ARTICLE 19

Human Rights Due Diligence and Internet Infrastructure

Pilot Project Outcome Report

8 June 2021

THE DANISH INSTITUTE FOR HUMAN RIGHTS

ARTICLE 19
Free Word Centre
60 Farringdon Road
London,
EC1R 3GA
United Kingdom

T: +44 20 7324 2500
F: +44 20 7490 0566

E: info@article19.org
W: www.article19.org

Tw: @article19org
Fb: facebook.com/article19org

A19/DIG/2021/002

Contents

Table of abbreviations

CDN	Content delivery networks
DANE	DNS-based Authentication of Named Entities
DIHR	Danish Institute for Human Rights
DNS	Domain name system
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
GDPR	General Data Protection Regulation
HRIA	Human rights impact assessment
HTTPS	Hypertext Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IP	Internet Protocol
ISP	Internet service providers
IXP	Internet exchange points
PIR	Public Interest Registry
SIDN	Stichting Internet Domeinregistratie Nederland
TLD	Top-level domain
UNGP	UN Guiding Principles on Business and Human Rights

Executive summary

Human rights scrutiny of the information and communication technology (ICT) sector has steadily increased since the first commitments to human rights online were made during the World Summit on the Information Society in 2003. Since 2011, the *UN Guiding Principles on Business and Human Rights* (UNGPs) have affirmed that all companies, including those that provide the services and technologies that make up the global Internet, have a responsibility to respect human rights by undertaking human rights due diligence. However, the uptake and scrutiny of corporate due diligence activities in the ICT sector over the last decade has happened unevenly, concentrating on Internet applications, platforms, and services that are more public-facing and largely overlooking infrastructural technologies and services including Internet registries and registrars, content delivery networks (CDNs), and Internet exchange points (IXPs).

The design, implementation, and management of Internet infrastructure is critically important to the free and full expression of human rights online. Infrastructure facilitates how people connect to the Internet, whether to access information, express their opinions, or exercise their right to freedom of association by connecting with other users. Due to its 'hidden' nature, Internet infrastructure can be exploited by governments to request access to personal information and data or to block online content. Many of these decisions are made unilaterally by Internet infrastructure providers, despite the impact it can potentially have on people, especially marginalised communities. Additionally, Internet infrastructure providers employ people, procure goods and services produced and provided by people, and run their operations in ways that can have ripple effects on society. Due diligence activities help companies comprehensively identify the potential and real impacts of their policies, practices, products, and services on human rights and take actions to mitigate them.

Nevertheless, there is a low rate of adoption of human rights impact assessments (HRIAs) and other forms of due diligence at the infrastructure level of the Internet. This problem is due in significant part to the lack of specific tools for conducting assessments or due diligence for these particular types of providers, and the fact that human rights are not yet normalised as essential considerations among them.

From 2017 to 2020, ARTICLE 19 and the Danish Institute for Human Rights (DIHR) conducted a pilot project in partnership with three Internet registries and registrars, with the objectives of: developing, testing, and refining a first-of-its-kind, publicly available model for assessing the particular human rights impacts and risks of Internet infrastructure providers; applying the tool to develop recommendations for each partner company; and educating key staff and management personnel of each partner company on the human rights framework and human rights due diligence.

Following the conclusion of this three-year project, this outcome report provides an overview of the corporate responsibility to protect human rights at the infrastructural level, explains the current state of human rights due diligence among Internet infrastructure providers, presents the major human rights risks and challenges for Internet infrastructure providers that were identified through the project, and presents key observations, conclusions, and recommendations that may be useful for Internet infrastructure providers as well as stakeholders in academia and civil society that are advocating for greater human rights due diligence in the ICT sector.

In general, significant progress has taken place in the ICT sector since the start of this project: there has been an increase in the number of companies that have made public commitments to human rights; increases and improvements in transparency reporting; greater focus on human rights in global and regional policy discussions, in part due to the leadership of key Internet registries and registrars; and greater alignment of dispute resolution systems with human rights standards. However, this outcome report identifies several fundamental sector-wide gaps that remain:

- The majority of Internet registries and registrars still lack explicit commitments to human rights and clear inclusion of human rights in existing due diligence systems, though certain systems may address specific human rights implicitly.

