fails to continue with her/his education.	• Right of the child to education: CRC art. 28

Box 3, below, provides **further insight into how the right to privacy, specifically, can act as a gateway**, and that if those rights are negatively impacted many other interrelated human rights may also be impacted.

BOX 3: COMPANY INVOLVEMENT IN NEGATIVE IMPACTS: PRIVACY AS THE GATEWAY FOR HUMAN RIGHTS PROTECTION IN THE DATA ECONOMY

Contribution by Isabel Ebert, on behalf of the German Institute for Human Rights.

The interlinkages between human rights impacts and business operations in the data economy require new, holistic methods to identify, assess, prevent and mitigate negative impacts on human rights. This requires a degree of rethinking human rights in relation to the technological lifecycle and data ecosystem, and it requires a different mindset when thinking about actual and potential human rights impacts, away from linear thinking and towards building processes in multi-disciplinary teams that e.g. can identify blind spots in AI and find systemic biases in context-specific environments along all AI lifecycle stages, starting in product development.

Privacy has a gateway function for human rights protection in the data economy, meaning that adverse impacts on the right to privacy can lead to wide variety of further human rights impacts that companies can be involved in. That being said, it is important to re-emphasize that virtually all human rights can be affected by data-driven business and need to be taken into account.

An intrusion into the private sphere of an individual lays bare the data that data-driven business models require. Therefore, protecting and respecting the right to privacy will also protect other rights, such as freedom of expression and right to health, which is why it can be considered a gateway right. Conversely, failing to respect the right to privacy can be seen as a gateway for further human rights impacts in the data economy. Importantly, this privacy gateway logic should not overlook the exploitation of data that had initially been shared voluntarily by users and/or that later was combined in big data ecosystems. Moreover, even if a user might have withheld consent in the first place, data can still be shared for other means without consent, or one user might be impacting non-users by sharing their data on their behalf and without their consent (see Stakeholder engagement, for more on non-users vs rightsholders). These interdependencies between the use of individual data and interlinkages between users in a data ecosystem demonstrate that the right to privacy is a cornerstone in the discussion about digital rights, as an

ever-increasing number of rights is influenced by digital contexts. Moreover, it is not only about single individuals' rights, but instead about interconnected collective effects, as it touches upon a wide range of related rights.

Two examples illustrate how failure to respect the right of privacy can enable negative impacts on other human rights through insights gained by the initial privacy breaches:

1. A health insurance company might decide to use data from data brokers or other sources that reveal users' fitness levels, e.g. health data acquired from self-tracking devices. Hence, the insurer might choose not to offer an individual customer a competitive insurance policy based on data that the insurer obtained through breaching the privacy of the user. As a result, the right to health of the individual might be violated as rightsholders could face financial discrimination by having to pay a higher premium than those clients who willingly share their data with the insurance company, or they might be denied healthcare services altogether.
2. In the context of smart cities, users of various apps and technologies are transmitting valuable personal data on a daily basis, yet data sharing policies can be opaque. It is often unclear who is allowed to use what kind of data, and for what purposes. Business actors might in such scenarios treat personal data as a proprietary technology, use it for services unrelated to the original use case that they sought consent for, or sell personal data to third parties, thus infringing on the privacy and property rights of rightsholders. Third parties in turn might use the data for their respective purposes, such as hiring and recruiting, or health insurance schemes.

As shown above, even though the discourse around digital technologies and human rights has been largely focused on privacy, a wide range of human rights beyond privacy can be affected by the same technologies. Due to the global nature of the data economy, this phenomenon is not limited by sector-specific boundaries, national borders or legal jurisdictions. Instead, the data economy is built on the use of new technologies that enable transnational data flows and are applied in a wide range of interconnected sectors ranging from health care, insurance, and construction to food, private security, and a wide range of services.

Edited excerpt from "Business & Human Rights in the Data Economy" by Ebert, Busch and Wettstein, (2020) for the German Institute of Human Rights.

