APC ISSUE PAPERS

BUSINESS AND DIGITAL RIGHTS: TAKING STOCK OF THE UN GUIDING PRINCIPLES FOR BUSINESS AND HUMAN RIGHTS IN THE ICT SECTOR

By David Sullivan

INTRODUCTION

In the five years since the UN Human Rights Council adopted the Guiding Principles on Business and Human Rights (hereafter the Guiding Principles), human rights scrutiny of information and communication (ICT) companies has escalated significantly.[1] More governments than ever are pressuring companies to censor content, network shutdowns have become disturbingly routine in many countries, and Edward Snowden's revelations have undermined the credibility of Western governments and companies associated with the "internet freedom agenda."[2]

Just as significantly, companies' own commercial interests and business models have major human rights implications. In his first report, UN Special Rapporteur on the right to privacy Joseph Cannataci warns, "The data

1 United Nations. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework.* www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

2 Fontaine, R. (2014). *Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in a Post-Snowden Era.* Center for a New American Security: Washington, DC. www.cnas.org/internetfreedom#.V1ng5pMrJsM

David Sullivan is a consultant working at the intersection of technology and human rights. He previously served as the first policy and communications director at the Global Network Initiative, and continues to work as a consultant for GNI. The views expressed in this paper are those of its author.

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

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."[3] Company repositories of personal data provide a tempting target for state and non-state actors alike, from intelligence agencies to criminals. And company actions affect a wide set of rights beyond freedom of expression and privacy. Nominally well-intentioned initiatives to increase access to the internet, particularly through zero rating of selected content, have been widely criticised by global civil society for failing to safeguard user rights.[4] Decisions that companies make about what content and behaviour does or does not violate their own terms of services have huge ramifications on individuals' rights to assembly and association online. And although some companies are beginning to take new steps to respond to technology-related violence, especially against women, on their products, services and platforms, few explicitly consider this to be a human rights obligation.[5] For companies, loss of trust is an existential threat to business models. A recent survey covering 24 countries found only 30% of global citizens think governments are doing enough to keep personal information secure and safe from private companies, and a majority are more concerned about their online privacy than they were a year ago.[6] Although some companies have responded to human rights risks through participation in multistakeholder accountability initiatives, or by increasing transparency reporting about government requests and lobbying to reform government surveillance, many companies in the ICT sector have taken little in the way of action to commit to respect human rights according to the Guiding Principles, or recognise their full range of impacts, negative and positive, on all human rights.[7] Against this backdrop, the debate on whether the Guiding Principles provide adequate corporate accountability for human rights abuses continues. In 2014, Ecuador and South Africa put forward a Human Rights Council resolution to establish an intergovernmental working group formed to discuss the creation of a legally binding treaty to regulate transnational companies under human rights law, which met for the first time in 2015.[8] When weighing how to work with governments to hold companies accountable while also collaborating with companies to press against government overreach, civil society organisations must consider whether a global treaty process will contribute to or detract from other efforts to protect and respect the rights of users who face more threats from more governments and companies than ever around the world.

This issue paper takes stock of the implementation of the Guiding Principles in the ICT sector, using their three pillars to explore key issues, implementation gaps, and emerging best practices for technology companies. These are:

- The state responsibility to protect human rights
- The corporate responsibility to respect rights
- The need for access to effective remedy when rights have been violated.

A complete analysis of the impact of ICT companies on all human rights is beyond the scope of this paper, which focuses on some of the most salient rights impacted by companies, looking at both civil and political rights as well as economic, social and cultural rights. With its transformative potential to help advance human rights, the ICT sector should be driving global discussion about how best to achieve respect for human rights in the private sector. By taking stock of progress made thus far and implementation gaps, this report concludes with recommendations intended to provide a roadmap to move ICT sector risks and opportunities to the centre of the business and human rights debate.