- Existing assessment frameworks and tools used by Internet registries and registrars heavily focus on aspects related to management and operations and are limited in assessing the impacts of their products and services on the communities that rely on them and society at-large.

- Human rights standards and expectations are generally not set as part of terms of engagement or agreements made with third-party suppliers and business partners.

- In general, the human rights framework is not applied to the development of internal company standards that can have clear human rights implications, such as anti-abuse policies.

While we focused the three test cases of this pilot project on Internet registries and registrars, the assessment model, conclusions, observations, and recommendations are applicable to all types of Internet infrastructure providers. This outcome report is designed to be a resource to any stakeholder working towards the widespread adoption of human rights due diligence in the ICT sector.

Introduction

Human rights scrutiny of the ICT sector has steadily increased since the first commitments to human rights online were made during the World Summit on the Information Society in 2003. According to the 2011 *UN Guiding Principles on Business and Human Rights* (UNGPs), all companies have a responsibility to respect human rights by undertaking human rights due diligence. This responsibility extends to companies that provide the services and technologies that make up the global Internet.

In recent years, newsworthy incidents such as the Facebook–Cambridge Analytica data scandal, Google's censorship of search results in China, and the suspension of Donald Trump and other high-profile individuals from social media platforms such as Twitter and Facebook have contributed to increased public scrutiny of the impacts that the policies and practices of powerful Internet companies have on the expression of human rights, particularly in the context of privacy and freedom of expression. In response, these companies have taken some action in apparent recognition of their due diligence responsibility: recent examples include Google's 2019 HRIA of a facial recognition product and the launch of the Facebook Oversight Board in 2020. However, whatever initial efforts have been made are largely concentrated on Internet applications and web platforms; the progress on the adoption and implementation of the UNGPs has been even slower among Internet infrastructure providers. Even the due diligence actions of companies such as Facebook and Google, which provide infrastructure-level products, have specifically focused on their public-facing content-layer products and services.

In ARTICLE 19's 2018 report, *Public Interest, Private Infrastructure*, we analysed Internet infrastructure providers within the broader ICT sector to identify the key drivers of adoption of human rights standards. As we expect with more public-facing Internet companies, we found that the primary drivers are reputational threats and concerns, such as scandals resulting in public pressure, and top-down accountability, where human rights due diligence is established as an internal priority by the company's executive leadership. With less public scrutiny on infrastructure providers, given the 'hidden' nature of their products and services within the Internet ecosystem, incentivising these companies to develop strong human rights due diligence presents a particular challenge. On this basis, we identified two problems that must be addressed to normalise fundamental due diligence

activities among them. First, there must be assessment tools and models that take into account the particularities of the policies, practices, products, and services of Internet infrastructure providers. Second, especially in the absence of public scrutiny and pressure, the human rights framework and corporate responsibility to human rights must be normalised among the key executive decision-makers within these companies.
To respond to these problems, ARTICLE 19 and DIHR launched a pilot project in 2017 that concluded in 2020. As part of the project, we partnered with three Internet registries and registrars of top-level domain names (TLDs) to serve as test cases:

1. Stichting Internet Domeinregistratie Nederland (SIDN), a Dutch Internet registry responsible for managing the '.nl' TLD.

2. Blacknight Internet Solutions Ltd., an Irish owned ICANN accredited registrar and hosting company specialising in serving the hosting and co-location needs of businesses. It is the market leader for the '.ie' TLD.

3. Public Interest Registry (PIR), a US Internet registry responsible for managing the generic TLDs '.org', '.ngo', and '.ong'.

The pilot project was designed to meet three major objectives:

1. To collaboratively develop and refine a human rights risk self-assessment tool that is tailored to the particularities of the products, services, policies, and practices of Internet infrastructure providers.

2. To test the tool by conducting a high-level human rights gap analysis of company policies, operations, and safeguards of the selected registries and registrars, and develop recommendations for each partner.

3. To educate staff and management of the selected registries and registrars on a basic understanding of human rights and corporate human rights due diligence and to demonstrate its relevance to their activities.

