THE TECH SECTOR AND NATIONAL ACTION PLANS ON BUSINESS AND HUMAN RIGHTS

A THEMATIC SUPPLEMENT TO THE "NATIONAL ACTION PLANS ON BUSINESS AND HUMAN RIGHTS TOOLKIT 2017 EDITION"

JULY 2020

THE DANISH INSTITUTE FOR HUMAN RIGHTS

GLOBAL PARTNERS DIGITAL

THE TECH SECTOR AND NATIONAL ACTION PLANS ON BUSINESS AND HUMAN RIGHTS
A thematic supplement to the "National Action Plans on Business and Human Rights Toolkit 2017 edition"

July 2020

The Danish Institute for Human Rights (DIHR) is Denmark's national human rights institution. Its mandate is to promote and protect human rights and equal treatment in Denmark and abroad. The Human Rights and Business Department is a specialised unit within the DIHR focusing on the role of the private sector in respecting human rights.

Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

Report Authors:

Richard Wingfield
Head of Legal at Global Partners Digital

Ioana Tuta
Adviser, Human Rights and Business at the Danish Institute for Human Rights

Tulika Bansal
Senior Adviser, Human Rights and Business at the Danish Institute for Human Rights

ACKNOWLEDGMENTS

The authors would like to thank all of those who supported the development of this thematic supplement. Particular thanks goes to Sebastian Smart who helped develop the first draft of the supplement. The authors would also like to recognise the contribution of the Equal Rights Trust and thank their Head of Legal and Programmes, Ariane Adam for her input in highlighting the discriminatory impacts of the activities of the tech sector, outlining state and private actor non-discrimination obligations and private actor responsibilities, and providing guidance on how such obligations and responsibilities should be addressed in the NAP process and content.

The authors also pay thanks to the many reviewers of the initial draft of this thematic supplement, and whose comments, feedback and suggestions were invaluable: Dunstan Allison-Hope, Rémy Friedmann, Nora Götzmann, Emil Lindblad Kernell, Rikke Frank Jørgensen, Peter Micek, Daniel Morris, Isedua Oribhabor, Jason Pielemeier, Dr. Roxana Radu, Sabrina Rau, Elin Wrzoncki and the Australian Human Rights Commission.

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

68 Hanbury St, Spitalfields
London E1 5JL, United Kingdom
www.gp-digital.org

e-ISBN: 978-87-93893-56-6

CONTENTS

1. Introduction

Recent decades have seen wide-ranging transformations in almost all areas of human activity as a result of digital technological innovation and development, with significant consequences for the equal exercise and enjoyment of human rights. There is no doubt that digital technology offers a range of opportunities to enhance the realisation of a wide range of human rights. Digital technology can provide greater access to education and healthcare, and make the provision of these and other public services more efficient. New online platforms have enabled individuals to access and share news, information and ideas more easily, as well as communities and groups to mobilise and assemble.

As this thematic supplement was being written, the world came to a near standstill due to the COVID-19 pandemic. Through it, we saw how society became increasingly dependent on digital technology: to stay in touch with our family and friends, for educational purposes, to speak to colleagues in the workplace and, perhaps most importantly, to receive information.

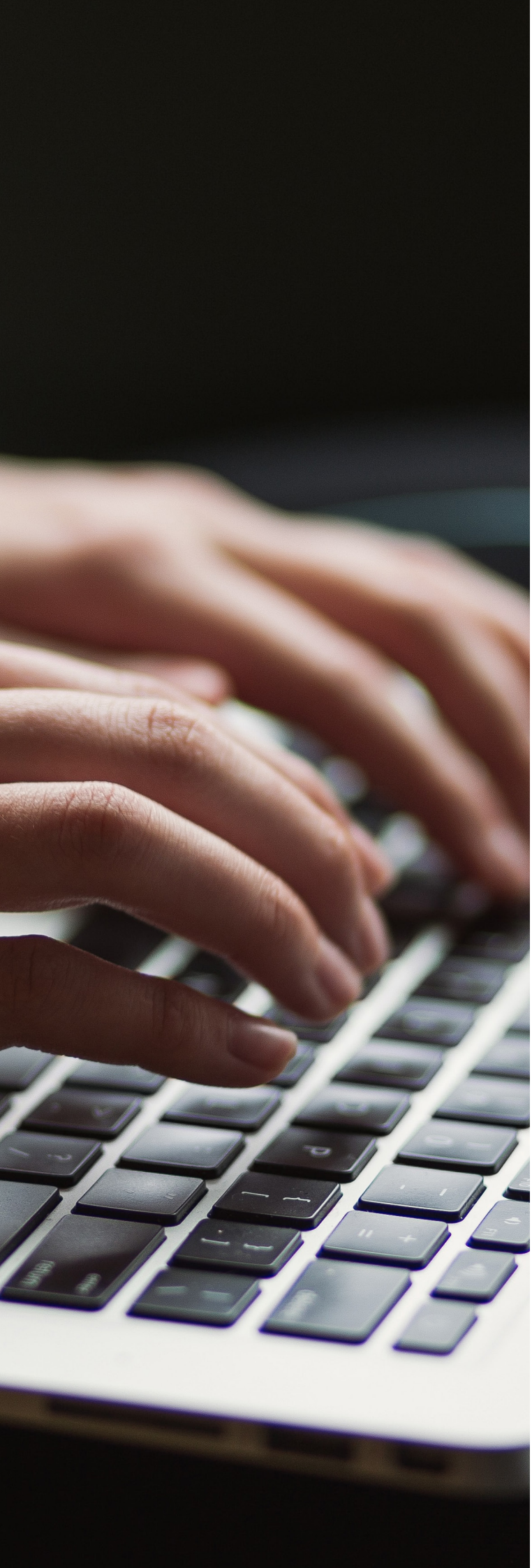
However, certain applications of digital technologies can also pose serious risks to human rights. The activities of tech companies in particular, such as software developers, social media platforms, search engines and internet services providers have been linked to adverse impacts on the rights to privacy, freedom of expression, freedom of association, non-discrimination and even the right to life.[1] As with the benefits of technology, times of crisis often reveal the risks. COVID-19 saw misleading information about the virus spread on online platforms, and tech companies with questionable records on data protection and privacy offer "solutions" to governments on how to monitor individuals and populations.

The human rights impacts associated with the development and deployment of digital technologies have been on the public agenda for almost two decades, with increasing attention paid to the operations and business models of the "big tech" companies, i.e. the most dominant companies in the tech sector. The features of the large-scale use of digital technologies, however, raise unique challenges for the protection and respect of human rights:

- Impacts take place at both the national, regional and global level as a result of the globally interconnected internet infrastructure, meaning national-level responses are often ineffective or insufficient;

- The scope of the impacts is far-reaching with millions of users (and other individuals) facing human rights risks;

- The link between tech companies and human rights abuses is not always obvious because of the highly specialised nature of their activities, and the lack of transparency in the development of digital technologies such as automated decision-making and artificial intelligence;



©Kaitly Baker

• The identification of human rights risks can be complicated by the rapid pace of development and innovation in the field;

• Some of the issues raised are new and therefore have been addressed to a limited degree in international jurisprudence and human rights legal scholarship. (It should be noted that recently there has been increased emphasis and attention to the link between human rights and the tech sector, not least by different UN Special Rapporteurs.)

The general understanding and awareness of human rights linked to digital technologies has been on the rise in the business sector. High-profile cases such as the Cambridge Analytica case and the Snowden revelations have received significant attention, contributing to a vibrant political debate on the human rights responsibilities of both states and businesses in the age of big data and social platforms. Nonetheless, the tech sector is addressed only in a very limited manner in existing National Action Plans on Business and Human Rights (NAPs), if at all (see Section 1.3), despite the fact that NAPs are critical opportunities for states to develop and set out the measures that will be taken to ensure that human rights will be protected and respected when it comes to tech companies' activities. There is, more broadly, a need for greater synergies between the business and human rights and the tech communities, as a crucial element for advancing the accountability of tech companies,

and designing regulatory and policy frameworks which are fit for purpose and aligned with international human rights standards.

1.1 ABOUT THIS THEMATIC SUPPLEMENT

Against the backdrop of the challenges outlined in the introduction, this thematic supplement has been developed as a tool to assist state actors and other stakeholders in the development of NAPs, and aims to provide advice on the integration of tech sector-related risks. It complements the toolkit developed by the International Corporate Accountability Roundtable and the Danish Institute for Human Rights on NAPs (the ICAR-DIHR Toolkit).[2]

This thematic supplement is primarily targeted towards states that are engaged in the process of initiation, consultation, drafting, implementation or updating of NAPs, and in both states where digital technologies developed by tech companies are used (host states) and where multinational tech companies are domiciled or registered (home states). However, it may also be useful for civil society organisations, tech companies and other stakeholders engaged in the NAP process.

As of 1 June 2020, NAPs have been adopted in 24 states as an important step towards the dissemination and implementation of the UN Guiding Principles on Business and Human Rights (UNGPs).[3] Endorsed by the Human Rights Council in 2011, the UNGPs make clear that that business enterprises have a responsibility to respect human rights wherever they operate independently of states' ability to fulfil their own human rights obligations (Principle 11).

The UNGPs also reiterate the state duty to protect against abuses by business enterprises by taking appropriate steps to prevent, investigate, punish and redress through effective policies, legislation, regulations and adjudication (Principle 1). The UNGPs provide a strong normative basis to assess tech sector-related human rights impacts and develop concrete policy actions and measures to close protection gaps. Some of the NAPs which have been adopted do already make references to digital technology and the tech sector;[4] however, most references remain broad and lack the level of ambition required to address the scale and scope of negative human rights impacts in the sector.

While all human rights can be impacted by the digital technologies developed by tech companies, this thematic supplement focuses on three of the rights most affected: the rights to privacy, freedom of expression and equality/non-discrimination. This supplement will be updated in the future to include other technology and tech sector-related human rights issues so that it can become a convergence point for organisations working at the intersection of technology and human rights.

This thematic supplement is structured in three sections.

The rest of **Section 1** provides information on the scope of this thematic supplement, and a reflection on existing references to the tech sector in NAPs.

Section 2 looks at the relationship between the tech sector and human rights, focusing on the rights to privacy, freedom of expression and equality/non-discrimination, with an overview of the tech sector's impacts on these rights, as well as regulatory trends.

Section 3 starts by looking at how tech sector-related considerations can be included in the NAP process, with a focus on stakeholder mapping and engagement and the involvement of groups at risk. The section then looks at how tech sector-related considerations can be included in the contents of NAPs themselves, and includes a "Tech Sector and NAPs National Baseline Assessment (NBA) Template" with guiding questions to assess existing human rights protections in relation to the tech sector and uncover gaps in the implementation of the UNGPs in this respect. The two tools - the NBA Template and the NAP checklist - should be used in conjunction with the more comprehensive ICAR-DIHR Toolkit to develop, evaluate and revise NAPs.

This thematic supplement should be taken as a set of minimum elements for consideration in the development of a NAP. State actors should always consult with relevant stakeholders that operate in and/or may be affected by the tech sector throughout the development and implementation of NAPs to ensure that it will be as effective as possible.

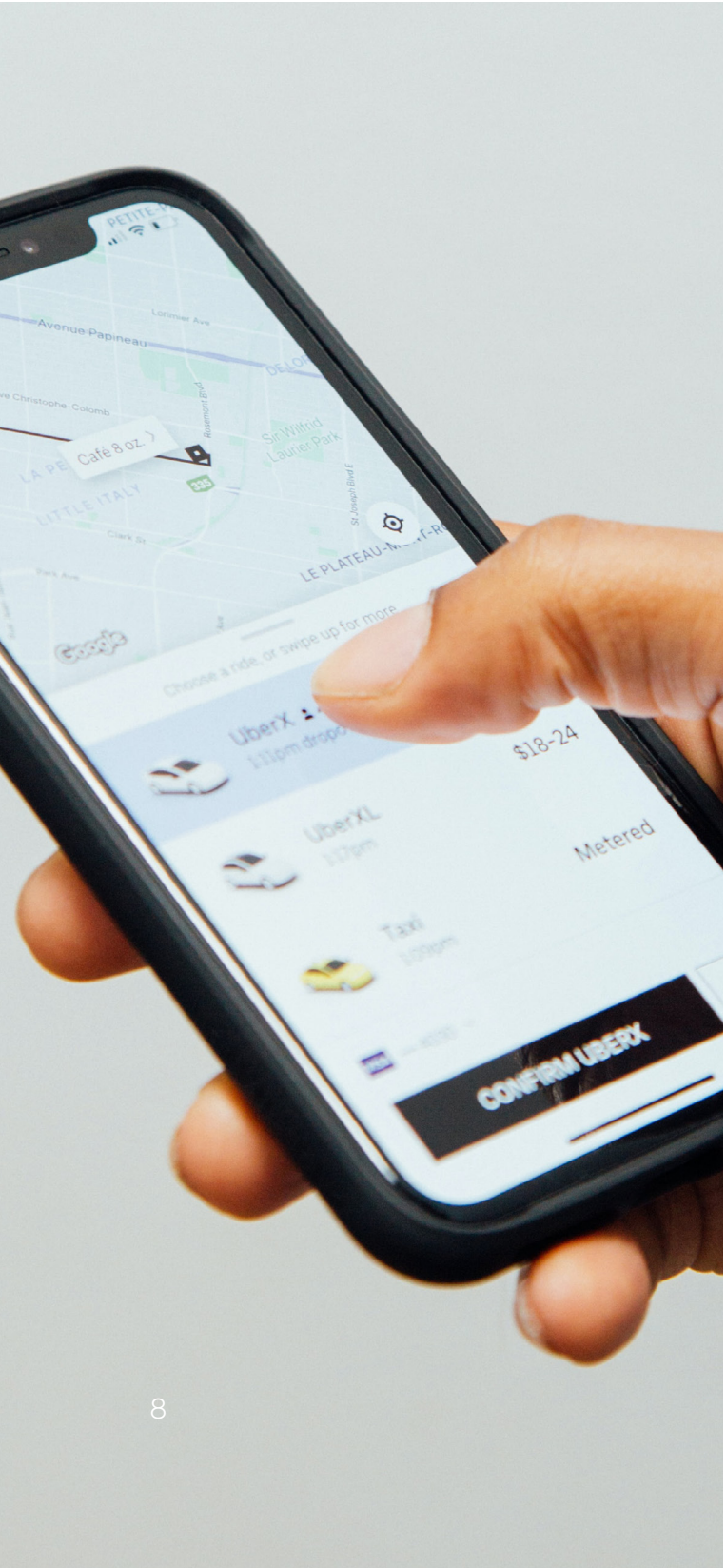
1.2. THE SCOPE OF THIS THEMATIC SUPPLEMENT

1.2.1. COMPANIES IN SCOPE

The scope of this thematic supplement is the "technology sector" (or "tech sector"). There is no single or authoritative definition of the type of industries and companies covered by this category. What complicates a clear definition is the fact that almost all companies today, regardless of sector, size or location, use the internet and digital technology to develop and distribute their products and services. A logistics company might use specific management software, a retailer may provide goods through an online platform or may market its products online, a financial institution might use cloud computing services to store and manage vast amounts of data.