3 Canattaci, J. (2016). Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

4 Open Letter to Mark Zuckerberg Regarding Internet.org, Net Neutrality, Privacy, and Security, 18 May 2015. https://www.facebook.com/notes/accessnoworg/open-letter-to-mark-zuckerberg-regarding-internetorg-net-neutrality-privacy-and-/935857379791271

5 Buni, C., & Chemaly, S. (2016, 13 April). The Secret Rules of the Internet. *The Verge*. theverge.com/2016/4/13/11387934/internet-moderator-history-youtube-facebook-reddit-censorship-free-speech

6 2016 CIGI-Ipsos Global Survey on Internet Security and Trust. https://www.cigionline.org/internet-survey-2016

7 Ranking Digital Rights. (2015). *2015 Corporate Accountability Index*. Washington DC: New America Foundation. https://rankingdigitalrights.org/index2015

8 A/HRC/RES/26/9, Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights. Resolution adopted by the Human Rights Council, 14 July 2014.

CONTEXT

FIVE YEARS SINCE RUGGIE

In June 2011, the Human Rights Council unanimously endorsed the Guiding Principles, the capstone of six years of work by the UN Secretary-General's Special Representative (SRSG) for Business and Human Rights John Ruggie. Anchored in the "Protect, Respect, and Remedy" framework, the Guiding Principles established a widely accepted vocabulary for understanding the respective human rights roles and responsibilities of governments and the private sector. In particular, they were viewed as a positive alternative to deadlock over previous UN efforts to regulate transnational corporations' human rights through a code of conduct that was widely criticised by the business community. Although not universally accepted, with many civil society organisations arguing the Guiding Principles were insufficient to ensure company conduct,[9] their uptake by an increasing number of companies in a variety of sectors has driven an evolving business and human rights debate.

ICT company responsibilities were not the focus of most scrutiny during the creation of the Guiding Principles. Aside from supply chain conditions for workers in hardware factories and in the sourcing of raw materials, the human rights risks for internet companies were usually considered narrowly in the context of censorship and surveillance occurring mostly in restrictive environments, particularly China.

Wider consideration of the relationship between ICT companies and human rights exploded during the Arab Spring revolutions, the Occupy movement, and with the growing ubiquity of social media and ICT tools in global activism. At that time, social media companies were widely hailed as heroic enablers of democratic activism, even while telecommunications companies were criticised for acceding to government demands to shut down networks such as during the Tahrir Square protests in Egypt, and the role of niche companies providing surveillance technology to governments with troublesome human rights records was revealed through forensic analysis by technologists and human rights groups.

At the same time, the issue of human rights online became strongly associated with the "internet freedom agenda" of the United States and like-minded allies in ways that raised concerns from many long-time digital rights advocates.[10] The moral authority of these mostly Western governments and companies has been severely undercut since Edward Snowden revealed the scope and extent of state surveillance, including surveillance undertaken by and through ICT companies.

Today, the conversation has shifted dramatically. Social media companies are accused of serving as "command-and-control networks of choice for terrorists and criminals,"[11] by some governments, as well as of neglecting the occurrence of widespread harassment and technology-related violence on their platforms, particularly against women. Through real-name requirements, account deactivation and content removal, companies exercise control over not just expression, but also association, assembly, access to information, participation in culture, and rights to work and education on a scale above and beyond that of many governments. The rise of "sharing economy" apps such as Uber and Airbnb has raised serious questions about their approach to labour rights. More generally, civil society organisations and data protection authorities have raised questions about whether algorithms and other data processing can lead to discrimination at scale.[12]

9 Human Rights Watch. (2011, 16 June). UN Human Rights Council: Weak Stance on Business Standards. https://www.hrw.org/news/2011/06/16/un-human-rights-council-weak-stance-business-standards

10 Ben Gharbia, S. (2010, 17 September). The Internet Freedom Fallacy and the Arab Digital Activism. *Nawaat*. https://nawaat.org/portail/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism/

11 Hannigan, R. (2014, 3 November). The web is a terrorist's command-and-control network of choice. *Financial Times*. https://next.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0