To meet these objectives, ARTICLE 19 and DIHR designed and conducted a three-day guided workshop with key legal, operations, and management staff from each partner company, consisting of interviews based on the assessment model and training on human rights and human rights due diligence. These workshops were preceded by planning meetings to contextualise the tool based on each company's needs and operations.

Following each workshop, ARTICLE 19 and DIHR used the findings to conduct a high-level human rights gap analysis, which led to tailored recommendations and a mutually agreed action plan with each partner company to improve their human rights due diligence. The first test case was conducted with SIDN and concluded in December 2017; the second test case was conducted with Blacknight and concluded in August 2018; and the third test case was conducted with PIR and concluded in March 2020. The tool and outcomes of each test case were publicly communicated to normalise and clarify what human rights due diligence looks like among infrastructure providers.[1]

This outcome report puts forward a comparative analysis of the three test cases in this pilot project. While this project focused on Internet registry and registrar operations, the assessment model, conclusions, observations, and recommendations are applicable to all types of Internet infrastructure providers. As such, the report presents an overall understanding of Internet infrastructure providers and their responsibility to human rights, cross-cutting findings of the human rights risks and trends that face them, and outlines several universal recommendations for Internet infrastructure providers and other supporting stakeholders within academia and civil society to enable more widespread adoption of human rights due diligence in the development, deployment, and operation of Internet infrastructure.

Internet infrastructure providers' responsibility to respect human rights

Why Internet infrastructure matters

Internet infrastructure comprises both physical and logical technologies and systems that connect computers and other devices around the world across different types of networks, from Bluetooth and Wi-Fi to 5G mobile and satellite networks. The physical layer consists of the tangible technologies that make up this network of networks, such as subsea cables, servers, cell towers, and routers. The logical layer consists of the rules and protocols that govern how data flows across these physical technologies.

The decisions that determine the design, implementation, and management of these infrastructure technologies and systems have an impact on who can connect to the Internet, how freely they can access and disseminate information, and who else can see what they do online. In his 2017 report to the UN Human Rights Council, David Kaye, the then UN Special Rapporteur on the protection and promotion of the right to freedom of expression, recognised the particular impacts that infrastructure providers such as Internet service providers (ISPs), IXPs, CDNs, and network equipment vendors have on human rights including freedom of expression, particularly in the context of surveillance and censorship.

A central aspect of global Internet infrastructure is the domain name system (DNS). Any Internet-connected device, including the servers that host the content that we produce and access online, has an Internet protocol (IP) address, so that incoming and outgoing data knows where to go. Domain names are identifiers for Internet resources, including websites, that help users more easily navigate their way online. For example, if a user wishes to access the ARTICLE 19 website, it would be easier to do so by remembering its domain name, 'article19.org', rather than the string of numbers that make up the IP address where ARTICLE 19's website is hosted. The DNS acts like a directory that connects domain names to their corresponding IP addresses, so that browsers can lead users to the right resources. The key Internet infrastructure providers that make up the DNS include Internet registries and registrars.

An Internet registry manages the administrative operations for TLDs, whether generic TLDs (gTLDs) like '.com' and '.org' or country-code TLDs (ccTLDs) like '.uk' and '.nl', and sets the policies by which individuals or entities can obtain a domain name associated with the TLD. An Internet registrar is an accredited entity that sells domain names to the public and registers domain names with the registry on behalf of the registrant. A registrant is an individual or entity that registers a domain name.

The operation and management of the DNS have fundamental impacts on human rights. Policies set by registries determine who can register websites or email addresses and under what domain names. Given how important websites are to how we disseminate and access content, these decisions can limit peoples' ability to freely and fully exercise freedom of expression and access to information, freedom of association, and right to political participation. The granularity, public availability, and security of registrant data that is collected by registrars also impacts peoples' privacy. The real and potential exposure of this data, which can include identifiable information such as locations and real names, can have a disproportionate chilling effect on marginalised and vulnerable people, who may choose not to register websites altogether out of a fear of being identified. Additionally, registries and registrars can employ people, procure goods and services, manage offices, and run internal operations (e.g. travel) in ways that can affect people and communities.