Moreover, the definition of the sector can become contentious when it has implications for the enforcement of regulation. For example, "gig" companies such as Uber and Airbnb have been challenged over their self-categorisation as platform companies which allows them to evade compliance with the stricter regulatory requirements applicable to traditional transportation and hospitality companies. Several courts around the world have heard

cases to decide whether Uber is a digital service or just a traditional company using digital technology.[5] In a 2017 landmark judgement, the European Court of Justice held that Uber is a transportation company - and not an information society service - and therefore subject to rules on taxi licensing.



©Charles Deluvio

Against this dynamic backdrop, this report does not propose a particular definition of the "tech sector", but notes that, at its broadest, it can be understood to comprise the cluster of industries whose business model enables access to and the functioning of the internet and digital technologies, including the development and distribution of digital products, services and content. This broad understanding would mean that the tech sector includes telecommunication companies; internet service providers; domain names companies such as registries and registrars; internet companies that provide content; communication and services such as search engines, social media platforms, messaging apps; and hardware and software companies including network equipment vendors.

In light of the limited human rights focus of this thematic supplement, i.e. the rights to privacy, freedom of expression and equality/non-discrimination (see section 1.2.2), the report focuses (and provide examples) primarily from those industries and companies where these human rights issues have been widely documented and are particularly salient. Notwithstanding this focus, many of the elements of this thematic supplement, in particular those related to privacy and data protection, will also apply to many other companies that use digital technology in some way, and so the impacts of a NAP which is developed in accordance with this guidance will have a broader reach.

The approach of the Sustainability Accounting Standards Board to defining the tech sector

The Sustainability Accounting Standards Board (SASB) is an independent standards-setting organization for sustainability accounting standards. SASB identifies five industries in the Technology and Communication sector: electronic manufacturing services and original design manufacturing;[6] hardware;[7] internet media & services;[8] semiconductors;[9] software and IT services;[10] and telecommunications.[11]

Given the increasing integration and convergence in this sector, a company can simultaneously belong to more than one of these industries. For example, a company such as Google active in multiple business segments is a search engine, a software developer and internet infrastructure company at the same time.

Human rights impacts beyond the tech sector

While the focus of this thematic supplement is on the human rights impacts of tech companies, any company which uses, deploys or relies upon digital technology can, in doing so, also potentially adversely impact individuals' human rights.

One example is the use of surveillance technology by companies to monitor their employees while at work, which can constitute a violation of the right to privacy. A 2018 survey by Gartner found that almost a quarter of organisations worldwide are using employee-movement data, and 17% are monitoring work-computer-usage data.[12] Some companies monitor their employees' use of social media even when they are not working, and there are cases where employees have had their employment terminated for expressing their opinion through social media.[13]

The increase in home working due to COVID-19 has led to some employers using new digital tools to monitor their staff remotely, including the websites that they visit. Digital products such as Sneek, which takes photographs through laptop cameras every few minutes, are being used by some employers to ensure that employees are using their laptops during working hours.[14]

Another example is the increased use of artificial intelligence by a range of different sectors, such as the financial services sector to make decisions about whether a person is eligible for a loan, or to determine the interest rate. There is strong evidence of the use of automated decision making in such instances leading to discriminatory outcomes, including on the basis of race and ethnicity.[15]

1.2.2. HUMAN RIGHTS IN SCOPE

This first iteration of the thematic supplement focuses on three of the human rights that have been most frequently considered in respect to the impacts of the tech sector: the rights to privacy, freedom of expression and equality/non-discrimination. As noted above, this thematic supplement will be updated to include other tech sector-related human rights issues so that it can become a more comprehensive resource.

The rights to privacy and freedom of expression are notably important since they are often considered as enabling the enjoyment of other human rights. For example, the right to privacy can enable the free development of an individual's personality and identity, and her ability to participate in political, economic, social and cultural life.[16] By taking advantage of the anonymity that certain online platforms provide, or encryption tools which guarantee confidentiality, individuals may feel more free to discuss personal or sensitive issues, and to engage in debate on controversial issues where speaking openly could lead to harassment or violence.

The enjoyment of freedom of expression - which includes the ability to impart, seek and receive information - is a catalyst for the realisation of associated rights such as the rights to freedom of association and peaceful assembly, the right to take part in the conduct of public affairs, the right to education, the right to take part in cultural life, and the right to enjoy the benefits of scientific progress and its applications. For example, it is often through online platforms that individuals have been able not only to communicate, but to organise protests or other mass movements. A range of online educational platforms and tools are now accessible to people whose opportunities to take advantage of more traditional forms of education are limited.

Non-discrimination constitutes a basic and fundamental principle relating to the protection of all human rights.[17] International human rights law recognises that to respect and guarantee human rights requires doing so without discrimination. The UNGPs also emphasise that they should be implemented in a non-discriminatory manner and, in the commentary to Principle 3, highlight that the failure to enforce existing laws on non-discrimination that directly or indirectly regulate business respect for human rights is often a significant legal gap in state practice.

The interrelatedness of all human rights works both ways, as well, meaning that adverse impacts upon the rights to privacy, freedom of expression, and equality/non-discrimination can also lead to restrictions on other human rights.

The rights to privacy, freedom of expression, and equality/non-discrimination

The right to privacy has long been recognised in international human rights law. Inspired by the wording of Article 12 of the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) provides at Article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks".

The right to freedom of expression can broadly be defined as an individual's right to freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Article 19(2) of the ICCPR, largely mirroring the language of Article 19 of the UDHR, provides that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".

The right to freedom of expression is strongly linked to the right to freedom of opinion. Article 19(1) of the ICCPR (again, mirroring the language of Article 19 of the UDHR), provides that "everyone shall have the right to hold opinions without interference".

While the right to freedom of opinion is an absolute right (i.e. no interference with the right can be justified), this is not the case for the rights to privacy and to freedom of expression, which are both non-absolute rights. However, they can only be limited or restricted in certain circumstances where:

- There is a clear legal basis;
- It is in pursuance of a legitimate aim; and
- It is a necessary and proportionate response to that aim

The rights to equality and non-discrimination have also long been recognised in international human rights law. Indeed, the right to non-discrimination underpins international human rights law with Article 2(1) of the ICCPR requiring that the rights recognised in the Covenant be respected "without distinction of any kind" thereby prohibiting discrimination in the enjoyment of all human rights (and mirroring, in part, Articles 2 and 7 of the UDHR). Article 26, however, provides a freestanding right to equality, building upon Article 7 of the UDHR, providing that:

- All persons are equal before the law;
- All persons are entitled without any discrimination to the equal protection of the law; and
- States must ensure that the law prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground.

The UN Human Rights Committee has noted that Article 26 of the ICCPR "prohibits discrimination in law or in fact in any field" and is therefore not limited to those rights which are provided for in the Covenant.[18]

The Human Rights Committee has also noted that to fulfil their non-discrimination obligations, states are required to adopt comprehensive anti-discrimination legislation.[19] As such, where states have duly implemented the right to non-discrimination, companies in the tech sector (as well as the private sector more generally) will have legally binding obligations not to discriminate in any area of activity.

As with the rights to privacy and freedom of expression, the rights to equality and non-discrimination are not absolute rights. Differentiation of treatment will only be permissible, however, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a legitimate purpose.

1.3. REFLECTIONS ON TECHNOLOGY IMPACTS IN EXISTING NAPS

As of 1 June 2020, NAPs have been adopted in 24 states.[20] Ten of these NAPs make reference to the tech sector. Of these, five contain specific actions and commitments relating to the tech sector. The other five simply note that there are human rights impacts related to the tech sector. The text of the ten NAPs which mention the tech sector can be found in Annex 1 to this thematic supplement, along with details of implementation of actions, where relevant and available.

In summary, the action points in the five NAPs which make commitments relating to the tech sector are varied: one relates to a roundtable on data protection (Finland), one to regulation of intermediary liability (Poland), one to guidance on the export of information and communications technology (United Kingdom), one on a mechanism to help identify lessons learned and best practices related to companies that promote human rights online (United States), and one on developing plans and measures to help workers who are replaced by technology (Thailand). In only one of these cases (the United Kingdom) has the state provided details on how the commitment has been implemented.[21]

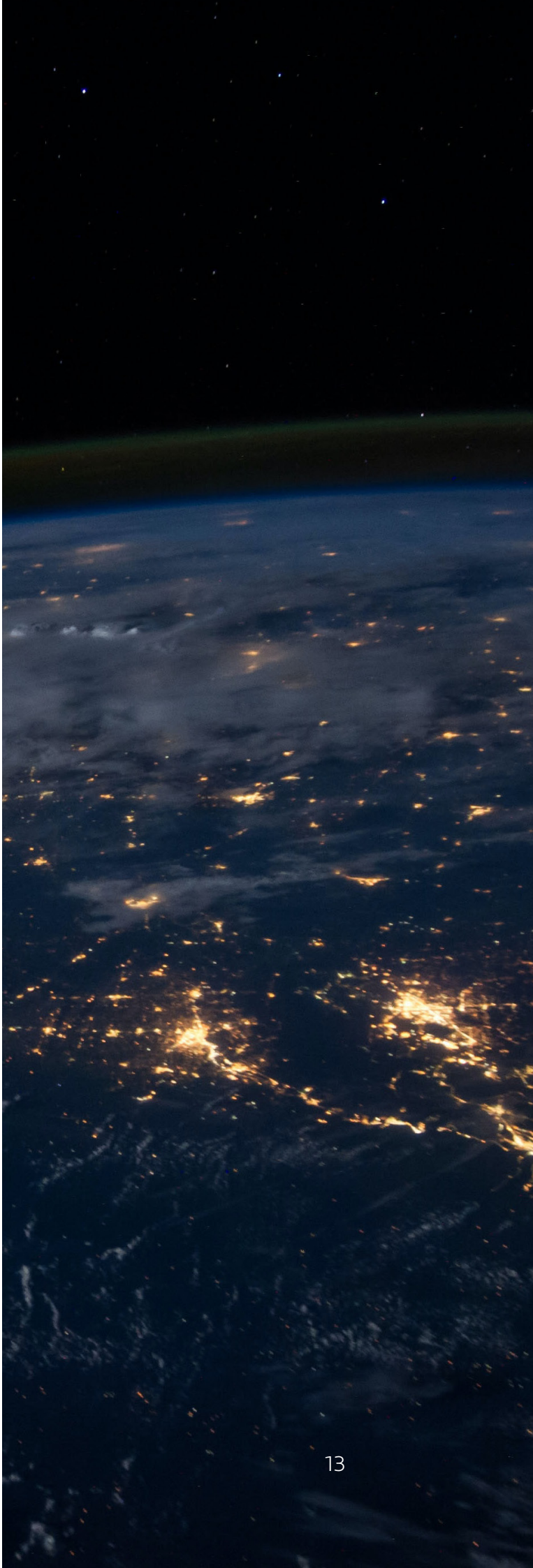
Three observations can be made based on the language and commitments in existing NAPs:

1. The wide range of risks to human rights, particularly privacy, freedom of expression and equality/non-discrimination, stemming from the activities of the tech sector are not fully considered in any NAPs

published so far. The NAPs which look at the tech sector tend to examine only one narrow aspect of the human rights risks posed by the sector, such as privacy (Finland), freedom of expression (Poland) or the right to work (Thailand). The right to non-discrimination is considered primarily in relation to employment, and the wide-ranging discriminatory impacts of the use of new digital technologies are unaddressed. While this might reflect the state's prioritisation of the most serious issues in its NAP, it may also represent a failure to fully consider the diverse range of human rights impacts that stem from the tech sector.

2. None of the commitments in the four NAPs with commitments related to the tech sector can be considered as fully SMART (specific, measurable, achievable, relevant and time-bound).[22] None of the five NAPs provide details on timelines for fulfilling the commitment or funding that would be provided. Nor do any of the four provide details on how outcomes would be publicised and their impact monitored.

3. None of the NAPs commitments related to the tech sector address Pillar III of the UNGPs which focuses on access to remedy. The focus in these five NAPs is on Pillar I (e.g. regulation of intermediary liability) and Pillar II (e.g. guidance on considering human rights when exporting technological products, and sharing best practice from corporate policies that promote human rights online).



© Nasa - Unsplash

2. THE TECH SECTOR AND HUMAN RIGHTS IMPACTS

As noted in Section 1., tech companies, and the digital products and services they develop and distribute, offer a range of opportunities to support the realisation and enjoyment of human rights. The development of strong encryption products helps protect the right to privacy, keeping people's personal data and communications secure. This is particularly important to groups at risk of discriminatory treatment by state or private actors. Social media platforms have provided new ways for billions of people around the world, including marginalised groups, to have their voices heard, making it easier than ever to communicate, and share information and ideas, strengthening equal enjoyment of their right to freedom of expression. And, as noted in Section 1.2.2., the rights to privacy and freedom of expression act as "gatekeepers" to the equal enjoyment of other associated rights. Such products and services also have broader benefits for human rights, enabling victims of human rights abuses to help expose and raise awareness of violations, as well as seek and obtain remedies.[23]

However, at the same time, these companies, and their products and services, can create risks to the rights to privacy, freedom of expression and equality/non-discrimination. A NAP that takes into consideration the tech sector can help avoid or mitigate such risks.

