
Chapter 12. Exploring the role of HRIA in the information and communication technologies (ICT) sector

Authors: Rikke Frank Jørgensen, Cathrine Bloch Veiberg and Niels ten Oever

12.1 INTRODUCTION

Human rights scrutiny of the information and communication technologies (ICT) sector has increased since the first commitments to human rights online were made during the World Summit on the Information Society in 2003. Human rights and ICT is currently on the international human rights agenda of several United Nations (UN) special rapporteurs (see, e.g., United Nations Human Rights Council [UNHRC], 2016a, 2016b, 2018a, 2018b). Mapping out the role of the ICT sector vis-à-vis human rights, however, is no straightforward task. Over the past twenty years, the sector has facilitated a revolution in access to information and communication; and it has had a transformative impact on individuals' ability to express, assemble, mobilize, inform, learn and educate around the globe. At the same time, the ability of states to compel action by ICT companies (such as to disclose private user information) has been the source of some of the most widespread and severe human rights abuses facilitated by the sector (Sullivan, 2016). Despite the growing awareness of such government pressures, ICT companies around the globe continue to be targeted by public authorities interested in accessing user data, controlling unwanted content and shutting down networks (UNHRC, 2016b). In response, ICT companies in some national contexts have taken on an important role in defence of their users' rights by pushing back against repressive state behaviour. Moreover, companies within the sector are increasingly attuned to the human rights framework and seek to develop standards on how to respond to – and mitigate – overreach by governments, as addressed in further detail in this chapter.

However, ICT companies' own commercial interests and business models also have major human rights implications. In his first report, the UN Special Rapporteur on the Right to Privacy, Joe Cannataci, warns, 'The data available for the profiling of individuals is now in order of magnitude larger than it was in 1991-1992 and the extent of risks for privacy associated with the use or misuse of that data are not yet completely understood' (UNHRC, 2016a). On a similar note, the UN Special Rapporteur on Freedom of Expression, David Kay, remarks, 'Vast social media forums for public expression are owned by private companies. Major platforms aggregating and indexing global knowledge, and designing the algorithms

that influence what information is seen online, result from private endeavour' (UNHRC, 2016b). One area of concern is the self-regulatory measures of these corporate platforms, such as blocking of alleged illegal or harmful content. The concern is particularly related to the platforms' means of 'content regulation' and privacy practices; for example, their day-to-day decisions on which content to remove or leave up, and the extent to which they collect, process, and exchange personal data with third parties. Similar issues are at hand at 'lower layers' of the services where companies in the business of providing internet infrastructure and hardware decide on the protocols and standards that influence what is, and what is not, possible on the internet (Cath & Floridi, 2017). Scholars and civil society groups have warned of a governance gap, where private actors with strong human rights impacts steer in the soft regime of guidelines and corporate social responsibility, with no legally binding human rights obligations, except when human rights issues have been transposed into national or regional legislation (see, e.g., Callamard, 2018; Laidlaw, 2015). The 2016 European Union (EU, 2016) General Data Protection Regulation, for example, stipulates privacy and data protection rules on companies doing business in EU member states.

This chapter provides an overview of how human rights are relevant to the ICT sector, including examples of adverse human rights impacts (Section 12.2) and of different types of human rights analyses performed in the sector (Sections 12.3). It then considers a concrete HRIA case study, targeting an internet registry in the Netherlands (Section 12.4). In conclusion (Section 12.5), the case study is used to highlight some of the challenges for conducting HRIA in relation to domain name management, namely: ensuring rights-holder engagement in the assessment process; developing a comprehensive terminology that captures not only the diversity of the sector, but also the diversity of potentially affected rights; determining responsibility for human rights harms; and the need to propose rights-respecting solutions to the current governance gap. The discussion is based on a review of the relevant literature, as well as the experience of the authors as practitioners working with the ICT sector and HRIA.

The chapter argues that it is challenging to identify the adverse human rights impacts in the sector due to the diverse range of activities, the physical and virtual footprints of the actors that comprise the industry, as well as the size and global character of affected rights-holders. Nevertheless, through the case study, the authors demonstrate ways in which the role of a domain name provider such as SIDN can be assessed, as an example of how to approach the broader scope of impacts pertaining to this type of infrastructure provider. The HRIA of SIDN was, however, only a pilot exercise and more assessments targeting different industry actors will need to take place to further qualify the approach.

12.2 IDENTIFYING HUMAN RIGHTS HARMS

Identifying the adverse human rights impact of the ICT sector is complicated by a number of factors. The sector comprises very diverse types of companies, including hardware producers, telecommunication and internet service providers, social media platforms, search engines, domain name registries and registrars, and various content aggregators. The diversity within the sector, the distributed architecture of the internet, and the direct link to core processes of public participation that many of the companies provide,

means that the business activities of the sector intersect with human rights in ways that are different from the more well-known business and human rights (BHR) examples, as we shall see below.