1.1.4 CUMULATIVE IMPACTS

Businesses may also be involved in cumulative impacts. **Cumulative impacts are the successive, incremental and combined impacts from multiple projects, products, services or activities affecting the same individuals.**[8] Different projects, products or services or different phases of a project can combine with incremental impacts from other existing, planned or future projects, products or services, leading to an accumulation of impacts. Table C, below, outlines some areas of concern around cumulative impacts from a human rights perspective.

TABLE C: HUMAN RIGHTS CONCERNS REGARDING CUMULATIVE IMPACTS

Why cumulative impacts must be considered	Examples
Cumulative impacts are areas of concern from a human rights point of view for a number of reasons: • **Cumulative impacts are often much harder to predict than singular impacts** from one project, product or service. Unless increased efforts are made by businesses and authorities to assess and analyse the potential for such impacts, it is much harder to prevent social changes that can have long-term impacts on human rights, such as the rights to freedom of expression, privacy, life and security of person.	When a facial recognition technology is used in combination with other tools, such as sentiment analysis, speech recognition and analysis, and so forth.
• While one or a **few pieces of 'borderline online content' (e.g. content that is close to amount to hate speech, misinformation or harassment) in isolation may not have significant human rights impacts**, when combined with thousands of pieces of similar content, it may result in severe cumulative human rights impacts. It is important to consider the cumulative impacts	A series of smaller events can trigger a much bigger social response if a 'tipping point' is reached, changing the situation abruptly, for example, many instances of 'borderline' online hate speech in conflict-affected areas can end up leading to offline communal violence.

since considering one piece of borderline content in isolation might result in leaning towards respecting freedom of expression; while considering thousands of pieces of borderline content in combination might result in leaning towards protecting personal security and safety.	A social response can also be triggered by poorly designed policies that prompt companies to repeat the same mistakes by not taking cumulative impacts into account.
• **Cumulative impacts can be severe**, **both in terms of the type of impact or the widespread nature of the impact**. Repetition may also increase the severity.	One camera with advanced facial recognition technology coupled with other digital products as well as biometric data and personal information can lead to severe impacts on an individual's right to privacy. The cumulative amounts of data gathered by companies can be shared and 'pooled' and thereby lead to significant impacts on the right to privacy due to the increased potential of highly accurate predictions and the ability to re-identify previously anonymised data. A singularly-occurring, minor impact such as incitement of violence that reaches a very limited group of individuals may not pose a significant human rights risk and therefore not be severe, but a series of such impacts may add up to a severe human rights impact.
• **Companies may not consider themselves responsible for cumulative impacts as they may make only a small contribution** to or are otherwise linked to these impacts.	One single actor providing a social media platform may collect only limited amounts of data, which is permissible and not harmful. However, many actors

This may especially be the case where their activities individually fit within socially acceptable limits, but the regulatory regime is not advanced enough to take account of accumulation of impacts over time.	may together collect large amounts of data, such as browsing history, location information, social media profiles and activities, which may be combined and which can then be used for targeted advertising that is discriminatory.
• **Populations most at risk are primarily affected by cumulative impacts**, as they are likely to have the least resilience to respond and the least capacity to demand a response from the authorities or businesses. This is particularly problematic in the case of cumulative impacts, since it may be more challenging for vulnerable or marginalised individuals and groups to seek a response from multiple actors contributing to the cumulative impact.	See the case above, where a lot of actors, including search engines, social media networks, and many others, may all be partly responsible for the cumulative impacts, which may require a response from all of them.
• **Cumulative impacts are sometimes slow and may build up incrementally over time**. Accordingly, it may be difficult to draw attention to the issues and prompt action from responsible parties.	If an individual is denied credit based on an algorithm developed with biased data, that denial may reduce that individual's credit score in other connected systems, making it less probable that the individual can e.g. secure an insurance policy; the lack of insurance may make it difficult for the individual to be qualified for a desirable professional position.[9] If these systems were not connected, the initial impact could have been minor; **in a connected ecosystem, there are more severe cumulative impacts**.