2.1. THE RIGHT TO PRIVACY (INCLUDING DISCRIMINATORY IMPACTS)

The business model of many tech companies relies upon the collection and processing of large amounts of personal data about the online and offline behaviour of individuals. This data is often used to create highly sophisticated profiles, covering many personal and sensitive aspects of a person's identity. While often used for commercial purposes, such as to enable micro-targeted advertising (a practice which, itself, has raised concerns relating to privacy, freedom of expression and equality/non-discrimination),[24] it has also been used to track and surveil individuals by the companies themselves, and sometimes provided to or hacked by state actors, such as law enforcement agencies. With the advent of new technologies such as 5G, the Internet of Things, and artificial intelligence (AI), the amount of data collected will only increase, meaning the prevalence of such uses of data will too.

This kind of business model has been increasingly scrutinised for its actual and potential adverse impacts on the rights to privacy and equality/non-discrimination. Personal data (including metadata), whether collected and

© Ev - Unsplash

shared with or without the consent of the individuals concerned, is not only used in and of itself, but is shared and correlated with other data sources to create even more highly detailed individual and group profiles. The consolidation of different data points in datasets, even if seemingly anonymised, raises critical questions about the users' rights to know, consent and exercise control over their personal data in accordance with their right to privacy. And as technology becomes more powerful, it is becoming easier to collect and process "big data", i.e. extremely large datasets. According to the UN Special Rapporteur on the right to privacy "the tendency of Big Data to intrude into the lives of people by making their informational selves known in granular detail to those who collect and analyse their data trails is fundamentally at odds with the right to privacy and the principles endorsed to protect that right".[25]

The Special Rapporteur has also highlighted the recognition of the right to privacy in international instruments as "a right strongly linked to concepts of human dignity and the free and unhindered development of one's personality".[26] The ability to maintain distinct contexts in which one discloses or conceals their identity without data surveillance can be crucial for groups at risk of discrimination; for example it can be crucial for LGBTI people living in a country where same-sex intimate conduct is stigmatised or illegal.[27]

Datasets are increasingly analysed by algorithms and other forms of AI, new technologies which are rapidly becoming part of the essential infrastructure of our societies. However, we are only beginning to understand the human rights impacts of AI, big data and associated technology.[28] Such technologies can lead to discrimination in various ways,[29] including being trained on biased data or biased samples, and therefore reproducing existing patterns of discrimination.[30]

For example, in 2018, Reuters reported that Amazon stopped using an AI system for screening job applicants because the system was biased against women: according to the report "the company realised its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way".[31] Based on the data processed, "Amazon's system taught itself that male candidates were preferable".[32]

The purchasing and selling of data by "data brokers" for commercial purposes, such as advertising, credit scoring and insurance risk analysis has been linked to a lack of transparency, the indefinite retention of data, and discriminatory outcomes by algorithms.[33] A study by ProPublica in 2017 revealed that Facebook advertisers could exclude certain groups from rental housing ads, including African Americans, people interested in wheelchair ramps, and Spanish speakers, despite the company having announced that it had built a system to spot and reject discriminatory ads.[34]

In the US, the criminal justice systems in some regions use a system known as COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) to help judges determine whether a person convicted of a criminal offence should be allowed to be supervised outside of prison rather than incarcerated. Research by investigative journalists in 2016 showed that COMPAS was racially biased: black individuals were almost twice as likely as whites to be labelled a higher risk but not actually reoffend, and white individuals were much more likely to be labelled as a low risk, but then commit further crimes.[35]

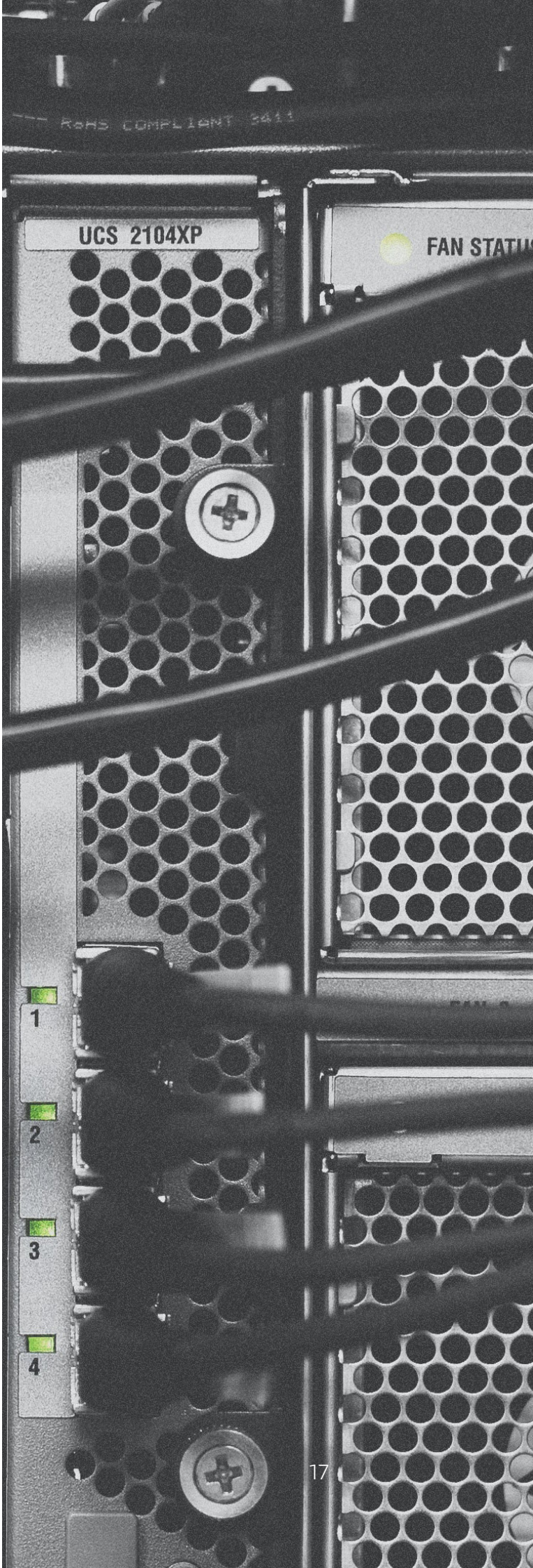
The opaque mass collection of vast quantities of information, including personal data, can also create risks of data breaches, misuse of that data and discrimination. The Cambridge Analytica scandal revealed that Facebook allowed the harvesting of data from 87 million users which was subsequently used to try to influence the outcome of the 2016 US presidential campaign.[36] The 2013 Yahoo data breach affected all three billion of Yahoo's user accounts, putting at risk the personal information of millions of its users with reports that stolen data was used by governments to target individuals.[37]

Tech companies, including internet service providers and internet exchange points, have come under particular pressure to share personal data with national security agencies engaged in digital surveillance with adverse impacts on privacy, equality/non-discrimination and other human

rights. For example, the US PRISM program of surveillance, exposed as a result of the 2013 Snowden leaks, has been criticised for amassing large amounts of data on Americans that were neither spy targets nor posed security threats. Moreover, the data collected in this way has been used to identify and investigate suspects in violation of the right to a fair trial.[38] A number of lawsuits against tech companies are currently ongoing in different jurisdictions for their role in facilitating human rights abuses perpetrated by states as a result of data collected through digital surveillance techniques.[39] Groups at risk of discrimination are particularly vulnerable to the sharing of mass data sets for state surveillance. For example, big data has fuelled the crackdown by the Chinese state against Uyghurs and other ethnic minorities in the region of Xinjiang.[40]

Frameworks and initiatives

Freedom House's 2018 "Freedom on the Net" report showed that, since June 2017, governments in 18 out of 65 states reviewed or passed new laws or directives to increase state online surveillance.[41] Some states have required tech companies to store their citizens' data on local servers with the objective to make the records more accessible to national security agencies or protecting them from theft or exploitation.[42] Against this backdrop, the International Principles on the Application of Human Rights to Communications Surveillance were developed by a multi-stakeholder group to clarify how international human rights



© Kvisthol

law applies to current communications surveillance technologies and techniques.[43] Tech companies have increasingly joined forces to push back against government requests for data collection regarding their users. Through the Reform Government Surveillance Coalition, companies such as Google, Apple, Facebook, Dropbox, Twitter and LinkedIn have requested the reform of laws and practices on government surveillance and access to information by the world's governments.[44]

Some states have raised concerns over the challenges that sophisticated encryption tools and products developed by tech companies to protect users' online security pose to law enforcement. In 2018, for example, the Five Eyes states, an intelligence alliance comprising the UK, US, Canada, Australia and New Zealand, issued a joint statement calling on tech companies to "voluntarily establish lawful access solutions" for encrypted content.[45]

The proliferation of digital risks to data security and protection has highlighted the inadequacies of many data protection frameworks. Globally, most information data protection and privacy laws have been informed by the data protection principles set in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 (and updated in 2013) and the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in 1981 (Convention No. 108). As a result, many states are revising or adopting new data protection and privacy laws.

While over 100 states have adopted data protection legislation of some kind, the EU's General Data Protection Regulation (GDPR) is the most far-reaching regulation adopted so far. Hailed for its potential to strengthen data protection and the right to privacy, the GDPR is part of a broader regulatory package being developed by the EU that includes the Cybersecurity Act and the revision of the ePrivacy Directive.[46] It also includes a police directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes.[47]

According to the European Data Protection Board, over 89,000 data breaches were logged by the national supervisory authorities in the first year after the GDPR came into force in May 2018.[48] A record fine of €50 million has been imposed on Google by the French Data Protection National Agency for violating the new law.[49]

The GDPR has informed similar legislation in other jurisdictions, such as the Californian Consumer Privacy Act and data protection laws in Argentina, Brazil and Indonesia. As noted at the start of this section, new technologies such as 5G, the Internet of Things, and AI will only accelerate the scope and scale of data collection and further obfuscate the distinction between personal and non-personal data. To stay ahead of the curve of digital

EU General Data Protection Regulation (Regulation (EU) 2016/679)

The General Data Protection Regulation (GDPR) entered into force in May 2018 and applies to all individuals, organisations and companies that collect, store and process personal data on individuals in the EU. Personal data is defined as any information that relates to an identified or identifiable living individual. Personal data is protected regardless of the technology used for processing or storing and applies to both automated and manual processing. The GDPR requires companies to obtain the explicit consent of the people ("data subjects") on which they hold data and write privacy policies "in an intelligible and easily accessible form, using clear and plain language". Importantly, to comply with the provisions of the GDPR, consent should not be hidden in terms and conditions and where processing has multiple purposes, consent must be obtained for all of them.

The GDPR also creates more transparency by requiring companies to inform users if data is transferred outside the EU, the data collected is used for a different purpose than originally intended and if the decisions taken using their data is automated, including by giving the possibility to contest it. It gives individuals stronger rights to access data held about them, to be notified promptly in the case of any breaches, and a "right to be forgotten" (a right to have personal data erased).

The GDPR also creates stronger enforcement mechanisms by giving national data protection authorities the power to fine a company up to 4% of its worldwide turnover for infringements, and incentivising their cooperation through the European Data Protection Board with the power to provide guidance and interpretation and adopt binding decisions in cross-border cases.

The GDPR also introduces some novel provisions, such as a requirement for data protection impact assessment in situations likely to result in a high risk to the rights and freedoms of individuals, and rights to data portability and not to be subject to a decision based solely on automated processing which produces legal or other serious effects concerning the person.

innovation, regulators and policymakers are increasingly exploring solutions that straddle previously distinct regulatory domains such as consumer protection, competition rules and data protection.

Although data protection laws and policies go some way towards mitigating the human rights harms of new technologies, including AI and big data, many of these technologies are increasingly being used in states that have not yet adopted comprehensive anti-discrimination laws, meaning that the legal framework to prevent discriminatory application is inadequate.[50]

© Marten Bjork

Responding to concerns around risks of discrimination specifically, the Toronto Declaration on Protecting the Right to Equality and Non-Discrimination in Machine Learning Systems was launched by a group of non-governmental organisations in 2018. The Toronto Declaration calls on governments and companies to ensure that machine learning applications respect the principles of equality and non-discrimination.[51]

2.2. THE RIGHT TO FREEDOM OF EXPRESSION (INCLUDING DISCRIMINATORY IMPACTS)

While social media platforms, messaging services and search engines provide new spaces for individuals to exercise their right to freedom of expression, these spaces - and therefore what people can say and do online - are governed almost entirely by a small number of tech companies. Their content moderation policies dictate what can and cannot be viewed, said and done on those platforms, and algorithms and AI are increasingly relied upon to inform such decisions, as well as to curate what information people see online. In his 2018 report to the UN General Assembly, the UN Special Rapporteur on the right to freedom of opinion and expression highlighted how the use of algorithms and AI to filter and personalise the content that individuals can access online undermines the

ability of rights-holders to form independent opinions by drawing on diverse ideas across ideological and political divisions.[52]

Freedom of expression concerns have been raised in respect to legislation and legislative proposals developed by governments and regulatory bodies to tackle certain forms of online content, expression and behaviour. This regulatory trend has come on the back of mounting evidence of online platforms being used to spread disinformation and political propaganda,[53] violence and abuse against women,[54] and hate and incitement to violence against various minority groups.[55] Violent incidents such as the 2019 New Zealand Christchurch Attack, the increase in white supremacist attacks globally and the campaign of ethnic cleansing against the Rohingya Muslim minority in Myanmar,[56] have exposed a disconcerting continuum between the online proliferation of hate content and the offline perpetration of violence.