The more obvious examples of BHR often include a relatively clear and identifiable human rights abuse and a relatively clear and identifiable duty-bearer, for instance related to labour rights violations or environmental harms. Likewise, some of the human rights abuses in the ICT sector look like these kinds of impacts, for example, the poor treatment of workers in factories owned by Apple's suppliers (Liao, 2018). There is, however, an additional layer of human rights harms in the ICT sector compared to these well-known examples. Besides having obligations towards their employees and the communities in which they operate, many companies in the ICT sector may negatively affect the human rights of billions of users, as part of the services and platforms they provide (BSR, 2014; see also Chapter 2 in this *Handbook*). This particular feature of the sector presents significant challenges for clarifying the human rights responsibilities of these companies. Thus, while ICT companies may be contributing to a range of more 'obvious' human rights abuses, the reach and impact on the communication and privacy of users worldwide is unique to the sector. Effectively, the role that many ICT companies play as gatekeepers and intermediaries in the online ecosystem implies that the way they prioritize, curate, remove, process, and share content affects what information users may communicate, access and view through their services and platforms. The notion of 'intermediaries' refer to 'third-party platforms that mediate between digital content and the humans who contribute and access this content' (DeNardis, 2014, p. 154). Likewise, self-regulatory measures to counter, for example, hate speech, affect the ways in which users encounter content and expression on sensitive topics. As the UN Special Rapporteur on Freedom of Expression notes, it remains an open question how freedom of expression concerns raised by corporate policy, design and engineering choices should be reconciled with the freedom of private entities to design and customize their platforms as they choose (UNHRC, 2016b). This points to the challenge of defining when a corporate interference in users' rights amounts to a human rights abuse, as well as the challenge of determining responsibility. From the perspective of international human rights law, the state is the primary duty-bearer responsible for respecting, protecting and fulfilling individuals' rights; including protecting individuals from abuses caused by non-state actors. As such, states incur responsibility not only for human rights abuses that they inflict themselves, but also those caused by third parties which they fail to prevent, punish and remediate. In relation to freedom of expression and privacy, state action has traditionally been an essential element of the alleged human rights violation (Land, 2018). For example, if a *government* orders a private platform to remove content, this constitutes a violation of the right to freedom of expression under human rights law unless the order pursues a legitimate aim, has a legal basis, and is proportionate (necessary to achieve the government's purpose and the least restrictive means for doing so). If the *platform* itself removes content, this is private action outside the direct reach of human rights law, unless there is no alternative venue for that speech (Jørgensen & Pedersen, 2017). Legally speaking, platforms such as Facebook, YouTube or Twitter constitute private property made open to the public, thus the relationship between the platform and the user is governed by the terms of service, rather than human rights law. Likewise, the information that users provide as they contribute to the platform is owned by the company and may be used according to the terms specified. While some of the most widely used platforms and services may affect

public and private life in a way traditionally reserved for public authorities, they are in most national contexts free from legally binding standards to protect human rights such as freedom of expression and privacy. Whereas this governance gap may have a positive impact on users' access to communicate in a repressive state context, it does not take away the challenge that this lack of human rights safeguards raises, including within democratic societies. Scholarship is only now beginning to address the broader societal implications of having the online domain of access, search, expressions, debate, social networks and so forth based on privately owned platforms and services, thus the 'double logic' of public participation and commercial interest (Gillespie, 2018; Jørgensen, 2017). In the next section, we will examine some of the initiatives taken by companies within the ICT sector to ensure respect for human rights.

12.3 HUMAN RIGHTS IMPACT ASSESSMENT IN THE ICT SECTOR

The activities and value chains of ICT sector companies are diverse and include everything from physical activities (such as building physical ICT infrastructure) to purely online activities (such as providing internet access or managing user-generated content). The diversity of the sector presents various challenges for HRIA in the context of ICT – including challenges such as the scale and global character of users; the uncertainly as to when a corporate practice constitutes an interference in users' rights (for example, sharing of user data); and the governance gaps mentioned above.

In accordance with the *United Nations Guiding Principles on Business and Human Rights* (UNGPs) business enterprises have a responsibility to respect human rights, which includes a requirement that businesses assess their human rights impacts as part of due diligence (UNHRC, 2011) (for a basic overview of HRIA see Chapter 1 in this *Handbook*). This requirement applies to all companies, regardless of the sector, and is thus directly relevant to companies operating in the ICT sector. It is also worth noting that in his report on 'freedom of expression and the private sector in the digital age' the UN Special Rapporteur on Freedom of Expression emphasized the responsibility of technical and business actors involved in internet governance to respect human rights (UNHRC, 2016b).

While HRIA is a relatively new concept, including in the ICT sector, several companies within the sector, such as hardware producers, have worked with human rights topics for years, as part of corporate social responsibility (CSR). For example, initiatives such as the Responsible Business Alliance (RBA) – previously the Electronic Industry Citizenship Coalition (EICC) – address topics such as worker rights and conditions, social and environmental responsibility, and equality and non-discrimination (see RBA, 2018). Also, several of the telecommunication companies have worked with risk assessments in relation to their human rights impact – for example, Ericsson (2018), Telia (2017) and Telenor (2016) (see also Chapter 2 in this *Handbook*).