Source: Myanmar Centre for Responsible Business (MCRB), Institute for Human Rights and Business(IHRB) & DIHR (2015), *"Tourism Sector-Wide Impact Assessment (SWIA)":* https://www.humanrights.dk/projects/myanmar-centre-responsible-business [Accessed July 30, 2020];

BSR (2019), *"Google Celebrity Recognition API Human Rights Assessment: Executive Summary":* https://www.bsr.org/reports/BSR-Google-CR-API-HRIA-Executive-Summary.pdf [Accessed July 30, 2020]; BSR (2019), *"Human rights review: Facebook oversight board":* https://about.fb.com/wp-content/uploads/2019/12/Oversight-Board-Human-Rights-Review.pdf [Accessed July 30, 2020]; Ranking Digital Rights (2020), *"2020 Indicators"*: https://rankingdigitalrights.org/2020-indicators/#glossary-targetedad [Accessed July 30, 2020].

Because developers of digital products or services, companies using or applying those products or services, and regulators all tend to focus on assessing individual impacts of specific projects, products or services, they tend to not consider the totality of impacts and what the cumulative impacts mean for rightsholders.[10]

For these reasons, it is of utmost importance that HRIAs of digital activities include considerations of cumulative impacts. It also illustrates the importance of reporting and sharing findings of HRIA with other actors active in the same digital ecosystem, as addressing cumulative impacts is likely to require coordinated responses.

Box 4, below, outlines some risks of cumulative impacts specifically on the right to mental health. The impacts are cumulative since they do not concern the use of just one digital product or service, but rather that all kinds of applications aim to maximise the users time on screen. In other words, spending two hours a day on one application might not be problematic, but if you have an addiction to five or eight applications it might severely impact your mental health.

BOX 4: EXAMPLES OF CUMULATIVE PSYCHOLOGICAL IMPACTS

As shown throughout this Guidance, digital business projects, products and services can have a variety of negative human rights impacts. Such negative impacts—particularly when discussing social media platforms and applications developed to drive user engagement and increase screen time—can also involve mental health and well-being, a crucial component of the right to health, particularly as cumulative impacts within the digital ecosystem are considered.

A large body of evidence across cultures, age groups and online activities has demonstrated negative impacts on psychological health from internet-related technologies. These impacts can take many forms, as suggested by the non-exhaustive list below of potential business involvements.

- Businesses that create cyber environments meant to maximize user engagement and screen time may, together with other products and services that are pursuing the same goal, can contribute to the development of "Internet Gaming Disorder and other manifestations of "Problematic Internet Use", including inattention with detrimental effects

on academic or professional performance, loss of interest in other activities and relationship difficulties.

- Businesses that provide platforms for expression, but that do not adequately moderate against harmful content such as hate speech and cyberbullying, can contribute to adverse impacts on the mental health of vulnerable individuals and may contribute to a more extremist and polarized online culture and society. Cyberbullying may be an even bigger problem than traditional bullying due to the greater ease by which one can bully online, the around-the-clock access to bullying platforms and the permanent nature of the harassment. This has been correlated with an increase in the rates of clinical depression and suicide among victims.
- A business that shares users' personal data in a way that allows it to be utilized for political surveillance or other intrusive uses (potentially after combining it with many other data sources) can, as we have seen throughout this Guidance, directly compromise the right to privacy (among other severe impacts). The psychological literature teaches us that privacy mediates crucial mental health functions, including contemplation, rejuvenation, catharsis, recovery and autonomy. As such, a serious threat to privacy is also a serious threat to psychological health.

Sources: Aboujaoude (2011), *"Virtually you: The dangerous powers of the e-personality", New York: W.W. Norton;* American Psychiatric Association (2013), *"Diagnostic and Statistical Manual of Mental Disorders",* Arlington, VA; Aboujaoude (2015), *"Cyberbullying: Review of an Old Problem Gone Viral",* Journal of Adolescent Health; Aboujaoude (2019), *"Protecting Privacy to Protect Mental Health: The New Ethical Imperative",* Journal of Medical Ethics 2019; Pedersen (1997), *"Psychological functions of privacy",* Journal of Environmental Psychology; Newton (Feb 25, 2019) *"The Trauma Floor":* https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona [Accessed July 30, 2020].