Another critical risk to freedom of expression online stems from various restrictions to access to the internet - and the platforms that run on it - imposed by governments seeking to control information flows. In 2018 alone, 196 internet shutdowns blocked user access to information in 25 countries which increased to 213 shutdowns in 33 countries in 2019.[57] Groups at risk of discrimination are particularly vulnerable to such arbitrary restrictions to access, which often amounts to unlawful measures taken by governments to silence dissenting voices.[58] Large shutdowns are frequently executed in regions where a marginalised ethnolinguistic or religious group forms a considerable part of the population.[59] Recent research recognises digital discrimination in access to communication technology as a global trend that strongly affects disenfranchised ethnic groups.[60]

The UN Human Rights Council has condemned measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and called upon all states to refrain from and cease such measures.[61] Such internet shutdowns and other techniques to control access to the digital world rely upon the involvement of those companies - through both coercive and non-coercive means - that operate and maintain the internet infrastructure including telecommunications and internet service providers, internet exchange points and content delivery networks.[62]

Risks to freedom of expression can also stem from the decisions of internet standard-setting bodies. For example, in 2019, a coalition of digital rights organisations publicly called upon the Internet Corporation for Assigned Names and Numbers (ICANN) to prevent the sale of the top level domain name ".org" - primarily used by charities and non-profit organisations - to a private equity fund. The coalition argued that the management of the domain name by a for-profit organisation could have financial and political implications

that would exacerbate the shrinking space for civil society around the world.[63]

Last but not least, civil society and digital rights advocates have highlighted that the realisation of freedom of expression online requires that states and private actors take measures to provide access to an affordable and meaningful internet connection. In a context where approximately 40% of the global population are not active internet users,[64] closing the digital divide among and within countries has become a critical human rights issue. Moreover, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has emphasised that the quality and type of internet access can also have adverse impacts on the right to freedom of expression. For example, threats to the principle of "network neutrality" and zero-rating schemes can unduly restrict and limit the type of content and information certain users can access online.[65]

Frameworks and initiatives

Against this backdrop, states are increasingly adopting legislation requiring or encouraging tech companies to identify and remove various forms of "harmful" content generated and uploaded by users, including by establishing intermediary liability regimes. For example, in 2018 Germany adopted a law, the Network Enforcement Act (or NetzDG), that requires tech companies to remove "manifestly unlawful" hate speech and postings within 24 hours of receiving a notification, with companies facing fines of up to €50 million for a failure to act. In April 2019, Australia amended its Criminal Code to criminalise the publication of "abhorrent violent material" and requiring tech companies to remove violent online material "expeditiously". The sanctions for non-compliance are high: companies could be fined up to 10% of their annual profit and company executives could risk jail time.

Similar regulatory developments are also being considered in other jurisdictions. In 2019, the UK revealed a plan for a new regulatory regime that would establish a "duty of care" on tech companies for the safety of their users, as well as an independent regulator to enforce compliance.[66] At the EU level, the European Parliament has endorsed draft rules that would require online platforms to remove terrorist content within an hour of notification by national authorities. A survey by Freedom House found that at least 17 countries approved or proposed laws in 2017 that would restrict online media in the name of fighting "fake news" and online manipulation.[67]

While the governments proposing laws such as these usually state that any restrictions they would have on freedom of expression would be justified, human rights experts have challenged the legal certainty, proportionality and necessity of some of these laws and proposals due to their vague definitions, high penalties and short timeframes. Many concerns have been raised that

such laws strongly incentivise the over-removal of content that represents lawful and legitimate forms of expression.

Beyond compliance with national laws, tech companies enforce their own rules (whether described as terms and conditions, community standards or otherwise) on the acceptable modalities and types of expression and behaviour on their platforms. The arbitrary application of these rules and their limited alignment with human rights standards have been argued to disproportionately restrict freedom of expression, often in a discriminatory manner.[68]

Civil society organisations have pointed to various instances of suppression of free expression on social media platforms, including LGBTI activism, reporting on ethnic cleansing and denunciation of racism and power structures.[69] An analysis of Facebook's and Twitter's terms of service concluded that their definitions and practices need to be further aligned with international standards on freedom of expression.[70] The identification of inappropriate content through the use of algorithms has been challenged for failing to correctly interpret culture and context-specific language cues. The UN Special Rapporteur on the right to freedom of opinion and expression has noted that there is a high risk that AI content moderation systems will remove content in accordance with biased or discriminatory concepts and as a result, that vulnerable groups are the most likely to be disadvantaged.[71]

© John Schnobrich

A number of experts and advocates have put forward human rights principles for content moderation to address the inappropriate and excessive account closures and content removal. For example, the Santa Clara Principles on Transparency and Accountability in Content Moderation consist of company guidelines aimed at ensuring that content moderation follows due process, such as providing notice and an opportunity for timely appeal to each user whose content is taken down or account suspended.[72] A coalition of civil society experts have developed the Manila Principles on Intermediary Liability as part of broader efforts to embed human rights principles in online content regulatory frameworks.[73]

In his 2018 report to the Human Rights Council, the UN Special Rapporteur on the right to freedom of opinion and expression advanced a set of human rights principles to guide the moderation of online content,[74] highlighting inter alia, that when companies develop or modify policies or products, they should actively seek and take into account the concerns of communities historically at risk of censorship and discrimination.[75]

Moreover, new content moderation governance models are emerging in response to calls for more accountability and transparency on social platforms. In 2019, the civil society organisation Article 19 launched a global public consultation on the setting up of Social Media Councils as multi-stakeholder fora to address content moderation issues on social media platforms on the basis of international standards on human rights.[76] In 2020, Facebook launched an independent Oversight Board tasked with reviewing appeals against the company's content moderation decisions.[77]

In addition to a rule-based approach to content moderation, public bodies and tech companies have partnered to develop social programs that would address online manipulation and misinformation. For example, policymakers in Italy have cooperated with journalists and tech firms to develop and pilot a nationwide curriculum on spotting online manipulation including "fake news" and conspiracy theories.[78] Apple launched a media literacy initiative to encourage critical thinking and empower students to be better informed. In the US, it partnered with several non-profit organisations such as News Literacy Project and Common Sense that provide nonpartisan, independent media literacy programmes.[79] WhatsApp has worked with organisations in India to design a digital literacy training program for its users.[80] Tech companies have partnered with civil society to combat disinformation on their platforms. The Argentinean organisation Chequeado runs a software application in partnership with Facebook to automatically match media claims on the network with fact-checking research.[81]

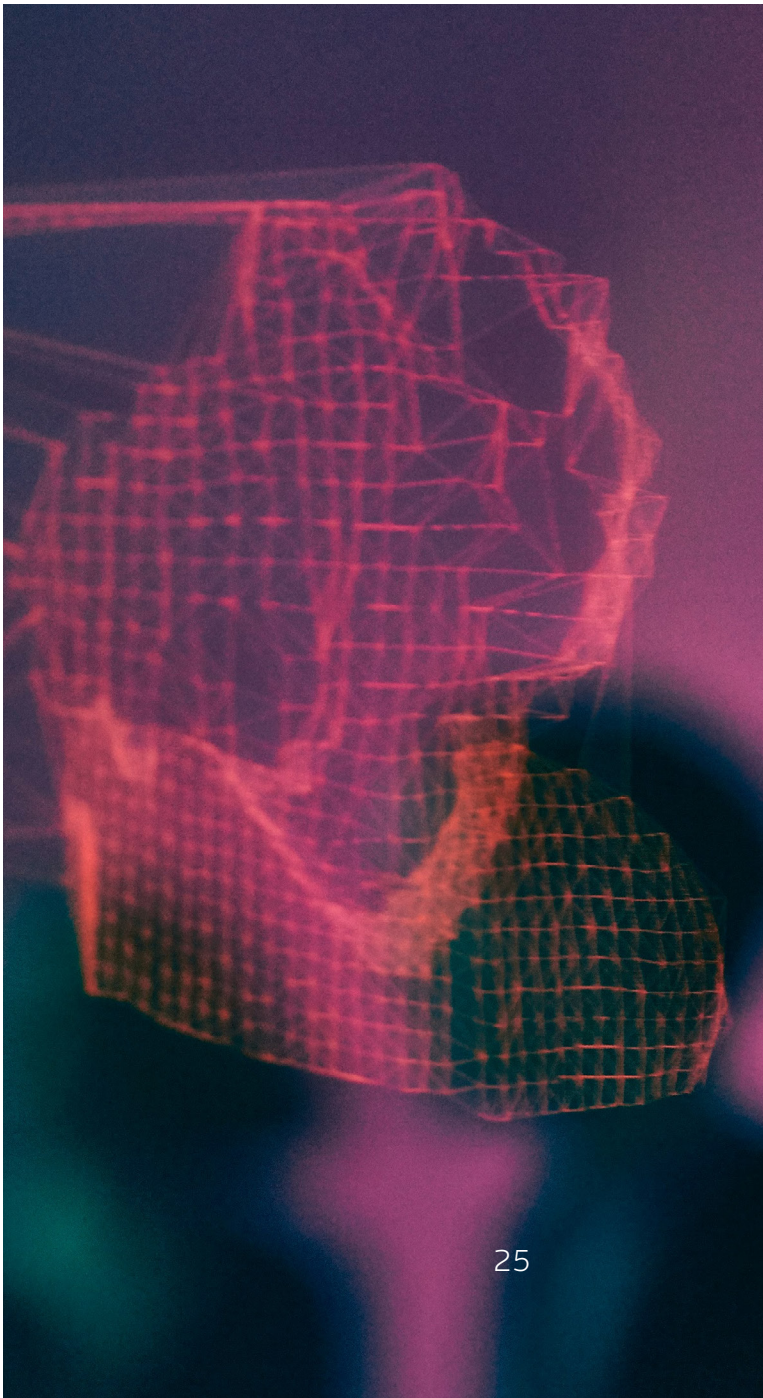
3. THE TECH SECTOR IN NAPS

This section builds on the guidance on the NAP lifecycle in the DIHR-ICAR Toolkit, and sets out how states can ensure that the specificities relating to the tech sector are considered in the NAP process and content.

3.1. STAKEHOLDER MAPPING AND ENGAGEMENT

As the DIHR-ICAR Toolkit notes, it is essential that all relevant stakeholders are meaningfully mapped and engaged during the development of a NAP. Their consultation should take place in an open, inclusive and transparent manner. State institutions with a mandate pertinent to the operations of the tech sector should be included in the design and implementation of the process, including through the allocation of resources for capacity-building, involvement in the collection of data and the public and expert consultations. Crucially, the stakeholder mapping should include individuals and groups whose rights to privacy, freedom of expression and non-discrimination are most at risk, such as human rights defenders, women and girls, ethnic or religious minorities, or persons discriminated against on the basis of their sexual orientation and gender identity. Strategies for engagement of these individuals and groups should be specifically developed to ensure that their rights are protected and their voices heard in the process.

There are a number of broad stakeholder categories which should be considered in a NAP process regardless of the business sector or policy area. To aid state actors using the DIHR-ICAR Toolkit, the categories set out in the Toolkit are listed below alongside, where relevant, specific stakeholders that should be considered when it comes to the tech sector.



© Ashwin Vaswani

Stakeholder Category	Specific Stakeholders for the Tech Sector
Executive government, including all relevant government departments, agencies, offices, and state-owned enterprises, as well as police and other law enforcement agencies	• Ministries for Communications and/or ICTs • Ministries of Justice • Offices focused on technology within other ministries e.g. a "tech ambassador" in the Ministry of Foreign Affairs[82] or a "technology and innovation bureau" in a Ministry of Economy • Police and law enforcement agencies with responsibility for cybercrime • Public procurement authorities and public buyers • Regulatory bodies whose mandates include the internet and digital technology • Regulatory bodies whose mandate cover traditional and new media organisations
Judiciary and administrative tribunals, alternative dispute resolution mechanisms, and informal justice actors	• Ombudsman for Digital Transformation (or similar) • Ombudsman for Equality (or similar) • Bar associations
Parliament, including relevant committees	• Parliamentary committees whose mandate covers communications and/or ICTs • Parliamentary committees whose mandate covers communications justice, crime and/or cybercrime

	• Parliamentary committees whose mandate covers equality and non-discrimination
Businesses, including significant industry sectors, business associations, small and medium enterprises (SMEs), the self-employed, sole traders, cooperatives, non-profits, and informal sector actors	• Tech sector industry bodies [83] • Tech companies operating in or based in the country
Labour unions and other workers' representative associations	• National and industry level labour unions that work on the issue of employee data collecting, suppression of workers' voices by monitoring social media, non-discrimination etc.
Representatives of affected groups or communities of rights-holders and human rights defenders, inside and outside the state's territorial jurisdiction, who may potentially be affected by the conduct of companies based in or controlled by the state	• Representatives of rights-holders that might be particularly marginalised, e.g. women and girls, LGBTI persons, ethnic and religious minorities etc. • Human rights organisations who focus on privacy, freedom of expression and/or the internet and digital technology (including digital rights organisations) • Equality defenders (civil society organisations, lawyers and others working on issues of equality and non-discrimination) • Consumer organisations that represent the rights of consumers/users whose rights may be breached • Media freedom organisations

NHRIs, ombudsman institutions, statutory equality bodies, and other national accountability mechanisms with a human rights mandate	• National human rights institutions • Data protection authorities • National equality bodies
CSOs with mandates addressing relevant issues	• Human rights organisations who focus on privacy, freedom of expression and/or the internet and digital technology (including digital rights organisations) • Equality defenders (civil society organisations, lawyers and others working on issues of equality and non-discrimination) • Where these organisations do not exist within the state, international organisations (such as Global Partners Digital, the Equal Rights Trust, Access Now, the Association for Progressive Communications, Article 19 and Privacy International) could be engaged
Media, including general news and specialist sources	• Online media companies • Online forums
Academia, including research institutes, individual experts, and relevant educational institutions, such as business schools	• Academic and research institutions who specialise in the internet and digital technology
International and regional actors, including relevant UN agencies and country teams, the World Bank, regional development banks, and the OECD	• International Telecommunication Union • UN Commission on Science and Technology for Development

• UNICEF, Children's Rights and Business Team

• Office of the High Commissioner for Human Rights (OHCHR)

• Council of Europe, Anti-discrimination Department

Regulatory Bodies

When it comes to the regulation of the tech sector (and technology more broadly), different states are taking different approaches. Some are giving existing regulatory bodies, such as data protection authorities, new functions and powers. Others are beginning to establish new regulatory bodies whose mandates touch upon different aspects of the internet or technology.