12 UNESCO. (2015, 4 April). Privacy expert argues 'algorithmic transparency' is crucial for online freedoms at UNESCO knowledge cafe. www.unesco.org/new/en/media-services/single-view/news/privacy_expert_argues_algorithmic_transparency_is_crucial_for_online_freedoms_at_unesco_knowledge_cafe/#.VzNUtRUrJsM. Also see NYU Law School conference Tyranny of the Algorithm? Predictive Analytics and Human Rights. www.law.nyu.edu/bernstein-institute/conference-2016

HUMAN RIGHTS AND ICT COMPANIES

The ICT sector consists of a wide variety of companies operating in different segments of the sector, from telecommunications providers to web- or cloud-based services and platforms, software, and hardware and equipment manufacturers.[13] ICT companies are most commonly associated with the rights to freedom of expression and privacy, with initiatives such as the Global Network Initiative[14] focused on protecting and advancing those rights in the sector. But their operations have implications for a much wider set of rights. The Human Rights Council has endorsed a broad approach to human rights and the internet through a series of resolutions affirming "the same rights that people have offline must also be protected online," as well as through resolutions on the right to privacy in the digital age.[15]

Recognition of the link between ICTs and human rights builds upon an impressive body of norms and principles for human rights and the internet that has been developed through a variety of processes. These include initiatives that range from APC's Internet Rights Charter, the Internet Rights and Principles Dynamic Coalition of the UN Internet Governance Forum and the NETmundial outcome document to regional initiatives such as the African Declaration on Internet Rights and Freedoms to national-level initiatives such as Brazil's Marco Civil Internet Bill of Rights and Italy's Declaration of Internet Rights.

The threat to free expression arising from government censorship of online content continues, reinforced by increasingly widespread and sophisticated mechanisms of censorship, surveillance, and network shutdowns. But social media and ICT companies also impact other civil and political rights, such as the rights to assembly and association.[16] Technology-related violence against women, or acts of gender-based violence committed, abetted or aggravated by use of ICTs are a violation of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and "cause psychological and emotional harm, reinforce prejudice, damage reputation, cause economic loss and pose barriers to participation in public life, and may lead to sexual and other forms of physical violence."[17] Economic, social and cultural rights, such as the right to education, the right to work, and the right to take part in cultural life are just as significantly affected by ICTs as civil and political rights. These rights are often given insufficient attention in the wider business and human rights debate, and in the context of digital rights in particular. This is partly due to the incorrect view that the International Covenant on Economic, Social and Cultural Rights (ICESCR) is less important that the International Covenant on Civil and Political Rights (ICCPR), and partly because the complete fulfilment of these rights requires "progressive realisation" over a period of time. It also does not help that the US, a key jurisdiction for many ICT companies, has ratified neither the ICESCR nor CEDAW. Although states are obligated "to monitor and regulate the conduct of non-State actors to ensure they do not violate the equal right of men and women to enjoy economic, social and cultural rights," the corporate responsibility to respect human rights is often interpreted to imply a minimal duty on companies to help realise these rights.[18] In fact, the Guiding Principles clearly articulate that all human rights are universal, interdependent, and interrelated, and companies should account for their responsibilities to respect all these rights.

It should also be noted that although the human rights community has an understandable tendency to focus on the adverse impacts on rights that ICT companies cause or to which they contribute, technology companies do have undeniably positive impacts on human rights. In fact, many ICT companies go well beyond their responsibilities under the Guiding Principles to help promote and protect human rights either through innovations in their products and services, or through corporate social responsibility initiatives. The extent to which such activities are framed in explicit human rights terms, and

13 OECD. (2011). OECD Guide to Measuring the Information Society. www.oecd.org/internet/ieconomy/oecdguidetomeasuringtheinformationsociety2011.htm

14 https://globalnetworkinitiative.org

15 A/HRC/RES/20/8, The promotion, protection and enjoyment of human rights on the Internet. Resolution adopted by the Human Rights Council, 16 July 2012.