1.2 ESTABLISHING IMPACT SEVERITY

When a full list of identified *actual* and *potential* impacts that a company *causes, contributes to* or is *directly linked to*, has been compiled the identified impacts need to be addressed. **In order to determine the order of priority in which the identified impacts should be addressed, the severity of the impacts should be defined.** The focus on the severity of impacts may lead a company to address an action with which it has less involvement over other impacts that it is more directly involved with, but which have less severe consequences. In other words, severe potential impacts that a company is directly linked to, may be prioritised for immediate preventive or mitigating actions over an impact that the company is contributing to, if the former has been identified as more severe.

As an example, a social media company may be contributing to potential negative impacts on the right to privacy since it has not created sufficient security systems to protect its platform against hackers. At the same time, the company is made aware of gender-based offline violence fuelled by false content spread on its platforms. The company is more involved in and has more direct control over the security systems but may decide to prioritise actions to mitigate gender-based violence because of the severity of impacts on the right to health, the right to security of person, the right to life and the irremediable character of such impacts.

It is important to note that the purpose of establishing impact severity is not to establish which impacts need to be addressed, but the priority with which these impacts should be addressed (see Phase 4: Impact Mitigation and Management).

According to the UNGPs[11], **the following should be considered when assessing severity**:

- **All adverse human rights impacts** that a company causes, contributes to or is directly linked to need to be addressed.
- Where it is not possible to address all impacts simultaneously, the impacts should be **addressed in order of their severity** (i.e. most severe impacts are addressed first).
- **Severity is determined by:**
    a) **Scope** (how widespread the impact is, or the number of people impacted)
    b) **Scale** ('seriousness' of the impact, or how grave the impact is), and
    c) **Irremediability** (the ability to restore impacted individuals to a situation at least the same as, or equivalent to, their situation before the impact).
- While it is not necessary for an impact to have more than one of the characteristics above to be considered 'severe', it is often the case that **the greater the scale or the scope of an impact, the less it is 'remediable'**.
- Assessment of severity should pay **special attention to how human rights impacts may differ for different groups or individuals** at heightened risk of becoming vulnerable or marginalised, including women, children, ethnic minorities, persons with disabilities, LGBT+ individuals, and others.

If many severe **potential** human rights impacts have been identified, and they cannot be dealt with simultaneously, **a second order consideration for prioritising action is the likelihood of potential impacts materialising**. This, according to the B-Tech Project at the OHCHR, includes considering:[12]

- **Developer or user interests, motivations and incentives**: Is it in the interests of users to use or misuse the products or services in ways that may pose risks? Is it in the interest of developers to develop the products or services in ways that may pose risks?
- **Users' technological know-how and capability:** Does the users' know-how (or lack of it) alter the likelihood that the use-case and adverse impacts identified will occur? Are there any existing technical barriers that will make the negative use-case unlikely in practice?
- **Developer's ability to consider human rights in the design:** Does the developer understand the concept of human rights to the extent that the digital product or service can be designed in a way that the identified potential human rights impacts can be avoided?
- **Local policy and laws:** Are there government policies and laws that will make the use-case more or less likely to occur in practice?

There are **five further points** to note regarding the assessment of impact severity:

1. Establishing impact severity must be undertaken **in dialogue with the individual rightsholders and community members who are or may impacted**, and/or with organisations that represent them. In ex-ante assessments, in particular, this may include engaging with rightsholder proxies (see Stakeholder Engagement Section, for more on rightsholder proxies).
2. **Consideration of vulnerability must be an integral component of establishing the severity of the impact**. For further explanation of the different factors that might give rise to vulnerability, see Stakeholder Engagement section.

For example, if a company asks for its employees' consent for using a 'smart' human resources tool that uses natural language processing to analyse worker sentiments, the impact on non-unionised part-time workers may be greater than on unionised permanent employees, since the former are less likely to be empowered to not consent.