As for the internet companies, some of the major platforms, including Google and Facebook, are united in the Global Network Initiative (GNI). The GNI was established in 2008 in order to address the specific human rights risks that the sector had been exposed to (Maclay, 2014). It started as a multi-stakeholder initiative to guide internet companies when

governments make requests that may violate international human rights standards on freedom of expression and privacy; for example, requests for content removal that are not lawful, legitimate and proportionate (Jørgensen, 2018). In 2016, the Telecommunication Industry Network, a coalition of European internet and telecommunication providers, joined the GNI. The GNI approach has been to assist participating companies by developing guidelines and good practice on how to anticipate and respond to situations in which host country law and practice differ from international standards on freedom of expression and privacy. Moreover, GNI members commit to undergo assessment by an independent third party on a periodic basis in order to evaluate their compliance with the GNI principles (Maclay, 2014). The third-party assessments are not publicly available, however, a summary report is published by the GNI. Also, several of the internet and telecommunication companies publish annual transparency reports in which they reveal aggregate numbers about government requests for interference in their users' communication. The GNI principles were written before the UNGPs but have been subsequently updated.

In 2015, one of the first ICT sector-wide impact assessments (SWIA) was carried out in Myanmar (Myanmar Centre for Responsible Business [MCRB] et al., 2015; see also Chapter 5 in this *Handbook*). While Myanmar continues to be a high-risk country with lack of adequate policy and legal frameworks to protect human rights, the ICT sector is playing an increasingly important role in transforming the country. Besides encouraging responsible business practices in the growing ICT sector in Myanmar, the SWIA accounts for the wider impacts on society associated with the growing use of ICT, such as surveillance of communications and online hate speech (MCRB et al., 2015).

In short, a variety of approaches exist within the sector, with the 'older' members of the industry being most attuned to the broader range of human rights topics, while the 'younger' internet companies have focused mostly on how to mitigate government overreach in relation to the communication of their users. Few (if any) of the major internet platforms have recognized the full range of their impacts, negative and positive, on all human rights, including economic, social and cultural rights. The focus on freedom of expression and privacy by the platforms is not surprising, as these two rights have attracted a lot of attention in the public debate, whereas working conditions of content moderators, for example, is a less covered topic.

While different models for human rights risk assessment in the ICT sector exist, the following is a list of some of the common components, focusing in particular on the right to freedom of expression and privacy as two areas of concern for the ICT sector (Samway, 2014):

1. Review the international legal basis for freedom of expression and privacy.
2. Review the general human rights landscape in the relevant country or region, with a particular focus on rule of law, freedom of expression and privacy.
3. Map local laws, regulations, court decisions or administrative practices regarding the protections of freedom of expression and privacy.
4. Map business and product plans for entry into the market in order to determine potential risk areas for the company's products and services.
5. To the extent that an ICT company's products have the potential to promote human rights, the company should reiterate this objective in the HRIA.
6. Conduct risk scenarios based on the company's products and operations.

7. Propose strategies for mitigating those risks and protecting human rights.

The Danish Institute for Human Rights (DIHR) is one organization that has developed a *Human Rights Impact Assessment: Guidance and Toolbox* (HRIA Toolbox), which provides guidance and practical tools for conducting, commissioning, reviewing or monitoring HRIA of business projects and activities (see Götzmann et al., 2016). If we compare the components outlined by Samway (2014) to those outlined by the DIHR, we find a number of similarities, but also a number of differences. A key difference is in the scope and content of the DIHR's HRIA Toolbox being much more comprehensive for assessing human rights impacts at the project level, whereas the components outlined by Samway are for initial risk identification and assessment.

The nature of the ICT sector, in particular infrastructure providers, has less of a physical footprint in a specific physical location, but a more distributed one that includes many non-physical elements. However, the sector also has a number of more physical impacts, consider, for instance, the energy usage of large data centres in different parts of the world and the purchase of hardware, which might have been produced under conditions in breach of human rights. The case study presented in this chapter provides an example of how these various impacts on human rights have been assessed for an internet infrastructure provider (see Section 12.4).

As for the GNI, which includes some of the most powerful companies within the sector, their approach to consideration of human rights focuses exclusively on freedom of expression and privacy. Moreover, the guidelines developed by the GNI are oriented towards government interference, whereas corporate practices outside the government-company axe are left unaddressed (Jørgensen, 2018). As such, the risk assessments conducted pursuant to the GNI guidelines tend not to scrutinize the full range of business practices and procedures for their potential human rights impacts; for example, how the companies' terms of service may impact negatively on specific rights, whether their algorithms may discriminate against certain user groups, and how a potential negative impact may be remediated.