16 Comninos, A. (2012). *Freedom of peaceful assembly and freedom of association and the internet.* Association for Progressive Communications. https://www.apc.org/en/pubs/freedom-peaceful-assembly-and-freedom-association

17 APC Women's Rights Programme. (2015). *Technology-related violence against women: A briefing paper*. https://www.apc.org/en/system/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf

18 Nolan, J., & Taylor, L. (2009). Corporate Responsibility for Economic, Social and Cultural Rights: Rights in Search of Remedy? *Journal of Business Ethics, 87*(2); Lara, J.C. (2015). *Internet access and economic, social and cultural rights*. Association for Progressive Communications. https://www.apc.org/en/system/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29.pdf

whether or not they are captured in each company's human rights policy commitments and implementation of the Guiding Principles, varies greatly.

TREATY DISCUSSIONS

In parallel to the development of business and human rights in the ICT sector, the wider debate surrounding corporate accountability has accelerated in recent years, with the adequacy of the Guiding Principles called into question by some governments and wide sections of civil society. Although Ruggie was able to create a common vocabulary for understanding human rights responsibilities, the meaning and implications of that framework as applied in the real world remain highly contested. One only needs to look at the heated debate over the implementation of the Guiding Principles in the extractive sector, where some civil society organisations have argued that companies have effectively privatised human rights, to understand this context.[19] Legitimate concerns about the specific role of transnational corporations that are able to evade accountability for human rights violations by operating across jurisdictions have motivated recent movement to revive a global, legally binding treaty for such companies. But even some human rights organisations that have been highly critical of the Guiding Principles have warned against a treaty that creates an uneven situation for transnational and national companies. Ruggie himself has cautioned, "No future treaty, real or imagined, can substitute for the need to achieve further progress in the here and now," while also warning that efforts by industry to obstruct any further "international legalization" in business and human rights is also counterproductive.[20]

The first session of the open-ended working group took place in July 2015, and concerns about the exclusive focus on transnational corporations were reflected in the meeting, where the European Union unsuccessfully proposed modifying the programme of work to include reference to human rights abuses at the domestic level.[21] Following a second session in October 2016, the working group is tasked with preparing elements of a draft legally binding treaty.

Renewed debate about a treaty has largely proceeded independent of discussions about the ICT sector and its specific human rights risks. The focus on transnational corporations in the context of treaty talks arises from governance gaps that have arguably allowed transnational companies to operate in a rights-free zone. These are salient concerns for the ICT sector, which is as sophisticated as any in its approach to tax avoidance and the use of subsidiaries.

Although ICT companies are as culpable as those in other industries of shifting jurisdictions to avoid taxes (among other issues), they also interpret governments' jurisdiction on behalf of human rights. At the same time, transnational operations, when configured responsibly, can be a key tool to help companies respect rights. The GNI implementation guidelines, for example, call for companies to "interpret the governmental authority's jurisdiction so as to minimize the negative effect on freedom of expression" and "narrowly interpret the government authority's jurisdiction to access personal information, such as limiting compliance to users within that country." Yahoo put this approach into practice when it expanded its Vietnamese language services in 2009. Following a human rights impact assessment, the company noted that it had "decided to manage and operate our Vietnamese language services out of Singapore so the services would be governed by laws with stronger protections than those in Vietnam."[22]

PERCEPTIONS OF CORPORATE ACCOUNTABILITY IN THE TECH SECTOR

There is a strong libertarian impulse throughout large portions of the tech industry that views government as a source of problems and very rarely as a solution when it

19 Rights and Accountability in Development. (2016). *Principles without justice: The corporate takeover of human rights*. www.raid-uk.org/sites/default/files/principles_without_justice.pdf

20 Ruggie, J. (2014). The Past as Prologue? A Moment of Truth for UN Business and Human Rights Treaty. https://www.hks.harvard.edu/m-rcbg/CSRI/Treaty_Final.pdf

21 A/HRC/31/50, Report of the first session of the open-ended intergovernmental working group on transnational corporations and other business enterprises with respect to human rights, with the mandate of elaborating an internationally legally binding instrument, 5 February 2016.