Also, if a company uses automated decision-making in its credit risk scoring, a discriminatory or biased decision made on the basis of the scoring would be more severe for a poor individual than a wealthy individual, which perhaps also has the resources to appeal the decision.

3. In considering the scope—the number of people affected—it is essential to look not only at the absolute numbers of individuals affected, but to also consider in detail **who the individuals are** to ensure that any actual or potential discrimination is identified and included in assessing the impact's severity.

> **For example**, an analysis that focuses purely on the number of people affected might identify that for three identified actual impacts of a digital product, five out of 100 people experience each impact; however, if the five people impacted are always e.g. women human rights defenders, this should be observed in the analysis, as it may be due to systemic persecution against the particular group of people in the given context.

4. **Human rights expertise is key** to ensure that the assessment processes are adequately informed**.**
5. **Severity is not an absolute concept.** There is no universal threshold for when impacts are 'severe'. Rather, assessing severity of impacts is relative to the impacts identified. It involves professional judgment, dialogue, consideration of the interrelatedness of impacts (e.g. impacts on the right to privacy, a 'gateway right', might have impacts on a wide variety of other rights, such as right to security of person and right to freedom of assembly; see Box 3, above, for more) and analysis of long-term consequences.

1.2.1 FRAMEWORK FOR ASSESSING IMPACT SEVERITY

Above, it was clarified that severity of impacts is determined by considering the scale, scope and irremediability of the impacts. Table D below, provides one suggestion for how the above parameters to assess severity can be applied in HRIA practice.

TABLE D: PARAMETERS FOR EVALUATING IMPACT SEVERITY			
Scope	>20% of total population in area of impact or >50% of identifiable group	**A**	A human rights perspective places emphasis on rights and freedoms as they are enjoyed and exercised by specific individuals. It is therefore important to
	>10% of total population in area of impact or >10-	**B**	

	50% of identifiable group		consider scope (i.e. the number of people affected) not only in absolute numbers but also to consider more precisely, who the impacted individual users and other rightsholders are. Some impacts might be small in numerical terms but might be biased towards certain rightsholder groups that proportionally are hit harder. For example, maybe only 0.1% of users on a digital communication platform are impacted but if this is 25% of a religious minority, the latter number is more relevant than the former. Identifiable groups will be context specific ways of disaggregating the potentially affected people, for example female or male users etc.
	>5% of total population in area of impact or <10% of identifiable group	**C**	
Scale (including consideration of vulnerability)	May cause death or adverse mental or physical health effects that could lead to significant reduction in quality of life and/or longevity. This includes impacts on e.g. right to privacy that leads to related serious impacts on right to	**A**	Vulnerability needs to be an integral part of considering the scale, or seriousness, of the impact. This is because a person's particular circumstances, including their ability to respond to change, may have an influence on how 'serious' an impact may be for that individual. As well

	security of person or right to health.		as considering vulnerability as part of scale, assessors may wish to list vulnerability as a separate parameter, to demonstrate clearly how vulnerability has been considered in the analysis.
	A tangible human right infringement of access to basic life necessities (including education, livelihood, etc.) Impact to cultural, economic, natural and social aspects that have been identified as highly valued by identified groups or subject matter experts in the impact assessment process. Adverse impacts related to the delivery of public services that are identified as priority to livelihoods, health or safety in the impact assessment process. For example, an AI chatbot that supports individuals who are contacting public health services and that is less efficient in helping older persons, which leads to them receiving less adequate health advice than the general population.	**B**	
	All other impacts	**C**	
Irremediability	Difficult: the nature of the impact is such that it is difficult or impossible to remediate; complex	**A**	If an individual's right to health is impacted after being subjected to torture following in an arrest