Corporate responsibility and human rights due diligence

The concept of due diligence in relation to human rights, specifically, was first formally recognised when the UN Human Rights Council unanimously endorsed the UNGPs in 2011. The UNGPs are the first set of international standards for businesses regarding human rights and is an instrument to address the 'Protect, Respect, Remedy' framework. This framework sets out three pillars of responsibilities: the duty of states to protect human rights; corporate responsibility to respect human rights; and access to remedy when human rights abuses occur. While the UNGPs are a set of voluntary international standards, they have been increasingly normalised in the ICT sector over the past decade, as demonstrated by their adoption by several prominent international Internet and telecommunications companies, for example Facebook's reference to the UNGPs

regarding its work in Asia, Google's high-level commitment to the UNGPs, and Telenor's use of the UNGP framework in its human rights policy.

Human rights due diligence is an ongoing risk-management process to identify, prevent, and mitigate negative human rights impacts in the context of a company's products, services, operations, supply chains, and business partners. This process comprises several components: identifying risk points and relevant human rights; assessing actual and potential human rights impacts; integrating and acting upon the findings; tracking responses; and communicating how identified issues are addressed and to what extent the measures have been successful. Within these broad guidelines, each company can devise methodologies and procedures tailored to their size, operations, regulatory environment, and decision-making processes. Compliance with the UNGPs requires that companies fully carry out each component of the human rights due diligence process.

A particularly critical component of human rights due diligence is assessing human rights impacts. While human rights due diligence in relation to a company's activities and operations should be carried out on an ongoing basis, more detailed assessments of human rights impacts, or HRIAs, should be triggered when new risks arise, such as when a company enters or exits a new market or partnership, launches a new product or service, or significantly changes the functionality of an existing product.[2] Critically, HRIAs should draw on internal and/or independent external human rights expertise and involve meaningful consultation with potentially affected groups and other relevant stakeholders, as appropriate to the size of the business and nature of the operations. As any other business entity, Internet infrastructure providers must also respect human rights and exercise human rights due diligence.

Human rights due diligence of Internet registries and registrars in context

Over the course of this three-year pilot project, several external factors contributed to increased human rights awareness across the Internet infrastructure sub-sector and influenced the recommendations to SIDN, Blacknight, and PIR, as well as the general recommendations we issue in this outcome report. These developments largely related to the increasing importance of data protection and technical DNS security standards, the increasing implications of DNS-level policies and practices on the moderation of online content, and the increasing awareness of human rights due diligence in the Internet Corporation for Assigned Names and Numbers (ICANN).

Registrant data protection and security

During the pilot project, the 2018 EU General Data Protection Regulation (GDPR) entered into force, regulating all companies' handling of the personal data of EU citizens and residents, regardless of the companies' locations. Since then, the GDPR has galvanised Internet registries and registrars, ISPs, and other infrastructure providers, both inside and outside Europe, to implement data minimisation and security practices, retention limits, and other measures to protect peoples' privacy.[3] Data protection is critically relevant to registries and registrars as their core operations include the collection of registrants' information, correlated with the domain names they register. Registrant data can, and often does, include highly identifiable information that would be subject to the data protection requirements set out in the GDPR, including real names and addresses.[4] To comply with the GDPR, registries and registrars must now apply data minimisation principles to limit the personal data that is collected from applicants and registrants, while redacting personal data from being accessed through WHOIS, the public database of domain name registrations. Before the implementation of the GDPR, registrants' personal data would be fully accessible to the public through WHOIS.

The data of registrants and other users held by companies can be subject to requests for access from law enforcement and other government authorities. To be lawful, these

requests must comply with international standards on privacy and should be subject to strong procedural safeguards. By proactively disclosing information related to government requests received, as well as the responses to these requests, companies facilitate greater public scrutiny which can provide a check against requests that are unlawful or undermine due process. Transparency reporting of government requests for user data has continuously improved in the ICT sector over the last decade, and this adoption trend has increasingly included major Internet infrastructure providers. For example, in 2019, Cloudflare expanded its existing transparency reporting to include 'warrant canaries'. Warrant canaries are used as a workaround to government secrecy: in transparency reports, they signal to a company's users that the company has been served with a government request but has been prohibited from revealing the contents or existence of the request.