Australia: In 2015, Australia established the Children's eSafety Commissioner with a mandate to protect children's safety online. Since then, the body's (now the eSafety Commissioner) mandate has expanded to take action to prevent image-based abuse and other forms of prohibited content.[84]

Denmark: The independent Danish Data Ethics Council consists of members representing a broad mix of competencies from both the public and private sectors. The Council provides consultation and advice to the Danish government, parliament and public authorities on issues related to data ethics in the use of data and new technology, and to support a culture of responsible data use by companies and the public.[85]

United Kingdom: The Centre for Data Ethics and Innovation was established in 2018 with a mandate to "analyse and anticipate the opportunities and risks posed by data-driven technology" (with a particular focus on artificial intelligence) and to "put forward practical and evidence-based advice to address them".[86]

National Human Rights Institutions

National Human Rights Institutions (NHRIs) are increasingly taking an interest in technology and its impacts upon human rights, sometimes as part of their general work on business and human rights. As such, they may provide specific insight into how human rights such as privacy and freedom of expression are impacted by the tech sector during a NAP's development.

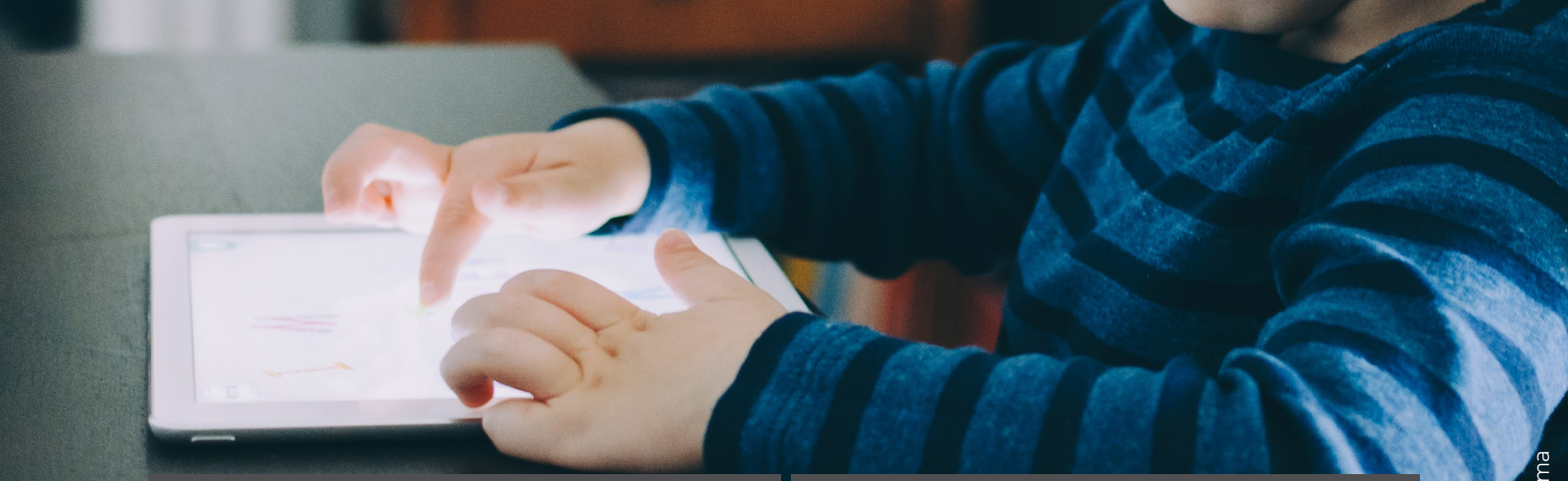
Australia: In 2018 the Australian Human Rights Commission (AHRC) launched a project on the relationship between human rights and technology. With advice provided by an expert Reference Group formed of academia, business, and state representatives, the project explores human rights issues linked to artificial intelligence, bias, big data, inclusive technology and the intersection between technology, freedom of expression and democracy. The AHRC plans to make recommendations on how to ensure human rights are prioritised in the design and governance of emerging technologies in 2020.[87]

Denmark: The Danish Institute for Human Rights has undertaken specific research on technology and its impacts on human rights since 2003.[88] It has contributed to standard-setting in this area at the UN, the EU and Council of Europe.[89] The Institute works with technology companies and it is also currently in the process of developing guidance on how to undertake human rights impact assessments of digital business activities.

Kenya: In February 2019 the Kenya National Commission on Human Rights (KNCHR), together with the Kenya Human Rights Commission and the Nubian Rights Forum, filed a petition before Nairobi's High Court challenging the roll out of a mandatory digital national ID registration system - the National Integrated Identity Management System (NIIMS). The KNCHR supported the other petitioners in arguing, inter alia, that the NIIMS violated the right to privacy because no adequate protections had been assured and the rights to equality and non-discrimination as regards the Nubian community and other marginalised groups who would face further exclusion. On 30 January 2020, the High Court ruled that the Kenyan government should halt the roll out until there is "an appropriate and comprehensive regulatory framework on the implementation of NIIMS". The judgment acknowledged the importance of having a data protection framework and a clear regulatory framework that addresses the possibility of exclusion.

3.2. GROUPS AT RISK

As with other business sectors and policy areas, it is important to consider and respond to the needs and experiences of diverse groups, particularly groups at risk, when mapping (and engaging with) stakeholders.[90] When it comes to the tech sector, there are rights-holders and groups who are at particular risk of human rights violations, and the state should therefore identify those individuals, bodies and organisations that legitimately represent the interests of these groups, ensuring that their participation will not result in reprisals or any form of harassment. The table below includes select examples of adverse and discriminatory impacts on the rights to privacy and freedom of expression on persons with certain characteristics. This is a non-exhaustive list and states should ensure that all groups that may be disproportionately affected by policies relating to the tech sector are encouraged and enabled to participate in consultations.



© Kelly Sikkema

Characteristic/Group	Select examples of adverse and discriminatory impacts on rights to privacy and freedom of expression
AGE/CHILDREN	
Children are at a disproportionate risk of excessive data collection, online manipulation and abuse because of their evolving cognitive, social and emotional capacities. Companies collect data on children from birth onwards without their knowledge/awareness through the information shared by parents and the use of parental control devices. Targeted advertising and search engine models can be detrimental to children's development by influencing their preferences as consumers and ability to develop autonomous opinions. The increasing presence of children on social media and other digital platforms has increased the risks for sexual abuse, harassment and cyberbullying.[91]	• The US Federal Trade Commission has levied several fines on tech companies for collecting personal data on children without their parents' consent.[92] • According to Human Rights Watch, Russia's 2013 "gay propaganda law" bans the "promotion of non-traditional sexual relations to minors", which has had a negative impact on LGBTI youth trying to access websites with online education and support services.[93] • According to a recent study on the distribution of captures of live-streamed child sexual abuse, 98% of imagery depicted children assessed as 13 years or younger and 96% of the imagery featured girls.[94] • Schools in the US have hired social media monitoring companies to prevent school violence and shooting. However, the monitoring programmes have been challenged for disproportionately interfering with the teenagers' exercise of freedom of expression online.[95]

GENDER/WOMEN

The discrimination faced by women offline has permeated digital spaces. In 2018, the UN Human Rights Council adopted a resolution recognising the issue of discrimination and violence against women in digital contexts.[96] New terms have been introduced to make sense of emerging types of online violence such as "doxing", "sextortion", "trolling", online mobbing, online stalking and "revenge porn" (the non-consensual distribution of intimate contents). The publication without consent of intimate photographs represents gender-based violence that violates women's and girls' rights to privacy. Online threats and abuse prevent women from exercising their right to freedom of expression, including through withdrawal from digital platforms, public debates and public functions. Women human rights defenders, women in politics, and journalists, are at a heightened risk of online violence.[97]

Moreover, offline discrimination, inequalities and stereotypes have resulted in a gender digital divide whereby women and girls are much less likely than men to use the Internet and benefit from its online financial, educational, and social connectivity opportunities.[98]

• A 2018 study by Amnesty International found that women are more likely to be harassed and abused on Twitter, including through privacy violations such as doxing or sharing sexual or intimate images without consent. Online harassment often resulted in women self-censoring their posts and leaving Twitter all together. According to the report, Twitter has inadequately investigated and responded to reports of violence and abuse.[99]

• In 2019, a female elected member of the US House of Representatives resigned after nude photos released without her consent were posted online by media outlets.[100]

• A 2018 survey by the Inter-Parliamentary Union found that a significant number of European female members of the Parliament had experience of abusive, sexual and violent content on social networks.[101]

• In 2016, Al Jazeera reported on the existence of a market trading in videos of rape in the state of Uttar Pradesh, India.[102]

• According to a 2019 survey of women journalists in Pakistan, women reported that online violence has had a significant impact on mental health and that they have self-censored in order to counter online violence.[103]

• Activists have expressed concern that personal data, gathered through smart home devices and digital technologies, can be used to control and intimidate victims of domestic violence. [104]

	• According to the International Telecommunications Union, in 2017 the proportion of women using the Internet was 12% lower than the proportion of men using the Internet worldwide. The gap widened in Africa where the proportion of women using the Internet was 25% lower than the proportion of men using the Internet.[105]

HUMAN RIGHTS DEFENDERS

Human rights defenders across the world have relied on technology to organise, mobilise and advocate for human rights. Their digital presence increased their susceptibility to online surveillance and control via spyware products with adverse implications for their safety and privacy. Increasingly, governments have ordered internet shutdowns to silence human rights defenders.	• According to Amnesty International, the Israeli company NSO Group developed spyware technology used to silence human rights defenders in countries such as Mexico, Morocco, Saudi Arabia.[106] WhatsApp sued NSO Group in October 2019 accusing it that it helped the government break into the phones of approx. 1,400 users including journalists and political dissidents. • In 2019, a group of civil society organisations expressed concern over the global trend of persecuting digital rights defenders.[107] • According to Human Rights Watch, the internet shutdown imposed by the Sudan Transitional Military Council in 2019 prevented activists from reporting critical information in the context of a volatile political crisis.[108]

RACE; ETNICITY AND RELIGION

Discrimination on the basis of race, ethnicity and religion has extended into the online domain through digital surveillance, illegitimate restrictions on freedom of expression, as well as inadequate moderation of hate speech content.

• A 2019 data leak revealed that China tracked through a facial-recognition company and police contractor called SenseNets the locations of almost 2.6 million people in the region of Xinjiang where Uyghurs and other Muslim minorities live.[109]

• Vox reported on two scientific studies demonstrating that artificial intelligence models used by social media companies are 1.5 times more likely to flag tweets written by African Americans as "offensive" compared to other tweets.[110]

• A 2019 study by Cardiff University found a correlation between Twitter hate speech targeting race and religion and racially and religiously aggravated offences that happened offline over the same period.[111]

• In 2020, as part of the Black Lives Matter protests worldwide, greater attention was paid to the content moderation policies of major social media when it came to hate speech and the incitement of violence, and the need for greater action addressing how individuals use social media platforms to abuse human rights.[112]

	• In 2019, the Internet Corporation for Assigned Names and Numbers (ICANN) granted the company Amazon the exclusive right to administer the general top-level domain ".amazon" Some human rights experts argued that this decision will deprive Indigenous People in the Amazon area from economic development opportunities and that under international human rights law the company Amazon had a responsibility to ensure that Indigenous People were consulted before pursuing the application.[113] • In February 2020, the Myanmar government reinstated a shutdown of mobile internet traffic in five townships in Rakhine State and Chin State. Adding four townships in Rakhine state that had been cut off since June 2019, causing an information blackout that affects approximately one million people, the majority being the ethnic Muslim minority Rohingya. Blocking their ability to communicate makes it challenging to obtain help in times of conflict and for humanitarian agencies to provide assistance.[114]

NATIONAL OR SOCIAL ORIGIN / MIGRANT WORKERS	
Migrant workers have been increasingly the subject to right to privacy impacts by tech companies, due to their vulnerable position in society, where they lack protection.	• An investigation by the BBC uncovered that thousands of domestic workers in Kuwait are being illegally bought and sold on Instagram and their personal data such as pictures and race are made available to potential "buyers".[115]

© Markus Spiske

SEXUAL ORIENTATION AND GENDER IDENTITY

LGBTI persons face acute risks of hate speech and violence online, as well as disproportionate impacts on their right to privacy and restrictions on their right to freedom of expression.

• The UN Special Rapporteur on the rights to freedom of opinion and expression has highlighted that "platforms have suppressed lesbian, gay, bisexual, transgender and queer activism"[116] and "blocked the accounts of lesbian, gay, bisexual, transgender and queer users and activists, drag performers and users with non-English or unconventional names".[117]

• LGBTI communities have alleged that YouTube's algorithm blocks or suppresses videos containing LGBTI content by automatically enforcing age restrictions and by "demonetising" the videos – meaning that they deny the producers and revenue.[118]

3.3. CONDUCTING A NATIONAL BASELINE ASSESSMENT

An important stage in the NAP lifecycle is conducting a National Baseline Assessment (NBA).[119] As the DIHR-ICAR Toolkit states, "an NBA on business and human rights has the primary objective of assessing the current level of implementation of the UNGPs in a given state. It brings together an analysis of the legal and policy gaps in UNGP implementation with an overview of the adverse human rights impacts of business to identify the most salient human rights issues in a given context. In this way, it serves to inform the formulation and prioritisation of actions in a NAP."

The 'Tech Sector National Baseline Assessment (NBA) Template' should be used to determine how the rights to privacy, freedom of expression and equality/non-discrimination of those affected by the tech sector are protected as part of the state's legal and policy framework on business and human rights. It is designed to be used in concert with the full NBA Template contained within the DIHR-ICAR Toolkit.

In undertaking an NBA and utilising it as a tool to develop a NAP, states should analyse and evaluate specific measures that guarantee both state protection and corporate respect for the rights to privacy, freedom of expression and equality/non-discrimination, as well as effective remedy when these rights have been violated.