	technical requirements make remediation difficult; there is little acceptance of remediation by the identified group; the business partner involved in the impact has low capacity to remediate the impact; there is no viable replacement for loss caused by the impact.		enabled by digital surveillance technology, it can essentially not be remediated. If the business model depends on extensive data collection and sharing it will be difficult to remediate the impacts related to the data that has been shared since it is out of one company's control to retrieve it.
	Moderate: the nature of the impact is such that it is possible but not easy to remediate; technical requirements for remediating impacts are simpler; the identified impacted group accepts remediation; business partner involved in impact can deliver remedy if supported with some capacity development.	**B**	If the user of the 'smart recruitment system' can be capacitated to use the system in ways that are not causing negative impacts on human rights, and is trained on how to seek proper consent for the use of the system.
	Easy: the nature of the impact is such that it is easy to remediate; technical requirements for remediating impacts are simple; the identified impacted group accepts remediation; business partner has capacity to remediate the impact.	**C**	A telecommunications company that has identified risks of working together with one specific data broker due to privacy concerns can decide not to work with that specific broker.

Source: Adapted to digital activities based on previous work by Danish Institute for Human Rights and Community Insights Group.

Table E, below, illustrates how the framework above can be applied.

TABLE E: EXAMPLES OF ASSESSING IMPACT SEVERITY				
Impact Scenario	**Scope**	**Scale**	**Irremediability**	**Overall assessment**
A company has developed an algorithm that is used by a country's justice system to assist in sentencing decisions by calculating flight and recidivism risks, leading to potential impacts on the right to due process and a fair trial when the automated risk assessments cannot be appealed.	B: Whilst the absolute number of people affected may be small in the case of a highly accurate algorithm that is only assisting judges, a further look into the case shows that the people primarily impacted are found to be indigneous and who have been identified as a vulnerable group.	A: There are human rights impacts of a significant scale due to the impacts on the right to a fair trial. This applies to everyone who is sentenced with support of the algorithm. However, the impacts are of an even greater scale in relation to the indigenous peoples impacted, since the impact on them is discriminatory in nature.	B: Depending on the nature of the sentences, it may not be possible to completely remedy the situation. For example, future job opportunities may be limited, implying life-long impacts. The sentences may cause long-lasting mental health impacts that and years of lost family life, that cannot necessarily be remediated. However, part of the impacts can be remediated by changing the discriminatory sentencing decision.	This might be considered to be an impact of high severity; it is an ongoing impact particularly impacting a vulnerable group and some cases (excessive prison sentences) cannot be remediated due to the related impacts on e.g. health and livelihood and right to family life.

1.3 ADVERSE IMPACTS AND BENEFITS

Human rights due diligence (HRDD), as outlined in the UNGPs, focuses on the 'adverse' human rights impacts of business activities. This raises the question of how generating benefits and positive impacts for individuals is to be considered in HRIA.

Businesses involved with adverse human rights impacts may try to focus the public's attention on the benefits of the digital projects, products and services they develop as strategies for legitimising those activities, rather than effectively addressing adverse impacts. According to the UN Guiding Principles **it is not acceptable for businesses to offset adverse impacts through positive contributions to human rights elsewhere.**[13]

> **For example**, this could include a company that develops surveillance technologies and claims that its technology is a 'net benefit' to society because it can help lower rates of violent crimes. However, its technology is also causing negative impacts on the right to freedom from discrimination due to increased wrongful arrests of individuals belonging to ethnic minority groups.

The UNGPs emphasis that, **first and foremost, companies should identify and address any adverse human rights impacts associated with their activities**. Any positive contributions should be separately considered.

Making a **clear distinction between positive contributions** (through, for example, increased efficiency in public administration, optimising user experiences, connecting individuals and promoting freedom of expression, or providing increased access to information) **and identifying and addressing negative impacts** (i.e. conducting human rights due diligence) is important for a number of reasons. **For example:**

- **Including both adverse impacts and positive contributions in the same assessment facilitates a space for the implicit offsetting of adverse impacts**—e.g. a company showcases the increased efficiency of decisions in standard administrative processes as a way of moving the emphasis away from adverse impacts caused by the automated decision-making involved, including human rights issues related to right to due process and its potentially flawed underlying data and assumptions made on the basis of that data.
- A human rights perspective places a significant emphasis on accountability, including the ability of rightsholders to claim rights and respective duty-bearers to meet their duties and responsibilities with regard to human rights.