The security of the DNS is also a critical factor that determines how well peoples' data is protected. Given the function of the DNS as the global directory for Internet resources, the data that flows through this system can indicate a person's web history or a website's audience to attackers or eavesdroppers who are watching this traffic. Despite this threat, users' domain name information has historically remained visible, despite more and more Internet traffic being encrypted. In response, participants in technical communities such as the Internet Engineering Task Force have focused efforts to develop and strengthen technical security protocols that can be implemented by Internet infrastructure providers across the DNS. Protocols such as DNS-based Authentication of Named Entities (DANE) and Domain Name System Security Extensions (DNSSEC) authenticate and encrypt communication channels, while DNS over HTTPS (DoH) encrypts DNS query data. Since the start of the project, Internet infrastructure companies have made some efforts to adopt these security protocols. For example, Microsoft has begun implementation and rollout of DANE and DNSSEC, while DNS service providers such as Internet Systems Consortium have already introduced support for DoH in their products.

Content moderation at the infrastructural level

In recent years, Internet infrastructure providers increasingly moved to stop providing services to specific websites based on objections to the content they host. For example, Cloudflare decided to ban several clients that had relied on its security and performance optimisation products, including the Daily Stormer in 2017 and 8Chan in 2019. Domain hosting companies Google and GoDaddy also refused to provide services to the Daily Stormer in 2017. Although Internet infrastructure providers are not social media companies, decisions such as these have major implications for freedom of expression and access to information online. Given the concentration of this sub-sector, the decision of just a few key service providers can mean that certain websites no longer have access to the infrastructure required to operate as part of the World Wide Web, effectively censoring them completely. This decision-making power demonstrates that Internet infrastructure providers are not neutral, and the processes by which these decisions are made should be clear and transparent, consistently applied, and subject to strong procedural safeguards.

Since 2017, the power of Internet infrastructure providers over the availability of online content has only grown: in recent years, 'DNS abuse' has become a particular focus within the sub-sector.[5] While the term 'DNS abuse' has been used to identify behaviours where domain names are used by malicious actors to spread malware, launch botnets, and carry out attacks, the vague and overbroad term has also been linked to content-related issues, such as trademark infringement. Internet registries are required to take action against 'DNS abuse' as part of their operator agreements. However, as content moderators, registries have very few options: if they decide to censor content, their only course of action is to completely take down the domain name of the website hosting the content, effectively removing the website from the World Wide Web. In registries' overzealous efforts to remain compliant with their contracts, this stipulation may lead to the takedown of websites hosting content that is actually lawful under international freedom of expression standards, without clear guidelines or safeguards for appeal.

Human rights due diligence in the ICANN

The ICANN is a global non-profit organisation that is responsible for coordinating the operation and management of the DNS. Its key functions include the delegation of TLDs and overseeing the distribution of unique Internet resource identifiers, including domain names. Much like the Internet registries and registrars that it accredits and contracts, ICANN's decision-making power over the DNS has strong implications for freedom of expression, privacy, and other human rights. In recent years, ICANN has increasingly recognised its responsibility to human rights: in 2018, the organisation commissioned an internal HRIA of its daily operations. The recommendations that resulted from the assessment included improvements to workplace practices and enhancements to its existing grievance mechanism. Although ICANN has not yet fully addressed the recommendations of the HRIA, it is an important step towards normalising the use of the HRIA model among Internet registries and registrars and legitimising the relevance of human rights due diligence more broadly in DNS operations.

While the examples in this section constitute important developments across the Internet infrastructure sub-sector, there is still significant room for improvement. Actions such as detailed reporting of content takedown requests or the establishment of complaint and appeals mechanisms are crucial steps towards fully meeting the corporate responsibility to uphold human rights due diligence, but they are not yet normalised at the infrastructure level. Although the Internet infrastructure providers that are consistently making improvements include sector leaders such as PIR and Cloudflare, this contingent nevertheless constitutes a relatively small part of the overall sector, and one that is based in North America and Europe. It is clear that there is still a need to normalise and operationalise the full realisation of human rights due diligence among Internet infrastructure providers.