Efforts by civil society organizations (CSOs) to understand the application of human rights principles to internet intermediaries have also emphasized resistance to state pressure rather than understanding the impacts of business conduct and practices. The *Manila Principles on Intermediary Liability* developed by a broad coalition of civil society actors serve as an example of this (Electronic Frontier Foundation [EFF], 2015). The principles focus on government efforts to impose liability on companies for the content they transmit, and the associated chilling effect this liability has on the willingness of these companies to be platforms for free and open expressions (EFF, 2015).

Most recently, the human rights discourse is making its way into the realm of domain name management, as illustrated by the case study we consider next.

Box 12.1: Norms and standards for the ICT sector

The UNGPs provide the authoritative framework for identifying the human rights responsibilities of non-state actors, including in the ICT sector. The UNGPs are rather generic and cover all sectors, all countries and businesses of all sizes, but other initiatives

have supplemented with norm development for the ICT sector specifically. Such initiatives include the European Commission's *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (Knopf & Mayer-Scholl, 2013), the Global Network Initiative's (2017) *Principles on Freedom of Expression and Privacy*, the *Manila Principles of Intermediary Liability*, which establish baseline protection for intermediaries in accordance with freedom of expression standards (EFF, 2015), and the Ranking Digital Rights (2018) Corporate Accountability Index that proposes a methodology to evaluate companies in the ICT sector based on their adherence to international freedom of expression and privacy standards.

12.4 INTERNET REGISTRY CASE STUDY

12.4.1 Introduction

As outlined in the previous section, a number of examples exist of ICT sector HRIAs, predominantly in the internet and telecommunications sector and with a specific emphasis on the rights at risk in relation to government interference (including content removals and shutdowns of internet and telecommunication services). However, an area of the ICT sector that has received limited focus is that of the infrastructure providers, such as Top Level Domain (TLD) Registries. To make a contribution in this regard, this case study focuses on one such TLD to provide example insights regarding the human rights implications of such registries.

The basic function of a TLD registry in the Domain Name System (DNS) is to facilitate the translation of a human-readable domain name (such as example.com) into an IP-address. A TLD is the part of the domain name after the dot, such as .com. A TLD registry is responsible for administering the database of all domain names registered in each TLD that they are responsible for. Also, they generate the 'zone file' that allows DNS resolvers to route internet traffic to and from internet domains anywhere in the world. The international root-zone file refers to all the authoritative TLD registries. The authoritative root-zone file gets coordinated through the international Internet Corporation for Assigned Names and Numbers (ICANN).

There are two types of TLDs: (1) country code TLDs, such as .nl; and (2) generic TLDs, such as .info. ICANN accredits registries to operate generic TLDs. Country code TLDs are often delegated to a registry based on historical attribution of roles and through agreements with individual parties or governments. The agreements between ICANN, and the registry operators outline the responsibilities for each party (ICANN, 2017).

In April 2017, the UK-based freedom of expression organization ARTICLE 19, the DIHR and the Dutch internet domain registry SIDN (which manages .nl) collaborated to pioneer a model for assessing the human rights impacts of internet registries. The following sections describe and discuss the process and content of this model, which was meant as a pilot exercise for conducting HRIA of internet registries.

12.4.2 The HRIA Process

SIDNs interest in conducting the pilot HRIA was raised during the process of making a commitment to human rights part of ICANN's bylaw (Ten Oever, 2018). The HRIA pilot for SIDN was developed through close dialogue with ARTICLE 19 and the DIHR and included a number of phone calls and in-person meetings in Copenhagen and in the Netherlands.

The steps of the HRIA for SIDN were as follows:

1. Preparation: development of HRIA tool for internet registries – March-June 2017
2. Kick-off workshop: July 2017
3. Self-assessment: July-September 2017
4. Consolidation workshop: November 2017
5. Implementation, monitoring and reporting: ongoing from November 2017.

The preparation consisted mainly of ARTICLE 19, the DIHR and the general counsel at SIDN meeting to outline the various activities of SIDN and flesh-out how these activities potentially impacted on human rights. This was the first time ARTICLE 19 had been involved in designing and conducting a HRIA; it was also the first time that the DIHR had worked with an internet registry to conduct a HRIA. Previous experience of the DIHR within the ICT sector had been centred around telecommunications (this had included a collaboration with TeliaSonera in 2012 to support and review its corporate human rights work; see DIHR, 2012). Close collaboration in the planning phase was therefore vital for generating understanding among all three participating organizations regarding the activities of SIDN and linking these to human rights indicators to measure actual and potential impacts. A key challenge was understanding and mapping the core activities of SIDN as a TLD registry and identifying how these activities related to and impacted on human rights. This included engaging the registrars on the rights of registrants (in particular their rights to freedom of expression, privacy and non-discrimination). The process resulted in the development of both a HRIA tool and a HRIA implementation guidance outlining the process steps above. A generalized version of the tool and a description of the process was made publicly available by ARTICLE 19 and the DIHR late 2017 (ARTICLE 19 & DIHR, 2017).