This includes **recognising the differentiated yet complimentary duties and responsibilities of state and non-state duty-bearers**.

At the same time, it is important to recognise that the implementation of the UNGPs can be the single most important contribution to the realisation of human rights as well as the sustainable development goals.[14]

HRIA of digital activities include and refer to positive steps or outcomes to the extent that these are relevant in impact analysis and mitigation planning. However, the assessment itself is not focused on an evaluation of the business's contribution to human rights enjoyment. While the distinction between an action to address adverse impacts and a 'positive impact' or contribution may not necessarily always be clear-cut in practice, the point is that the HRIA should focus on the actual and potential adverse human rights impacts with which the business is involved and not on ad hoc positive contributions that do not relate to addressing such impacts.

One further aspect to note is that **strategic philanthropic projects** in the form of digital projects, products or service (e.g. a company making its digital products and services freely available to underprivileged school children to support digital learning) are considered to be a part of company operations and as such, may be included in the scope of HRIA. However, to the extent such projects are included in the scope of a HRIA the **primary focus should be on whether such initiatives have any adverse impacts on human rights in the way that they are selected, designed, implemented and monitored** (e.g. the digital products and services made freely available to vulnerable groups also collect data that is later used for targeted advertising).

END NOTES

[1] See e.g. Ranking Digital Rights (2019), *"Consultation Draft – Human Rights Risk Scenarios: Targeted Advertising"*: https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf [Accessed July 29, 2020].

[2] Sam Shead (Aug 21, 2020), *"How a computer algorithm caused a grading crisis in British schools"*, CNBC: https://www.cnbc.com/2020/08/21/computer-algorithm-caused-a-grading-crisis-in-british-schools.html

[3] See e.g. Access Now (June 4, 2016), *"Zero rating: a global threat to the open internet":* https://www.accessnow.org/zero-rating-global-threat-open-internet/ [Accessed September 22, 2020].

[4] UN Guiding Principle 13.

[5] B-Tech Project (2020), *"A B-Tech Foundational Paper: Taking Action to Address Human Rights Risks Related to End-Use:* https://www.ohchr.org/Documents/Issues/Business/B-Tech/taking-action-address-human-rights-risks.pdf [Accessed September 16, 2020].

[6] See e.g., *Thlimmenos v Greece* (2000), Bihar Human Rights Commission 12.

[7] Committee on Economic, Social and Cultural Rights (2000), *"General Comment No. 14: The right to the highest attainable standard of health (Art. 12)",* E/C.12/2000/4.

[8] Franks, Brereton & Moran (2011*), "Cumulative Social Impacts", in* Vanclay & Esteves (2015)*, "New Directions in Social Impact Assessment: Conceptual and Methodological Advances"*: https://www.rug.nl/research/portal/files/17534793/IAIA_2015_Social_Impact_Assessment_guidance_document.pdf [Accessed July 30, 2020].

[9] Hin-Yan Liu (2019), *"The digital disruption of human rights foundations",* in Human Rights, Digital Society and the Law: A Research Companion, Chapter: 5, Publisher: Routledge, pp.75-86.

[10] United Nations (2020), *"United Nations Global Compact, Human Rights and Business Dilemmas Forum, Cumulative impacts*": https://hrbdf.org/ [Accessed July 30, 2020].

[11] UN Guiding Principles 12 and 24.

[12] B-Tech Project (2020), *"A B-Tech Foundational Paper: Identifying and Assessing Human Rights Risks related to End-Use:* https://www.ohchr.org/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf [Accessed September 16, 2020].

[13] UN Guiding Principle 11.

[14] Danish Institute for Human Rights (2019), *"Responsible business conduct as a cornerstone of the 2030 Agenda – a look at the implications"*: https://www.humanrights.dk/publications/responsible-business-conduct-cornerstone-2030-agenda-look-implications

THE DANISH INSTITUTE FOR HUMAN RIGHTS