Common human rights risks and challenges for Internet infrastructure providers

While the test cases we conducted under this pilot project focused on Internet registries and registrars, the three partner companies we worked with differ from each other in terms of their mandates, sizes, and jurisdictions. SIDN and Blacknight, both EU-based companies, manage national domains that only individuals and companies within their national jurisdictions can use. PIR, on the other hand, is a US-based company that manages domains that are global and can be used by individuals or entities around the world. While SIDN and PIR provide registry services, Blacknight operates as a registrar. Across these differences, we were able to clearly identify commonalities in the risks and challenges that these and similar companies face. These observations are not exclusive to the operations of Internet registries and registrars and are applicable to all types of Internet infrastructure providers including ISPs, IXPs, and CDNs.

We have presented the common human rights risks and challenges below in accordance with the approach of our risk assessment tool, which focuses on the various roles that an Internet infrastructure provider holds: an **employer**, a **procurer of goods and services**, a **member of a broader community** and a **provider of services**. Additionally, the tool included **cross-cutting human rights due diligence** considerations that transect these roles.

Internet infrastructure provider as an employer

Anti-harassment

ARTICLE 19 and DIHR identified a general need for further capacity-building for management personnel in relation to the working environment, particularly to address harassment. These include, but are not limited to, good hiring practices, employee complaint mechanisms, and diversity and inclusion commitments.

Employee privacy

In multiple cases, we noted staff policies that potentially conflict with employees' right to privacy, on issues such as access to employees' data. While there are many legitimate grounds for employers to be able to access employee data, these interests must be adequately balanced against the employees' right to privacy.

Grievance mechanisms

Various types of grievance mechanisms were identified, such as whistleblower systems. However, often these were not developed to address human rights issues as such, but rather certain issues (e.g. potentially corrupt practices or unethical behaviour). Mechanisms to deal with employees' human rights concerns were generally lacking or not clear enough for employees to be able to access and use them.

Internet infrastructure provider as a procurer of goods and services

Responsibility of third parties

There was limited engagement on human rights considerations between the partner companies and vendors, suppliers, and other business partners. This includes both policy commitments as well as more direct engagement, such as contracting and other procurement-related activities.

Internet infrastructure provider as part of a broader community

Environmental impact

Impacts due to the physical footprint of registries and registrars were limited. However, regular international travel to global events such as ICANN were identified as a particular challenge. Some of the pilot companies have started developing climate and travel policies to further clarify their positions on reducing their contributions to climate change.

Internet infrastructure provider as a provider of services

Registry/registrar agreements

Considering the rights of registrants and other individuals potentially impacted by domain name-related activities, we noted the lack of human rights standards in operator agreements that registries and registrars make with ICANN.

Notice-and-takedown procedures

While there were policies and processes in place to govern decisions related to domain name takedowns and suspensions (e.g. anti-abuse policies), they were not developed in relation to human rights principles and do not take into account the implications of takedowns and suspensions on freedom of expression and access to information, freedom of association, and other rights. In general, there has been insufficient attention to freedom of expression, especially in the process of disabling domain names, where it must necessarily be balanced with other human rights.

Transparency

Registries and registrars can improve the transparency of domain names that have been suspended or disabled by publishing annual transparency reports, providing information such as how many domain names a registry or registrar has disabled over the reporting period, the reasons for these decisions, the number of appeals processes and outcomes, the number and sources of external takedown requests, etc. In general, there is insufficient reporting about processes that may have an impact on human rights.

Discriminatory price-setting

A challenge that remains difficult to address is the fees incurred by registrants to register domain names, particularly for registries that are further removed from the issue than registrars.

Registrant privacy

There is also a need to increase the focus on the protection of registrants' privacy, particularly in the context of personal data publication via WHOIS.

Cross-cutting due diligence considerations

Human rights commitments

At a high level, we identified that there was a general lack of human rights policies or explicit commitments to human rights and international human rights standards.

Human rights awareness

Staff should be informed about human rights standards relevant to them. This was not always the case. Where trainings and other resources were available, they principally concerned specific human rights issues (e.g. children's rights in relation to child sexual abuse materials).

Stakeholder engagement

There was limited engagement with affected stakeholders, particularly rights-holders or their proxies, in the assessment of products, services, and policies. We found that engagement with external stakeholders was heavily reliant on personal connections, implying a lack of institutional knowledge and potential issues in case of employee turnover.