The template below contains the minimum scoping questions in relation to the protection and respect of the rights to privacy, freedom of expression and equality/non-discrimination that states should consider when designing an NBA. The questions reflect the provisions of the UNGPs on the state duty to protect against human rights abuses (Pillar I), the corporate responsibility to respect human rights (Pillar II) and the provision of remedy by both state and non-state actors (Pillar III). Integrating these questions into a general NBA will allow policymakers to obtain granular information on the different forms of involvement of the tech sector with adverse and discriminatory impacts on privacy and freedom of expression, assess their severity and decide on whether and how these should be prioritised in the NAP.

States should consider consulting local experts at the outset of the NBA, as well as throughout its drafting process. Understanding the operations of tech companies and how they can impact human rights require specialised knowledge. It is advisable that the organisation conducting the NBA is adequately capacitated to analyse tech-related data, identify risks and understand the complex ecosystem in which tech companies operate.

As part of the NBA, the state could consider commissioning a sector-wide human rights impact assessment.[120] A tech-sector focused human rights impact assessment will help state actors and other stakeholders see the "bigger picture" of potential negative impacts of the tech sector's activities.

A note on extraterritoriality

While the UNGPs say that states are not generally required to regulate the extraterritorial activities of businesses domiciled in their territory and/or jurisdiction, they also recognise that states are not generally prohibited from doing so, providing that there is a recognised jurisdictional basis. The UNGPs recognise that there may be strong policy reasons for states to be clear about their expectations of businesses abroad. States do not have unlimited power to enact laws which apply to extraterritorial activities and must operate within the constraints of international law and comity.

While this will be a consideration in many sectors, it is particularly relevant for the tech sector given that many tech companies operate globally, and have products and services that will be available around the world, often in states where the company has no physical presence. Given the intangible nature of some digital activities, it can be challenging to pinpoint where activities occur and what national legal regime is applicable.

The regulatory framework which applies to companies in one state, particularly their home state, will often have impacts in others in which the company operates. For example, the EU's GDPR (see Box 4) sets higher standards than most other national data protection frameworks. Rather than having many different data protection policies for different states, some tech companies simply use the GDPR requirements as their global data protection policy, a positive development from a privacy perspective.

However, there are an increasing number of instances where courts are being asked to decide whether online content which violates national legislation can be removed globally by tech companies, rather than only in that state, raising various concerns, including over privacy and freedom of expression.[121]

States should therefore carefully consider the extraterritorial application of national legislation, including through court decisions, to ensure that NAPs, and the legal and policy frameworks that they adopt, ensure that tech companies respect the rights to privacy, freedom of expression and equality/non-discrimination in the states that they operate.

TECH SECTOR AND NAPS NATIONAL BASELINE ASSESSMENT (NBA) TEMPLATE

1. LEGAL AND POLICY FRAMEWORK

States should assess whether its legal and policy frameworks adequately protect against tech sector-related human rights abuses. States should also assess the extent to which these laws and policies contribute to preventing such abuses.

While the questions below focus on the rights to privacy, freedom of expression and equality/non-discrimination, they could be expanded to include additional human rights.

1.1. International, Regional and Other Standards

International Standards	Has the state signed, ratified, and implemented relevant international human rights instruments protecting the rights to privacy, freedom of expression and equality/non-discrimination, in particular the International Covenant on Civil and Political Rights? Since 2011, has the state received recommendations from the UN Human Rights Committee (or the treaty body monitoring the respective instruments) concerning the protection of the rights to privacy, freedom of expression and equality/non-discrimination in respect to the activities of the tech sector? If yes, what is the progress of the implementation of recommendations from this body? Since 2011, has the state received recommendations from the UN Special Procedures or the Universal Periodic Review concerning the protection of the rights to privacy, freedom of expression or equality/non-discrimination in respect to the activities of the tech sector? If yes, what is the progress of the implementation of recommendations from these bodies?

Regional Standards	Has the state signed, ratified, and implemented relevant regional human rights instruments, such as the: • American Convention on Human Rights • African Charter on Human and Peoples' Rights • European Convention on Human Rights? Since 2011, has the state received recommendations from any regional bodies concerning the protection of the rights to privacy, freedom of expression or equality/non-discrimination in respect to the activities of the tech sector? If yes, what is the progress of the implementation of recommendations from this body? Since 2011, has a regional human rights court found that the state violated its duty to protect against privacy, freedom of expression or equality/non-discrimination abuses by a tech company? If yes, what is the progress of the implementation of recommendations from this court?
Other Standards	Has the state signed, engaged with or otherwise endorsed the following standards and initiatives relevant to the tech sector and privacy, freedom of expression and equality/non-discrimination: • Asia-Pacific Economic Cooperation Privacy Framework • Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data • Council of Europe Recommendation No. R(99) 5 for the protection of privacy on the internet • Council of Europe Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems • OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data • Organization for Security and Cooperation

	in Europe's Amsterdam Recommendations on Freedom of the Media and the Internet • African Union's Declaration of Principles on Freedom of Expression in Africa • International Principles on the Application of Human Rights to Communications Surveillance • Manila Principles on Intermediary Liability • The Toronto Declaration on Protecting the right to equality and non-discrimination in machine learning systems • Freedom Online Coalition • Rabat Plan of Action?
1.2. National Laws and Policies	
Right to privacy	Does the constitution or legislation guarantee the right to privacy? Are there any exceptions in legislation that restrict the right to privacy? If yes: • Are these consistent with the permissible limitations set out under international and regional human rights law i.e. a clear and non-discriminatory legal basis, and necessary and proportionate to achieving a legitimate aim?
Data protection	Is data protection regulated, including the collection, storage, use and sharing of personal data? If yes: • Is it consistent with international best practice, such as the EU's General Data Protection Regulation? In particular: • Does it cover all forms of personal data? • Does it cover all users/individuals or only consumers? • Does it apply to all data processors in both the private and public sector?

	• Where consent is the legal basis for data processing, does it require the request for consent to be informed, clear, intelligible, accessible and in plain language? • Does it allow individuals to ask data processors for copies of their data, and to have it corrected or removed? • Does it provide for a right to data portability? • Does it include a right for individuals not to be subject to decisions with significant effects based on automated processing? Is there any legislation that enables governments to access data stored by tech companies (e.g. data retention, metadata laws)? Are there national supervisory mechanisms or bodies that can process complaints about data breaches and enforce the data protection legislation, such as a data protection authority? If yes: • Are these bodies adequately resourced? • How many data breaches by companies have they recorded over the last five years?
Encryption	Is there any legislation or policy which requires or encourages the use of strong encryption by tech companies for personal data or communications? Is there any legislation or policy which restricts or undermines the ability of tech companies to encrypt personal data or communications?
Surveillance	Is there any legislation or policy regulating the online surveillance, interception or interference of private communications? If yes: • Is it consistent with international best practice, such as the International Principles on the Application of Human

	Rights to Communications Surveillance? In particular: • Is the law sufficiently clear and precise such that individuals have advance notice of and can foresee its application? • Is surveillance only permitted when necessary to achieve a legitimate aim and undertaken in a non-discriminatory manner? • Does it only authorise surveillance when permitted by a competent judicial authority that is impartial and independent? • Does it enable tech companies to resist or challenge requests made to them by state agencies? • Does it limit transparency reporting by companies on the government requests for data? • What assessment has been made of the implementation of the legislation, and the involvement of tech companies in its implementation?
Freedom of expression	Does the constitution or legislation guarantee the right to freedom of expression? Is there any legislation on freedom of information? Are there any exceptions in legislation that restrict the right to freedom of expression? If so, are these consistent with the permissible limitations set out under international and regional human rights law i.e. a clear and non-discriminatory legal basis, and necessary and proportionate to achieving a legitimate aim? Is there any legislation that allows governments to block or restrict access to the internet?

Content regulation	Is there any legislation or policy regulating online content or tech companies' content moderation policies? If yes: • Is it consistent with international best practice, such as the Manila Principles on Intermediary Liability? In particular: • Are the rules governing intermediary liability precise, clear, and accessible? • Are intermediaries immune from liability for third-party content in circumstances where they have not been involved in modifying that content? • Does it ensure that intermediaries cannot be held liable for failing to restrict lawful content? • Does it prohibit strict liability on intermediaries for hosting unlawful third party content? • Does it prohibit intermediaries from being required to monitor content proactively? • Does it ensure that intermediaries are only required to restrict content where an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful? • Does it ensure that intermediary and the user content provider are able to exercise an effective right to be heard (except in exceptional circumstances)? • Does it impose short timeframes for the removal of unlawful content once brought to the attention of the intermediary? • Does it impose high financial penalties or other disproportionate sanctions for non-compliance? • Is there transparency over orders or requests tech companies receive to remove content?

Equality/non-discrimination	Does the constitution or legislation guarantee the right to non-discrimination? Has the state adopted a comprehensive anti-discrimination legal framework? • Does the legal framework prohibit discrimination on the basis of a non-exhaustive and explicit set of grounds? • Is multiple discrimination, including intersectional discrimination, prohibited? • Does the legal framework adequately define and prohibit all internationally recognised forms of discrimination, namely direct discrimination, indirect discrimination, harassment and failure to make reasonable accommodation? • Is protection from discrimination provided in all areas of life regulated by law? • Does the legal framework impose non-discrimination obligations on private actors? Are there any justifications to indirect discrimination included in the legal framework? If so, do they comply with international standards, namely pursue a legitimate aim and are appropriate and necessary? Are there any justifications to direct discrimination? These can only be justified in very exceptional circumstances against strictly defined criteria as direct discrimination rarely pursues a legitimate aim. Does the state's anti-discrimination legal framework require positive action where substantive inequalities are identified, including in accessing and using the internet and new technologies?

	• Has the state implemented positive action policies for accessing and using the internet and new technologies? Does the state incorporate equality impact assessments as an integral element of its policies? • Are equality impact assessments aimed at identifying and eliminating the actual or potential discriminatory effects of State policies?
Due diligence	Are companies, including tech companies, required or expected to undertake human rights due diligence or other forms of due diligence processes such as data protection and equality impact assessments, including to assess and report on their adverse human rights impacts? If yes: • Does the state provide any guidance or required methodology for due diligence processes?

2. THE RESPONSIBILITY OF THE TECH SECTOR TO RESPECT HUMAN RIGHTS

According to Pillar II of the UNGPs, tech companies have a responsibility to respect human rights and conduct adequate human rights due diligence. States should assess to what extent tech companies are fulfilling this responsibility and implementing human rights in their policies and operations.

The questions below can be used to gather information from tech companies on policies and management procedures to respect human rights in accordance with the expectations set by Pillar II of the UNGPs. They could be further tailored to the type of enterprise surveyed (multinational company, SME, state owned company, publicly listed company) and expanded to include human rights issues beyond privacy, freedom of expression, and equality/non-discrimination.

2.1. Governance	
Public commitment	Do tech companies in the state have a public commitment to respect human rights? If yes • Is the commitment included in (i) a stand-alone human rights policy, (ii) in another policy such as sustainability or corporate social responsibility? Have tech companies in the state signed up to any multi-stakeholder initiatives with a human rights component such as the Global Network Initiative or the UN Global Compact?
Governance and management oversight	Do tech companies' senior leadership exercise oversight over how their policies and practices affect human rights? Is the public commitment to respect human rights integrated in all business functions and operations?
Internal implementation	Do tech companies have mechanisms in place to implement their commitments to human rights?

2.2. Specific Human Rights	
Right to privacy	Do tech companies' policies and commitments demonstrate concrete ways in which they respect users' right to privacy?
Data protection	Do tech companies provide data protection policies that are clear and accessible to users? Do tech companies provide notice to users when they change their privacy policies?

	Do data protection policies: • clearly disclose what personal data is collected and processed, and how? • seek the users informed consent for the data collection, processing and sharing? • clearly disclose what personal data is shared and with whom? • clearly disclose the purposes for which personal data is collected, processed and shared? • clearly disclose how long personal data is retained? • clearly disclose to users how they can exercise control over the collection, processing and sharing of their personal data? • allow users to obtain copies of personal data held? • allow users to have personal data corrected or deleted?
Data security	Do tech companies: • clearly disclose information about their institutional processes to ensure the security of its products and services? • address security vulnerabilities when they are discovered? • publicly disclose information about their processes for responding to data breaches? • encrypt user communication and private content so users can control who has access to it?
Freedom of expression	Do tech companies' policies and commitments demonstrate concrete ways in which they respect users' right to freedom of expression?

Content moderation	Do tech companies: • publish content moderation policies that are clear and accessible? • provide notice to users when they change their content moderation policies? • disclose and regularly publish data about the volume and nature of actions taken to restrict content or accounts that violate the content moderation policies? • notify users when it restricts content or accounts? Do tech companies: • disclose their process for responding to government requests (including judicial orders) and private requests to remove content or accounts? • regularly publish data about government requests (including judicial orders) and private requests to remove content or accounts?
Non-discrimination	Do tech companies adopt non-discrimination policies covering all areas of activity, including theprovision of online and other digital services? Do tech companies provide suitable training and sensitisation on the right to non-discrimination to all their staff and other agents? Do tech companies integrate equality impact assess-ments in the design and roll out of their products and services? Do tech companies ensure that equality impact as-sessments are an essential element of the evaluation of their products? Do tech companies adopt policies to ensure reaso-nable accommodation is provided when required? Do tech companies ensure and promote equal accessibility to their services?

3. REDRESS AND REMEDY

States should assess what judicial and non-judicial remedies are available to individuals affected by tech companies, as well as their effectiveness.