The draft HRIA tool covered all aspects of SIDN operations – from human resources for their 85 staff, to the procurement of goods and services, their engagement with communities as well as their registry-related activities. The tool was aimed at supporting TLDs in identifying potential human rights impacts that are specific to the actions and operations of these particular actors, including the provision and maintenance of domain names, transparency, privacy, and engagement with third parties such as law enforcement agencies (ARTICLE 19 & DIHR, 2017). The HRIA tool contained scenarios and questions on TLD registry policies, procedures and performance within the areas in which the TLD may potentially be impacting human rights (see ARTICLE 19 & DIHR, 2017). The implementation guidance developed for SIDN provides a step-by-step guidance on the process of conducting a HRIA – including guidance on who to involve in the process, when to involve them, and how to follow up.

The second step in the HRIA process was a kick-off workshop. The workshop was attended by the CEO of SIDN as well as representatives for core SIDN functions to be involved in the assessment – including legal, human resources, accounts, technical and research staff. Six staff members attended the first workshop, with the general counsel acting as the main contact and internal focal point for the assessment. The purpose of the

workshop was twofold. First, the aim was to consolidate and adjust the draft tool developed by ARTICLE 19 and the DIHR. Second, the aim was to capacitate SIDN staff on human rights as they relate to the business activities and relationships of SIDN, and through this process create internal buy-in and support for the process as well as the follow-up actions coming from the assessment. The workshop included an introduction to HRIA, reflecting learning from other sectors besides ICT, as well as an overview of the potential challenges and dilemmas of applying this approach to internet registries. During the workshop, each section of the tool was discussed with a specific focus on the key registry services of SIDN and the tool was then adjusted based on this discussion.

The third step was for SIDN staff to evaluate the current operations against the scenarios, questions and indicators of the tool through self-assessment. This process proved less useful in terms of general awareness raising and capacity building of SIDN, as most questions were easily answered by key SIDN management personnel, which meant that there was limited involvement of the rest of the organization as well as external stakeholders.

The fourth step included a consolidation workshop. The workshop was conducted via teleconference and was attended by the same SIDN staff as the kick-off workshop as well as team members from the DIHR and ARTICLE 19. During the workshop each section of the self-assessment was discussed and analysed and based on this an overview of main observations (including a follow-up action plan with immediate to long-term follow-up actions) was developed. The observations included both recommendations and actions for SIDN to follow up on the assessment as well as recommendations and actions for ARTICLE 19 and the DIHR to improve the HRIA tool and process. An example of observations for SIDN included the need to further develop their internal diversity programmes and activities. During the workshop, a summary action plan to follow up on the assessment was also developed for SIDN with support from the DIHR and ARTICLE 19. Each follow-up action was assigned to a responsible person internally, resource implications were estimated and timelines were set. The assessment process further resulted in numerous changes and adjustments being made to the assessment tool itself (ARTICLE 19 & DIHR, 2017).

12.4.3 Reflections on the HRIA Process and Content

In this section of the chapter we reflect on the case study outlined above by comparing the process followed to 'good practice' criteria developed for HRIA. The purpose is to draw out strengths and weaknesses of the assessment that might inform development of HRIA methodology for the ICT sector going forward.

The DIHR's *Human Rights Impact Assessment: Guidance and Toolbox* (Götzmann et al., 2016) outlines ten 'key criteria' for HRIA, based on relevant literature and guidance (see also Chapter 1 in this *Handbook*).

When assessing the *process* of the SIDN pilot HRIA against the five process criteria (participation, non-discrimination, empowerment, transparency and accountability), a number of critical observations can be made on the level of meaningful participation of affected or potentially affected rights-holders during all stages of the impact assessment process. As can be seen from the process above, the direct engagement with rights-holders

as part of the HRIA process (except for own employees and communities in close proximity to the SIDN office in Arnhem, the Netherlands) was very limited. The website users, as well as the TLD registrants (i.e. individuals or organizations attaining a TLD for their website or email), have limited to no direct engagement with SIDN, and SIDN's main channel of engagement with them is through the registrars (i.e. the organization that manages the reservation of internet domain names with approval by the registry). SIDN, quite uniquely among registries, has a complaints mechanism where website users and registrants can make complaints about offensive TLDs and content. Further, SIDN also has a direct contract with registrants enforced by the registrars. Through the assessment, SIDN was asked to evaluate the complaints mechanism against the eight effectiveness criteria for non-judicial grievance mechanisms stipulated in the UNGPs (UNHRC, 2011). Consequently, SIDN was asked to evaluate whether the mechanism had brought about complaints that could indicate a lack of controls in managing human rights impacts experienced by rights-holders. However, this did not address the key challenge of the assessment of the mechanism not including direct engagement with registrars and registrants. The extent to which registrants were even aware of the mechanism was discussed by ARTICLE 19 and the DIHR with SIDN in some detail, including the extent to which registrars could be made to better inform about the mechanism to the registrars. The lack of direct engagement with rights-holders meant that the full HRIA was not performed in accordance with the 'participation' criterion, and that it relied solely on company self-assessment and user feedback collected and interpreted by the company against the HRIA tool developed by the DIHR and ARTICLE 19 for SIDN.