The way forward

Outcomes of the pilot project

Following the completion of their roles in the pilot project, SIDN, Blacknight, and PIR all demonstrated an increased focus on human rights through various actions. Notably, all three partner companies updated their policies in line with international human rights standards, implemented improvements to their transparency reporting procedures, and engaged with new stakeholders and forums.

SIDN has since increased its transparency and engagement with its affiliated registrars through an annual meeting, called SIDN Connect. It updated its terms and conditions to bring it in compliance with human rights standards. It has also improved its statistical reporting of dispute resolutions for notice-and-takedown requests of .nl domain names, voluntarily appointed a data protection officer, and entered into several new partnerships with institutions including Privacy by Design, a foundation that creates and maintains free and open-source software. SIDN also set up SIDN Academy as a vehicle to share knowledge, including of security and privacy standards, with their registrars and set up a Legal Help Desk for registrars.[6]

Blacknight has since significantly changed its policies to comply with the GDPR through liberalisation of domain name registration rules and new arrangements for document and data retention, and drafted a new alternative dispute resolution policy and law enforcement guidelines to increase privacy protections for registrant data.[7] It also increased its transparency reporting to include sections on formal litigation, requests from law enforcement, requests from Irish consumer protection agencies, and the number of requests for non-public WHOIS information.

PIR has since committed to incorporate an explicit commitment to international human rights in its existing policies, a new appeals mechanism for registrants of PIR-managed domain names, and a new standards of behaviour document for third-party vendors.[8]
One of the major outcomes of the project is that the three partner companies have become ambassadors for strong human rights due diligence, contributing to a ‘multiplier effect’ that

can galvanise change not just at the company level, but sector-wide. SIDN, Blacknight, and PIR have publicly discussed their positive experiences of conducting human rights due diligence in a variety of forums, including RIPE NCC, the regional Internet registry for Europe, the Middle East, and Central Asia,[9] the global Internet Governance Forum,[10] the Internet Engineering Task Force, and ICANN. Following these discussions, surveyed participants recognised the use of HRIAs as a way to bridge the gap between Internet technical communities and the business and human rights field, including subject matter experts such as those working on children's, cultural, or lesbian, gay, bisexual, transgender, queer, and intersex (LGBTQI) rights. To normalise the consideration of human rights at the infrastructural level, it must be championed within the sector by companies that can demonstrate the feasibility and incentives of conducting due diligence activities.

Concluding observations and considerations

It is not a simple task to identify the negative human rights impacts of Internet infrastructure providers. While the assessment of certain activities can be straightforward, such as assessing providers' impacts as employers, the virtual footprint related to their core activities may make the overall assessment difficult. Further complicating the issue is that, due to the concentrated nature of this sub-sector, a small entity can potentially impact a disproportionately high number of rights-holders globally.

The assessments conducted through this project identified gaps in companies' responsibilities in relation to human rights; however, they do not constitute full HRIAs. In tandem with internal assessments of potential human rights impacts, like those we conducted with the three partner companies, it is essential to engage in consultations with rights-holders, those affected both directly and indirectly, in meaningful ways. These engagements are important to holistically determine the company's human rights impacts. Moving forward, Internet infrastructure providers, including the three partner companies, should use the tools and outcomes from this pilot project to conduct full HRIAs.

As this project focused on Internet registries and registrars based in the EU and United States, it has become clear that merely following national laws can, in certain contexts, prove to be effective for engendering respect for human rights. Even in jurisdictions where there are strong systems of governance and rule of law, there are nonetheless several accountability gaps at play. For example, our engagement with PIR led to recommendations to bring its policies and practices in compliance with strong data protection standards such as the GDPR, given the lack of a federal data protection regulation in the United States. In contexts where human rights issues are not sufficiently addressed in national laws, HRIA and gap analyses can be even more valuable tools for uncovering these gaps, especially when dealing with the relatively unique impacts associated with the provision of services among Internet infrastructure providers.

While all three partner companies are based in the Global North, the use of HRIAs among companies in the ICT sector in the Global South, such as MTN South Africa, is growing. Moving forward, we recognise the importance of working with companies based in the Global South—in full partnership with local civil society organisations—as part of supporting a truly global uptake of strong human rights due diligence.