3.1. State-based mechanisms

Judicial mechanisms	Are there affordable, prompt, and effective judicial remedies before independent and impartial tribunals for tech sector-related human rights abuses?
Accessibility of remedies	Is access to justice for victims of tech sector-related human rights abuses accessible, taking into account diverse situations and needs, including, for example, geographic, linguistic, and cultural barriers? Do legal rules related to evidence and proof ensure that victims of tech sector-related human rights abuses are not unduly inhibited in obtaining redress? • Are rules on proof in civil proceedings adapted to ensure that when persons allege they have been subjected to discrimination establish facts from which it may be presumed that there has been discrimination (prima facie case), it is for the respondent to prove that there has been no breach of the right to non-discrimination? Are financial or other forms of support provided for individuals or groups who have been victims of tech-sector related human rights abuses, for example through legal aid? If so, who is eligible for these financial or other forms of support? Is legal advice and assistance available for individuals or groups who have been victims of tech-sector related human rights abuses? If so, who is eligible for these forms of legal aid and assistance.

	Are collective complaints, class action lawsuits and other forms of group litigation possible where there have been violations of human rights by the tech sector affecting multiple people? Are appropriate measures in place to ensure that individuals are protected from any adverse treatment or consequences in response to bringing a claim alleging violations of human rights by the tech sector?
Access to information	Does the state facilitate access to information in relation to available remedy mechanisms? If yes: • Is this information easily accessible and digestible?
State-based non-judicial mechanisms	Are there policies in place to promote access to state-based non-judicial grievance mechanisms, such as a data protection authority, a national human rights institution, or an ombudsperson? If yes: • Are these mechanisms legitimate, independent, accessible, predictable, equitable, transparent, and rights-compatible? Have there been any complaints lodged with the OECD NCP, if one exists, about tech companies? Have there been complaints or concerns raised with the national human rights institution, if one exists, about tech companies?
Remedies and sanctions	Are judicial and non-judicial mechanisms able to provide effective remedies, including sanctions, for tech sector-related human rights abuses? • Are such remedies and/or sanctions enforced effectively?

3.2. Non-state-based mechanisms	
Tech companies	Do tech companies provide accessible grievance and remedy mechanisms to address users' human rights concerns? Are these mechanisms legitimate, independent, accessible, predictable, equitable, transparent, and rights-compatible in accordance with the effectiveness criteria as per the UNGPs?

3.3. Extraterritoriality	
Extraterritoriality	Does the state exercise extraterritorial jurisdiction over the actions of companies headquartered or registered therein, or their subsidiaries, for human rights abuses committed abroad, particularly in relation to tech sector operations? Conversely, does the state exercise control over foreign registered tech companies operating in its jurisdiction? Do global/foreign tech companies submit to the jurisdictions of national courts?

Tech Sector and NAPs Checklist

The following checklist contains the minimum elements needed for states to ensure that the human rights implications of the tech sector are adequately taken into account as they begin the process of developing, evaluating, or revising a NAP. It has been designed in concert with the NAP Checklist found in the Toolkit.

1. Governance and Resources

- Identify all relevant government departments, agencies and other public bodies and institutions with a mandate relevant to technology, the tech sector and/or privacy, freedom of expression, and equality/non-discrimination, and ensure they are included in all steps of the NAP process. These should include, where they exist, not only relevant government departments but also regulatory bodies, national human rights institutions, ombudspersons and data protection agencies.

- Adequately resource these departments, agencies, bodies and institutions to ensure they are able to play an active role in stakeholder mapping, consultation, provision of capacity building and policy input.

2. Stakeholder Mapping and Participation

- As part of wide stakeholder mapping, conduct a specific mapping of all non-state actors with expertise and/or an interest in the development of policy relating to technology, the tech sector and/or privacy, freedom of expression and equality/non-discrimination.

- Facilitate the meaningful participation of these actors, ensuring the representation of multiple and diverse interests and providing adequate resources and capacity building where needed.

- Identify those most at risk of adverse and discriminatory impacts on privacy and freedom of expression and ensure they can participate in the process by taking into account their specific needs and vulnerabilities.

3. National Baseline Assessment

• Ensure that the organisation conducting the NBA has expertise on the tech sector and issues related to privacy, freedom of expression and equality/non-discrimination.

• Include questions specific to the tech sector and privacy, freedom of expression and equality/non-discrimination in the NBA, incorporating the results of the Tech Sector and NAPs NBA in this thematic supplement.

• Identify policy and regulatory gaps and the most salient privacy, freedom of expression and equality/non-discrimination risks.

4. Scope, Content and Priorities

• When considering the scope of the state's jurisdiction, take into account the importance of extraterritoriality in respect to the operations of the tech sector.

• Prioritise for action the most severe impacts of the tech sector and ensure that all commitments relating to the industry are specific, measurable, achievable, relevant, and time-specific.

5. Accountability and Follow Up

• Publish information about the NBA and NAP in an accessible, easy-to-understand format, in languages understood by all stakeholders, ensuring that any stakeholders affected by the tech sector who were consulted understand how their input was taken into account.

• Include stakeholders included in the framework for monitoring and reporting on the implementation of the tech sector-related actions in the NAP, including in any further policy development

ANNEX 1: THE TECH SECTOR IN EXISTING NAPS

STATE	COMMITMENT(S)
Czech Republic (2017) 	There are no tech sector-specific commitments in the Czech NAP. Instead, it refers to technology solely in the context of access to justice and the courts, noting that the judiciary "could benefit from the advantages delivered by advanced technology".
Finland (2014) 	The Finnish NAP notes that "[t]he protection of privacy that is particularly related to electronic communications has received plenty of attention in recent public discussion" and that "[p]rivacy questions related to electronic communications are particularly important in Finland, where the ICT infrastructure enjoys a strong position". The NAP commits to organising "a roundtable discussion (...) on how to ensure the protection of privacy in Finland with the authorities, ICT companies and the civil society".
Ireland (2017) 	There are no tech sector-specific commitments in the Irish NAP. However, it does refer to the fact that there are a large number of multinational tech companies in Ireland, and that Ireland's Data Protection Commissioner has responsibility for oversight of a large amount of data and has been involved in some high-profile cases. The NAP notes that the government is committed to supporting the Data Commissioner and has provided a fourfold increase in funding in its work.
Luxembourg (2018) 	There are no tech sector-specific commitments in the Luxembourg NAP. Instead, the NAP simply notes "the potential risk of negative impacts on human rights that activities in the private sector may have ... – including in the information and communication technologies – including the field of artificial intelligence – data protection ...".

Poland (2017) 	The Polish NAP makes a commitment to "draft a regulation to counteract restrictions on the freedom of speech, on the one hand, and to block illegal content on the Internet, on the other". These regulations would clarify the procedure for notice and takedown of illegal content online, and strengthen legal safeguards for freedom of expression in the activities of electronic service providers.
Sweden (2015) 	There are no tech sector-specific commitments in the Swedish NAP. However, it does note that: "Internet freedom and privacy are among the great global issues of the future. It is fundamental for Sweden that the human rights that apply offline also apply online."The NAP notes that Sweden helped ensure that the OECD Guidelines for Multinational Enter-prises now call on com-panies to support human rights on the internet, and that Sweden was one of a group of countries that tabled resolutions on internet freedom in the UN Human Rights Council in 2012 and 2014.
Switzerland (2016) 	There are no tech sector-specific commitments in the Swiss NAP. However, it does refer to the potential for "technologies for internet and mobile communication surveillance" to be used for both civilian and military purposes. It goes on to note that "[t]he export or brokerage of technologies for internet and mobile communication surveillance is governed by goods control legislation" and that "[t]he transfer of intellectual property, including expertise and the grant of rights, concerning technologies for internet and mobile communication surveillance was also made subject to license".
Thailand (2019) 	The Thai NAP focuses on technology primarily in the context of labour, noting that a key challenge in this field is to "protect labour from using technology to replace labour". In the list of planned activities, the NAP includes "Making plans or measures to support remedies and help groups of dismissed workers in accordance with regulations set for relief". The Ministry of Labour is in charge of this activity, with a timeframe of 2019-22

United Kingdom (2013,in 2016)

The UK NAP committed to "develop guidance to address the risks posed by exports of information and communications technology that are not subject to export control but which might have impacts on human rights including freedom of expression on line."

In 2014, the UK government, along with techUK, a technology trade association, and the Institute for Human Rights and Business published "Assessing Cyber Security Export Risks: Human Rights and National Security".

United States (2016)

The US NAP notes that:

"The impact and importance of business conduct in the ICT sector has grown as social, commercial, educational, and recreational interactions increasingly take place online."

The NAP commits the US government, "working with other agencies and stakeholders, [to] develop a regular mechanism to identify, document, and publicize lessons learned and best practices related to corporate actions that promote and protect human rights online". It also commits the government to "foster continued engagement among relevant stakeholders to support ongoing dialogue and collaboration on respecting human rights within the ICT sector".

ENDNOTES

1 See, for example, UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/35/22, 30 March 2017; UN Human Rights Council, Report of the Special Rapporteur on the right to privacy, UN Doc. A/HRC/40/63, 27 February 2019; UN Human Rights Council, Report of the Special Rapporteur on extreme poverty and human rights, A/74/493, 11 October 2019 and Jørgensen, R. F., Human Rights in the Age of Platforms ed., MIT Press, 2019.

2 International Corporate Accountability Roundtable and Danish Institute for Human Rights, National Action Plans on business and human rights Toolkit: 2017 edition, 2017, available at: https://www.humanrights.dk/publications/national-action-plans-business-human-rights-toolkit-2017-edition.

3 For the most recent figures, see Global Naps, available at: https://globalnaps.org/.

4 See below at Section 1.3.

5 A database of such legal actions can be found at the Digital Watch Observatory of the Geneva Internet Platform, available at: https://dig.watch/trends/uber.

6 The industry provides essential design, manufacturing, and assembly services to hardware companies. See the SASB Industry Brief at https://www.sasb.org/standard-setting-archive/technology-communications-industry-briefs/

7 The industry consists of companies that design or manufacture technology hardware products, including personal computers, consumer electronics, communications equipment, storage devices, components, and peripherals. See the SASB Industry Brief at https://www.sasb.org/wp-content/uploads/2019/08/SASB_Hardware_Brief.pdf

8 Internet media consists of search engines, Internet advertising channels, online gaming, social networks, as well as educational, medical, health, sports, and news online content. Internet-based services consist of companies selling services mainly through the Internet, such as event ticket sales, travel booking, photo sharing. See the SASB Industry Brief at https://www.sasb.org/wp-content/uploads/2019/08/SASB_Internet_Media-Services_Brief.pdf

9 The industry includes companies designing or manufacturing semiconductor devices, integrated circuits, their raw materials and components or capital equipment. See the SASB Industry Brief at https://www.sasb.org/wp-content/uploads/2019/08/SASB_Semiconductors_Brief.pdf

10 The industry includes companies that develop and sell application and system software through cloud-based and physical platforms, e.g. general applications software for personal and enterprise computers and mobile devices, specific software for engineering design, digital media, and healthcare. See the SASB Industry Brief at https://www.sasb.org/wp-content/uploads/2019/08/SASB_Software-IT_Brief.pdf

11 The industry consists of wireless and wireline telecom carriers. Wireless providers provide wireless telephony voice, data, text messaging, Internet, and satellite communications services. Wireline telecom providers operate wired infrastructure to provide telephony services, video programming distribution, and Internet services. See the SASB Industry Brief at https://www.sasb.org/wp-content/uploads/2019/08/SASB_Telecom_Brief.pdf

12 Sheng, E., "Employee privacy in the US is at stake as corporate surveillance technology monitors workers' every move", CNBC, 15 April 2019, available at: https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html.

13 The Economist, "The case for free speech at work", 27 February 2020, available at: https://www.economist.com/leaders/2020/02/27/the-case-for-free-speech-at-work.

14 Holmes, A., "Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working — and the service is seeing a rapid expansion since the coronavirus outbreak", The Business Insider, 23 March 2020, available at: https://www.businessinsider.nl/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3/.

15 Ennis, D. and Cook, T., "Bias from AI lending models raises questions of culpability, regulation", BankingDive, 16 August 2019, available at: https://www.bankingdive.com/news/artificial-intelligence-lending-bias-model-regulation-liability/561085/.

16 UN Human Rights Council, Resolution 34/7. The right to privacy in the digital age, UN Doc. A/HRC/RES/34/7, 7 April 2017.

17 UN Human Rights Committee, General Comment No.18: Non-discrimination, UN DOC. HRI/GEN/1/Rev.9 (Vol. I), 10 November 1989.

18 UN Human Rights Committee, General Comment No.18: Non-discrimination, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), 10 November 1989, Para 12.

19 See, for example, UN Human Rights Committee, Concluding Observations: Iceland, UN Doc. CCPR/C/ISL/CO/5, 31 August 2012, Para 6.

20 For the most recent figures, see Global Naps, available at: https://globalnaps.org/.

21 In May 2016, the UK updated its first NAP (adopted in 2013), and set out the actions taken to meet the commitments in the inaugural NAP, including those related to the tech sector: HM Government, Good Business: Implementing the UN Guiding Principles on Business and Human Rights, Updated May 2016, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/522805/Good_Business_Implementing_the_UN_Guiding_Principles_on_Business_and_Human_Rights_updated_May_2016.pdf.

22 The lack of SMART commitments and actions in NAPs generally has been noted. See, for example, Danish Institute for Human Rights, National Action Plans & Business and Human Rights: An Analysis of Plans from 2013 - 2018, 2018, pp.