The DIHR, ARTICLE 19 and SIDN were very aware of this issue, and in order to better reach potentially affected rights-holders, SIDN, the DIHR and ARTICLE 19 decided to reach out to the CSOs representing the views and concerns of rights-holders during the assessment. This was done through presentations at Internet Governance Forums (IGFs), which included first that SIDN and ARTICLE 19 spoke of the assessment at the IGF in the Netherlands in the fall of 2017. Further, SIDN, ARTICLE 19 and the DIHR also spoke to their experiences at the global IGF in December 2017 (see IGF Geneva, 2017). However, the overall engagement with rights-holders was only limited to this level of engagement.

When assessing the *content* of the SIDN HRIA pilot against the five content criteria (benchmark, scope of impacts, assessing impact severity, impact mitigation measures, and access to remedy) the assessment tool and guidance was more aligned. It considered all human rights, across all business relationships and also included guidance on assessing impact severity. However, given the key gap in the process described above, the HRIA itself and the commitments in terms of follow-up were highly dependent on the truthfulness, knowledge and capacity of SIDN staff. The way in which the nature and structure of the industry presents a challenge to the identification and engagement with actually and potentially affected rights-holders will be discussed further in the next section of this chapter.

12.5 CHALLENGES

In this final section, we will highlight some of the key issues and challenges related to carrying out HRIA in relation to infrastructure providers, drawing on some of the experiences from the internet registry case study.

12.5.1 Difficulty of Assigning Responsibility

The internet was designed as a distributed architecture (Saltzer et al., 1984) in which there are no central technical points of control. Nonetheless, the internet is tied together through the distribution of unique IP addresses, Autonomous System Numbers and the delegation of unique domain names. Ensuring the distribution of these unique identifiers to facilitate communication is what ICANN (2018) aims to facilitate and coordinate through a self-described 'bottom-up, consensus-based, multi-stakeholder process' in which businesses, civil society and governments jointly discuss ICANN's policies. Because of its central place in the internet architecture it has been argued that this makes ICANN a de facto hybrid public-private regulator (Mueller, 2002; Weinberg, 2002). ICANN often emphasizes its narrow technical remit and non-political nature, but there are many examples that show that here once again the technical is political. An example that shows ICANN's involvement in traditionally intergovernmental issues is its decision to deny contested territories like Western Sahara or Somaliland a country code TLD (Park, 2009). ICANN claims that it solely uses the ISO country list for abbreviation but at the same time there are standing exceptions, for instance for Great Britain (which uses .uk instead of .gb) and the United States (which not only uses .us but also .gov). Other discussions that illustrate ICANN's contentious nature revolve around the delegations of TLDs. The registrar who controls a domain can largely determine who will be able to register a domain and under what conditions – a decision which becomes especially sensitive where it comes to domains such as .amazon and .gay. These delegations beg the question of whether a company should control a domain, or a specific community, and the answers to such questions can hardly be called 'technical' (on the political nature of HRIA see also Chapters 15, 22 and 25 in this *Handbook*).

Other examples include: the recurring debates in ICANN about privacy protection (or lack thereof) in the WHOIS database (a public directory with information on 'who is' responsible for a domain or IP address); the central, limited adoption of Internationalized Domain Names (IDNs) (the possibility to represent domains in non-latin characters); and the limited adoption of improved security protocols such as DNSSEC. These debates are complicated because the solutions cannot be implemented by ICANN. ICANN coordinates the delegation of the authority to distribute TLDs and IP-addresses. In the case of gTLDs they do have contracts with the registries on the specific conditions, but this is not the case for ccTLDs where there is a mere agreement. Registries in their turn do not have a full say about the conditions under which registrars can sell domains, let alone the detailed obligations of registrants. To make matters more complicated, the policies that ICANN implements are developed in part by the registries and registrars. In a largely self-regulatory environment such as the global internet it is complicated to organize the collaboration of independent entities such as registrars, who often have limited commercial incentive to adopt technologies such as DNSSEC and IDNs. This shows a downside to the distributed nature of the internet architecture: it is hard to roll-out improvements that do not directly result in a higher profit margins or introduce even more complexity. HRIAs can provide a partial answer to this by making these issues more visible and thus increase accountability among the myriad of domain name providers. On the other hand, HRIAs might form a significant burden for smaller domain name providers with small profit margins and without in-house legal expertise.