In addition to the actions that individual companies can take, the outcomes of this project suggest that human rights issues at the infrastructural level are systemic and therefore require multi-stakeholder approaches. Issues such as content moderation are complex and should not be carried out unilaterally without transparency, expert consultation, or the opportunity for affected parties to appeal decisions. As such, it is important that governing organisations such as ICANN are engaged in discussions on human rights, so that sector-wide human rights standards are developed, communicated, and implemented. As the partner companies have shown, early adopters in the sector can be effective champions for building commitments in these spaces.

Initial recommendations for Internet infrastructure providers

Drawing from the outcomes, observations, and lessons learned from this pilot project, we have identified a core set of initial recommendations for registries, registrars, and other

Internet infrastructure providers to begin meeting their responsibility to respect human rights:

- Develop stand-alone human rights policies and/or include explicit commitments to human rights and international human rights standards in existing policies (e.g. codes of conduct, employee handbooks etc).

- Engage in a full HRIA to assess the provider's most salient human rights issues, considering all types of activities.

- Explicitly include human rights considerations in existing due diligence systems (e.g. regarding privacy, anti-corruption etc).

- Include human rights standards in supplier codes of conducts (or similar), conduct supplier risk identification based on human rights, include human rights expectations in contracts with both suppliers and business partners, and monitor suppliers' and business partners' adherence to such requirements.

- Conduct external stakeholder engagement, with rights-holder groups in particular, in the assessment of impacts of products, services, and policies, and ensure that the engagement is structured and not overly dependent on the contacts and networks of specific staff members.

- Build the general capacity through regular trainings and workshops for staff on understanding human rights framework and assessing and addressing human rights issues in their respective roles. This can include using annual trainings and regular webinars and workshops.

- Make existing grievance mechanisms (e.g. whistleblower protections) available for human rights-related concerns, or set up new grievance mechanisms tailored for that purpose.

- Publish detailed transparency reports as a standard practice to know and show that the company respects human rights.[11]

These recommendations are designed to serve as a starting point for further investigation and do not constitute a comprehensive checklist. While it is not an easy task, companies must consider *all* of their impacts on human rights. One opportunity to support this responsibility is to conduct human rights risk assessment workshops with external and/or internal human rights experts, as we conducted in this project. By fostering a broad approach, it is possible to comprehensively assess companies' involvement in negative impacts within their respective value chains, dismissing certain potential negative impacts as 'not applicable' while ensuring that adequate responsibility is taken for others.

We conclude this pilot project with the hope that it will mark the start of a wider, structural shift, in which all Internet infrastructure providers and the wider ICT sector understand their responsibility and take decisive steps to ensure that they continuously respect human rights.

Endnotes

[1] See 'Sure, we respect human rights! Don't we?', SIDN, 2018; 'Talking human rights and business at the UN', Blacknight, 2018; and 'Assessing human rights impacts at Public Interest Registry', PIR, 2020.

[2] For more on HRIAs in the ICT sector, see DIHR's *Guidance on Human Rights Impact Assessment of Digital Activities*, November 2020.

[3] See, e.g., 'Domain name enforcement in a post-GDPR era', CSC Global, 2017.

[4] For more information, see Kathryn Elliot, 'The who, what, where, when, and why of WHOIS: Privacy and accuracy concerns of the WHOIS database', *Science and Technology Law Review*, 2009.

[5] PIR and Blacknight, among other leading registries, are leading the conversation on DNS abuse. See, e.g., Jon Nevett, 'Doing our part for a safer, stronger DNS', CircleID, 2019.

[6] See SIDN's *Annual Reports* 2017–2019.

[7] See Blacknight's Legal page and Policies page.

[8] See 'Assessing human rights impacts at Public Interest Registry', PIR, 2020.

[9] See 'RIPE 78: Human rights, women in tech, and more', Blacknight, 2019.

[10] See, e.g., the session hosted by ARTICLE 19: *A Multistakeholder Approach to HRIAs: Lessons from ICANN*, Internet Governance Forum 2018.

[11] See, e.g., *Transparency Report*, SIDN, 2020.