21-23, available at: https://mk0globalnapshvllfq4.kinstacdn.com/wp-content/uploads/2018/11/nap-analysis-full-report.pdf.
23 See, for example, Kreps, S. E., Social Networks and Technology in the Prevention of Crimes against Humanity" in Rotberg, R.R. (ed.), Mass Atrocity Crimes: Preventing Future Outrages, World Peace Foundation, 2010; Hargreaves, C. and Hattotuwa, S., ICTs for the Prevention of Mass Atrocity Crimes, ICT for Peace Foundation, October 2010, available at: http://ict4peace.org/wp-content/uploads/2010/11/ICTs-for-the-Prevention-of-Mass-Atrocity-Crimes1.pdf.
24 See, for example, Amnesty International, Surveillance Giants, 2019, available at: https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/
25 UN Human Rights Council, Report of the Special Rapporteur on the right to privacy, UN Doc. A/72/43103, 19 October 2017, Para 75.
26 Ibid.
27 See, for example, Amnesty International, Surveillance Giants, 2019, available at: https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/.
28 See, for example, the research undertaken by the University of Essex's Human Rights, Big Data and Technology project, available at: https://www.hrbdt.ac.uk/.
29 See Borgesius, F. Z., Discrimination, Artificial Intelligence, and Algorithmic Decision-Making, Directorate General of Democracy, Council of Europe, 2018, available at: https://rm.coe.int/discrimination- artificial-intelligence-and-algorithmic-decision-making/1680925d73.
30 Ibid.
31 Dastin, J., "Amazon scraps secret AI recruiting tool that showed bias against women", Reuters, 10 October 2018, available at: https://www.reuters.com/article/us-amazon-com-jobs-automation-in...-ai-recruiting- tool-thatshowed-bias-against-women-idUSKCN1MK08G.
32 Ibid.
33 Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, May 2014, available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
34 Angwin, J., Tobin, A. and Varner, M., "Facebook (Still) Letting Housing Advertisers Exclude Users by Race", ProPublica, November 2017, available at: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin. In March 2019, Facebook announced restrictions to targeting options for housing, employment, or credit ads in the USA as part of a settlement with civil right organisations.
35 Angwin, J. et al., "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks", ProPublica, 23 May 2016,

available at: https://www.ProPublica.org/article/machine-bias-riskassessments-in-criminal-sentencing.

36 Confessore, N., "Cambridge Analytica and Facebook: the scandal so far", The New York Times, 4 April 2018, available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

37 Perlroth, N., "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack", The New York Times, 3 October 2017, available at: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

38 Human Rights Watch, Dark Side Secret Origins of Evidence in US Criminal Cases, 9 January 2018, available at https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

39 See a list of cases at the Business and Human Rights Resource Centre, Corporate Legal Accountability Hub, available at https://www.business-humanrights.org/en/corporate-legal-accountability/case-profiles/industry/technology.

40 Human Rights Watch, China: Big Data Fuels Crackdown in Minority Region, available at: https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.

41 Freedom House, Freedom on the Net 2018, The Rise of Digital Authoritarianism, available at: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

42 Ibid.

43 See https://necessaryandproportionate.org/principles.

44 See https://www.reformgovernmentsurveillance.com.

45 Five Country Ministerial, Statement of Principles on Access to Evidence and Encryption, available at: https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf.

46 European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 12 March 2019, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

47 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj.

48 European Data Protection Board, 1 year GDPR - taking stock, 22 May 2019, available at: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.

49 Commission Nationale de l'Informatique et des Libertés, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019, available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.
50 See the Equal Rights Trust's submission to the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance in relation to the acute and structural threats that new information technologies such as big data, machine learning, and AI pose to the rights to non-discrimination and racial equality human rights principles and standards, available at https://www.equalrightstrust.org/news/equal-rights-trusts-submission-un-special-rapporteur-contemporary-forms-racism.
51 Access Now, The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems, available at: https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/.
52 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/73/348, 29 August 2018, Para 12
53 See, for example, the 2019 study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, February 2019, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.
54 Amnesty International, Toxic Twitter: A Toxic Place for Women, March 2018, available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.
55 UN Human Rights Council, Report of the independent international fact-finding mission on Myanmar, UN Doc. A/HRC/39/64, 12 September 2019, Para 74. The report makes explicit reference to the role of Facebook in spreading hate speech vis-à-vis the Rohingya in Myanmar.
56 Ibid.
57 Access Now, The State of Internet Shutdowns Around the World: #KeepItOn Report, available at: https://www.accessnow.org/keepiton/.
58 Ibid.
59 Global Network Initiative, Disconnected: A Human Rights-Based Approach to Network Disruptions, June 2018, available at: https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf.
60 Weidmann, N. B., Benitez-Baleato, S., Hunziker, P., Glatz, E. and Dimitropoulos, X. (2016), Digital discrimination: Political bias in Internet service provision across ethnic groups. Science, 353(6304), 1151-1155
61 UN Human Rights Council, Resolution 32/13. The promotion, protection and

enjoyment of human rights on the Internet, UN Doc. A/HRC/RES/32/13, 18 July 2016.
62 See, for example, UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/35/22, 30 March 2017.
63 Electronic Frontier Foundation, NGO Community Urges ICANN to Scrutinize the .ORG Sale, March 2020, 9 March 2020, available at: https://www.eff.org/deeplinks/2020/03/ngo-community-urges-icann-scrutinize-org-sale.
64 Worldwide digital population as of January 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/.
65 UN Human Rights Council, Resolution 32/13. The promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/RES/32/13, 18 July 2016.
66 BBC, Websites to be fined over 'online harms' under new proposals, 8 April 2019, available at: https://www.bbc.com/news/technology-47826946.
67 Freedom on the Net 2018, The Rise of Digital Authoritarianism, p. 2, available at https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf
68 See, for example, Electronic Frontier Foundation, EFF, Human Rights Watch, and Over 70 Civil Society Groups Ask Mark Zuckerberg to Provide All Users with Mechanism to Appeal Content Censorship on Facebook, 13 November 2018, available at: https://www.eff.org/press/releases/eff-human-rights-watch-and-over-70-civil-society-groups-ask-mark-zuckerberg-provide.
69 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/38/35, 6 April 2018, Para 27.

70 See, for example, Article 19, Facebook Community Standards: Analysis against international standards on freedom of expression, 30 July 2018, available at https://www.article19.org/resources/facebook-community-standards-analysis-against-international-standards-on-freedom-of-expression/; Article 19, Twitter Rules: Analysis against international standards on freedom of expression, 6 September 2018, available at https://www.article19.org/resources/twitter-rules-analysis-against-international-standards-on-freedom-of-expression.
71 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/73/348, 29 August 2018, Para 15.
72 See https://santaclaraprinciples.org.
73 See https://www.manilaprinciples.org.
74 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc.

A/HRC/38/35, 6 April 2018, Paras 41-63.
75 Ibid., Para 48.
76 Article 19, The Social Media Councils Consultation Paper, June 2019, available at https://www.article19.org/wp-content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf
77 Facebook, Preparing the Way Forward for Facebook's Oversight Board, January 28, 2020, available at https://about.fb.com/news/2020/01/facebooks-oversight-board/.
78 Horowitz, J., In Italian Schools, Reading, Writing and Recognizing Fake News, The New York Times, 18 October 2017, available at: https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html.
79 Apple, Apple teams with media literacy programs in the US and Europe, 19 March 2019, available at: https://www.apple.com/uk/newsroom/2019/03/apple-teams-with-media-literacy-programs-in-the-us-and-europe/.
80 Freedom House, Freedom on the Net 2018, The Rise of Digital Authoritarianism, available at: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
81 Ibid.
82 See, for example, the Office of Denmark´s Tech Ambassador, https://techamb.um.dk/en/.
83 Relevant regional industry bodies include the European Internet Services Providers Association, Asia Pacific Top Level Domain Association, Council of European National Top-Level Domain Registries.
84 See https://www.esafety.gov.au.
85 See https://www.justitsministeriet.dk/ministeriet/raad/dataetisk-raad
86 See https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation.
87 For more information, see the Human Rights and Technology Discussion Paper, December 2019, https://www.humanrights.gov.au/about/news/human-rights-and-technology-discussion-paper-launches
88 See https://www.humanrights.dk/research/research-areas/research-technology
89 See for more information, relevant publications by Rikke Frank Jørgensen: https://www.humanrights.dk/staff/rikke-frank-jorgensen
90 International Corporate Accountability Roundtable and Danish Institute for Human Rights, National Action Plans on business and human rights Toolkit: 2017 edition, 2017, available at: https://www.humanrights.dk/publications/national-action-plans-business-human-rights-toolkit-2017-edition, Section 2.1.7.
91 See Committee on the Rights of the Child, General Day of Discussion on Digital Media and Children's Rights, 2014, https://www.ohchr.org/EN/HRBodies/CRC/Pages/Discussion2014.aspx. For more information about the impacts of online

gaming on children, see also https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

92 See BBC News, Toy firm VTech fined $650,000 over data breach, 9 January 2018, available at https://www.bbc.com/news/technology-42620717; US Federal Trade Commission, FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers, 30 November 2010, available at: https://www.ftc.gov/news-events/press-releases/2010/11/ftc-settles-company-failed-tell-parents-childrens-information; US Federal Trade Commission, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, 4 September 2019, available at: https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

93 Human Rights Watch, No Support: Russia's 'Gay Propaganda' Law Imperils LGBT Youth, December 11, 2018, available at: https://www.hrw.org/report/2018/12/11/no-support/russias-gay-propaganda-law-imperils-lgbt-youth

94 Internet Watch Foundation, Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse, May 2018, avilable at: https://www.iwf.org.uk/sites/default/files/inline-files/Distribution

95 See, e.g., Leibowitz, A., "Could Monitoring Students on Social Media Stop the Next School Shooting?", The New York Times, 6 September, 2018, available at: https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.

96 See UN Human Rights Council, Resolution 38/5. Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts", UN Doc. UN Doc. A/HRC/RES/38/5, 2 July 2018.

97 See, for example, UN Human Rights Council, Report of the UN Special Rapporteur on violence against women, its cause and consequences on online violence against women and girls from a human rights perspective, UN Doc. A/HRC/38/47, 14 June 2018.

98 UN Human Rights Council, Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective, UN Doc. A/HRC/35/9, 5 May 2017.

99 Amnesty International, Toxic Twitter- A Toxic Place for Women, March 2018, available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

100 Human Rights Watch, Internet Bringing New Forms of Violence Against Women Resignation of US Rep. Katie Hill Highlights Severe Protection Gaps, 28 October 2019, available at: https://www.hrw.org/news/2019/10/28/internet-bringing-new-forms-violence-against-women.

101 Inter-Parliamentary Union and Parliamentary Assembly of the Council on

Europe, “Sexism, harassment and violence against women parliamentarians”, Issues Brief, October 2018.

102 Ashraf, A., “A dark trade: rape videos for sale in India by Asad Ashraf, Al Jazeera, 31 October 2016, available at https://www.aljazeera.com/indepth/features/2016/10/dark-trade-rape-videos-sale-india-161023124250022.html.

103 Kamran, H., Hostile Bytes, A study of online violence against women journalists, October 2019, available at: http://digitalrightsmonitor.pk/wp-content/uploads/2019/11/Hostile-Bytes.pdf.

104 Leitão, R., Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse, Designing Interactive Systems Conference, June 2019, available at: https://dl.acm.org/doi/10.1145/3322276.3322366.

105 See ICT Facts and Figures 2017, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.

106 Amnesty International, Israel: Amnesty International engages in legal action to stop NSO Group’s web of surveillance, 13 May 2019, available at: https://www.amnesty.org/en/latest/news/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance/.

107 Statement for the protection of digital rights defenders, 18 December 2019, https://www.accessnow.org/join-our-statement-for-the-protection-of-digital-rights-defenders/.

108 Human Rights Watch, Sudan: End Network Shutdown Immediately Internet Vital for Safety, Communications in Crisis, 12 June 2019, https://www.hrw.org/news/2019/06/12/sudan-end-network-shutdown-immediately.

109 Financial Times, Data leak reveals China is tracking almost 2.6m people in Xinjiang, 17 February 2019, https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812.

110 Ghaffary, S., “The algorithms that detect hate speech online are biased against black people”, Vox, 15 August 2019, available at: https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter.

111 Williams, M. L., Burnap, P., Javed, A., Liu, H. and Ozalp, S., “Hate in the Machine: Anti-Black and Anti-Muslim Social Media Posts as Predictors of Offline Racially and Religiously Aggravated Crime”. The British Journal of Criminology, Vol. 60 (1), January 2020, p. 93–117.

112 UN News, “UN human rights office welcomes moves to curtail spread of hatred and violence online”, 29 May 2020, available at: https://news.un.org/en/story/2020/05/1065092.

113 See University of Essex letter to the Board of ICANN, 22 April 2019, available at: https://www.icann.org/en/system/files/correspondence/van-ho-doyle-to-chalaby-22apr19-en.pdf

114 Human Rights Watch, Myanmar Again Cuts Rakhine State’s Internet, 5 February 2020, available at: https://www.hrw.org/news/2020/02/05/myanmar-again-cuts-rakhine-states-internet.

115 Pinnell, O. and Kelly, J., “Slave markets found on Instagram and other

apps", BBC News, 31 October 2019, available at: https://www.bbc.com/news/technology-50228549.

116 UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/38/35, 6 April 2018, Para 27.

117 Ibid., Para 30.

118 Alexander, J., "LGBTQ YouTubers are suing YouTube over alleged discrimination", The Verge, August 2019 https://www.theverge.com/2019/8/14/20805283/lgbtq-youtuber-lawsuit-discrimination-alleged-video-recommendations-demonetization. YouTube denies this, saying the company does "not automatically demonetize LGBTQ content".

119 International Corporate Accountability Roundtable and Danish Institute for Human Rights, National Action Plans on business and human rights Toolkit: 2017 edition, 2017, available at: https://www.humanrights.dk/publications/national-action-plans-business-human-rights-toolkit-2017-edition, Section 2.2.

120 A sector-wide impact assessment (SWIA) aims to assess the potential impacts of a specific business sector in a particular geographic context. In doing so, an SWIA (a) addresses multiple levels of analysis; (b) aims to shape policy, law and projects; (c) involves extensive field research; (d) takes a broad view of human rights impacts, and (e) serves as a public resource. See, for example, the Sector-Wide Impact Assessment of Myanmar's ICT Sector undertaken by the Myanmar Centre for Responsible Business, available at: https://www.myanmar-responsiblebusiness.org/sectors/ict.html.

121 See, for example, Google Inc. v Equustek Solutions Inc. 2017 SCC 34 (Supreme Court of Canada) and Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18 (European Court of Justice); and Marsh, S., "'Right to be forgotten' on Google only applies in EU, court rules, The Guardian, 24 September 2019, available at: https://www.theguardian.com/technology/2019/sep/24/victory-for-google-in-landmark-right-to-be-forgotten-case.