12.5.2 Governance Gaps

The combination of a privately-owned distributed infrastructure and the voluntary nature of the UNGPs poses the risk of a governance gap. Governments do not have direct control over internet infrastructure, which is hard to regulate because of its cross-jurisdictional nature. Next to that, the complexity of the distributed internet infrastructure makes it a significant task to ensure that all actors undergo HRIA, or at least establish human rights due diligence processes.

Therefore, it is important that actors with a large footprint – including major domain name providers – implement HRIAs. As part of this, the companies should adopt measures to ensure they respect human rights so a significant part of the burden does not fall on the smaller companies which do not have the capacity to do impact assessments. A good example is the recent publication in the RFC-series, the formal document series of the Internet Engineering Taskforce, the Internet Architecture Board and the Internet Research Taskforce. RFC8280 is titled 'Research into Human Rights Protocol Considerations' (Ten Oever & Cath, 2017) and provides guidelines for protocol developers to assess the impact of their protocol on the ability of end-users to exercise their human rights. This development coincides with the recent adoption of an addition of a core value to respect human rights to ICANN's bylaws and the development of the GNI principles (mentioned above), which, considered together, indicates a growing trend towards the awareness of the sector of its impact on human rights. Whether this indicates an actual improvement in the ability of end-users to exercise their human rights remains to be seen and will heavily depend on the implementation of these commitments. If the ICT sector fails to provide sufficient human rights safeguards it can be expected that governments will increase their regulatory initiatives, which has recently included the 2017 German Network Enforcement Act and the 2016 EU General Data Protection Regulation.

12.5.3 Clarifying Expectations and Terminology

The relationship between technology, infrastructure, power, rights and freedom has been established in a wide range of academic literature (see, e.g., Deibert et al., 2010; Jørgensen, 2019; Land & Aronson, 2018; Mumford, 1964; Star, 1999; Winner, 1980). Nonetheless, there is no existing framework to identify and evaluate the wide range of human rights impact, including both 'conventional' types of human rights harms, as well as the extra layer of potential harms related to companies that provide the technical and communicative infrastructure for billions of users world-wide. Whereas the ICT sector has a thorough understanding of safety and security (even though it is not always succinctly implemented), the understanding of its impact on civil and political rights is still relatively limited, let alone measurable. If we turn to economic, social, and cultural rights, these have barely been the focus of attention, at least for many of the platform and infrastructure providers. This warrants joint engagement of engineers, human rights experts, and impacted communities to develop such understanding and provide mitigation strategies.

12.6 CONCLUSION

As outlined in this chapter, it is no easy task to identify the adverse human rights impacts of the ICT sector. The diverse activities, the physical and virtual footprints of the actors that comprise the industry, and the size and global character of affected rights-holders present many challenges for HRIA within the sector. In this chapter we have provided examples of ways in which different actors have attempted to identify, assess and address specific rights, rights-holder relationships, and interactions with authorities relevant to their specific role in the ICT value chain. Through the case study, we have demonstrated the ways in which the role of a domain name provider such as SIDN can be assessed (along with the more cross-cutting issues of any organization, such as employee relations, supply chain management and community engagement), as an example of how to approach the full scope of impacts pertaining to this type of infrastructure provider. This was, however, only a pilot exercise and more assessments targeting different industry actors will need to take place to further qualify the approach. This includes addressing the challenges that we have only briefly touched upon, such as ensuring rights-holder engagement in the assessment process; developing a comprehensive terminology that captures not only the diversity of the sector, but also the diversity of potentially affected rights; determining responsibility for human rights harms; and finally, proposing rights-respecting solutions to the current governance gap.

REFERENCES

ARTICLE19, & Danish Institute for Human Rights (2017). *Sample ccTLD human rights impact assessment tool: Introduction to the tool.* London, England: Author.

BSR (2014). *Legitimate and meaningful. Stakeholder engagement in human rights due diligence: Challenges and solutions for ICT companies*. New York, NY: Author.

Callamard, A. (2019, forthcoming). *The human rights obligations of non-state actors*. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms*. Cambridge, MA: MIT Press.

Cath, C., & Floridi, L. (2017). The design of the internet's architecture by the internet engineering task force (IETF) and human rights. *Science and Engineering Ethics, 23*(2), 449-468.

Danish Institute for Human Rights [DIHR] (2012). *TeliaSonera partners with the Danish Institute for Human Rights*. Retrieved from https://www.humanrights.dk/node/1540

Deibert, R., John P., Rohozinski, R., Zittrain, J., & OpenNet Initiative (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Electronic Frontier Foundation [EFF] (2015). *Manila principles on intermediary liability*. San Francisco, CA: Author.

Ericsson (2018). *Human rights*. Retrieved from https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/responsible-business/human-rights

European Union, European Parliament and Council (2016). *Regulation 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation)* (2016/679/EU).

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. New Haven, CT: Yale University Press.

Global Network Initiative [GNI] (2017). *GNI principles on freedom of expression and privacy*. Washington, DC: Author.

Götzmann, N., Bansal, T., Wrzoncki, E., Poulsen-Hansen, C., Tedaldi, J., & Høvsgaard, R. (2016). *Human rights impact assessment: Guidance and toolbox. Road-testing version.* Copenhagen, Denmark: Danish Institute for Human Rights.

Internet Corporation for Assigned Names and Numbers [ICANN] (2018). *Developing policy at ICANN*. Retrieved from: https://www.icann.org/policy

Internet Governance Forum [IGF] Geneva (2017). *A net of rights: Human rights impact assessments for the future of the internet.* Retrieved from https://igf2017.sched.com/event/CTt7

Jørgensen, R. F. (2017). What do platforms mean when they talk about human rights? *Policy & Internet, 9*(3), 280-296.

Jørgensen, R. F. (2018). Human rights and private actors in the online domain. In M. K. Land & J. D. Aronson (Eds.), *New technologies for human rights law and practice* (pp. 243-269). Cambridge, England: Cambridge University Press.

Jørgensen, R. F. (2019, forthcoming). *Human rights in the age of platforms*. Cambridge, MA: MIT Press.

Jørgensen, R. F., & Pedersen, A. M. (2017). Online service providers as human rights arbiters. In M. Taddeo & L. Floridi (Eds.), *The responsibilities of online service providers* (pp. 179-199). Oxford, England: Oxford University Press.

Knopf, J., & Mayer-Scholl, B. (2013). *Tips and tricks for advisors: Corporate social responsibility for small and medium-sized enterprises*. Brussels, Belgium: European Commission.

Laidlaw, E. (2015). *Regulating speech in cyberspace*: *Gatekeepers, human rights and corporate responsibility.* Cambridge, England: Cambridge University Press.

Land, M. (2019, forthcoming). Regulating private harms online. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms*. Cambridge, MA: MIT Press.

Liao, S. (2018, January 2016). Apple supplier workers have been exposed to toxic chemicals, report finds. *The Verge*.

Maclay, C. M. (2014). *An improbable coalition: How businesses, non-governmental organizations, investors and academics formed the global network initiative to promote privacy and free expression online* (Doctoral dissertation, Northeastern University, Boston, US).

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.

Mumford, L. (1964). *The myth of the machine: Technics and human development*. New York: Harcourt.

Myanmar Centre for Responsible Business [MCRB], Institute for Human Rights and Business [IHRB] & Danish Institute for Human Rights [DIHR] (2015). *Myanmar ICT sector-wide impact assessment.* Yangon, Myanmar: Authors.

Park, Y. J. (2009). The national CCTLD disputes: Between state actors and non-state actors. *International Journal of Communications Law and Policy, 13*(1), 185-204.

Ranking Digital Rights (2018). *2018 accountability index*. Washington, DC: Author.

Responsible Business Alliance [RBA] (2008, January 1). *Code of conduct 6.0*. Retrieved from http://www.responsiblebusiness.org/code-of-conduct/

Saltzer, J., Reed, D., & Clark, D. (1984). End-to-end arguments in system design. *ACM Transactions on Computer Systems (TOCS), 2*(4), 277-288.

Samway, M. A. (2014). Business, human rights and the internet: A framework for implementation. In M. Lagon & A. C. Arend (Eds.), *Human dignity and the future of global institutions*. Washington, DC: Georgetown University Press.

Sullivan, D. (2016). *APC issue papers. Business and digital rights: Taking stock of the UN guiding principles for business and human rights in the ICT sector*. Melville, South Africa: Association for Progressive Communications.

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist, 3*, 377-391.

Telenor (2018). *Human rights assessment.* Retrieved from https://www.telenor.com/sustainability/reporting/gri-index/human-rights-assessment/

Telia (2017). *Human rights impact assessments.* Retrieved from https://www.teliacompany.com/en/news/news-articles/2017/human-rights-impact-assessments/

Ten Oever, N. (2018). Productive contestation, civil society, and global governance: Human rights as a boundary object in ICANN*. Policy & Internet.*

Ten Oever, N., & Cath, C. (2017). *Research into human rights protocol considerations*. Retrieved from https://www.rfc-editor.org/info/rfc8280

United Nations Human Rights Council [UNHRC] (2011, March 21). *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding principles on business and human rights: Implementing the United Nations 'protect, respect and remedy' framework* (A/HRC/17/31).

United Nations Human Rights Council [UNHRC] (2016a, November 24). *Report of the Special Rapporteur on the right to privacy, Joesph A. Cannataci* (A/HRC/31/64).

United Nations Human Rights Council [UNHRC] (2016b, May 11). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (A/HRC/32/38).

United Nations Human Rights Council [UNHRC] (2018a, April 6). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (A/HRC/38/35).

United Nations Human Rights Council [UNHRC] (2018b, June 18). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, Dubravka Šimonović* (A/HRC/38/47).

Weinberg, J. (2000). ICANN and the problem of legitimacy. *Duke Law Journal, 50*(1), 187-260.

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(1), 121-136.