22 https://yahoobhrp.tumblr.com/tagged/our-initiatives

comes to social and economic policy.[23] Within this mindset, all that is required of socially responsible companies is to resist government overreach through technological and legal measures. It is informed by the vision of ICTs as liberation technology and a maximalist approach to free expression rooted in the US first amendment, and reflected in reflexive opposition to government involvement in internet governance. The same mindset tends to downplay the high degree of state involvement in ICT sector research and development, including the creation of the internet, as well as the close working relationships between state law enforcement and security agencies and ICT firms, many of which are or were partially or fully state owned, and the revolving door for senior executives between technology firms and government.[24] Even more problematically, the ICT sector is dominated by privilege: it is overwhelmingly male and deeply deficient in diversity. A GSM Association-commissioned study of gender diversity found that in three-quarters of telecommunications companies surveyed, women accounted for less than 40% of the workforce, with far worse gender gaps in senior positions.[25] Tech company policies and products reflect this bias, with negative consequences for users around the world.

For human rights, governments are not always the problem and nearly always form a key part of the solution. Voluntary action by companies to implement the Guiding Principles, from due diligence to grievance mechanisms, can and does contribute to improved human rights outcomes for billions of internet and ICT users, but is no substitute for legislation and regulation that impose mandatory requirements upon companies to respect rights.

23 Barlow, J. (1996, 8 February). A Declaration of the Independence of Cyberspace. https://www.eff.org/cyberspace-independence

24 Although the "revolving door" between technology companies such as Google and the U.S. government is a frequently cited example, this happens around the world. For example, former European Commissioner for the Digital Agenda Neelie Kroes recently joined the board of directors of Salesforce and the public policy advisory board of Uber.

25 www.gsma.com/newsroom/press-release/gender-diversity-in-the-telecommunications-sector

THE STATE RESPONSIBILITY TO PROTECT RIGHTS IN THE DIGITAL AGE

The state duty to protect against human rights abuses by business enterprises is a fundamental pillar of the Guiding Principles. This section explores progress on implementation of that responsibility in the ICT sector, identifying key issues, gaps, and emerging best practices.

KEY ISSUES FOR THE ICT SECTOR

In the ICT sector, the state responsibility pillar rests on a shaky foundation, because the Guiding Principles focus more on the duty of states to take measures to protect against rights violations by companies, and do not provide detailed guidance on situations in which states make requests or demands of companies that may involve them in human rights abuses.[26] Although ICT companies have very significant influence on human rights independent of governments, it is the ability of states to compel action by companies that is the source of some of the most widespread and severe human rights violations facilitated by the ICT sector.

Whether in states with serious human rights deficiencies or those with well-developed rights-based legal frameworks, violations of the rights to privacy, free expression, and other human rights occur stemming from government laws, policies, and actions intended to protect national security, fight terrorism, or for law enforcement purposes.

Further complicating the landscape, the ways that laws or policies intended to address legitimate purposes interact with the interconnected nature of the internet reverberate in unintended or unforeseen ways.

Recent examples from around the world demonstrate this effect:

- Pakistan's Draft Protection of Electronic Crime Bill, approved by the national assembly in April 2016 and currently under consideration of the senate, has provisions that could arbitrarily restrict rights to freedom of expression, assembly, association and privacy.[27]
- The right to erasure, or the "right to be forgotten" that is now formalised in the European Union's new General Data Protection Regulation, has the potential to address legitimate privacy concerns but also risks suppressing freedom of expression and access to information.[28]
- US legislation aimed at stopping sexual exploitation of children results in consenting young adults convicted for child pornography, and is a barrier to access to sexual health information, disproportionately affecting economically disadvantaged youth.
- Bans on encryption, which have been proposed in the US and UK, and already exist in various forms in Russia, Morocco, Kazakhstan, Pakistan and Colombia, not only interfere with the right to privacy, they also pose serious cyber security threats that make everyone's data less secure, and particularly threaten the activities of human rights defenders and journalists.[29]
- Laws in India and elsewhere aimed at regulating the conduct of internet intermediaries have been found unconstitutional in their overly broad effect on freedom of expression.
- The multilateral regulatory effort to curb the export of surveillance technology to repressive governments through the Wassenaar Arrangement, which was championed by human rights organisations, has been criticised by some of the very same organisations for vague definitions and overly broad rules that suppress information security research.[30]

26 Brown, I., & Korff, D. (2012). *Digital freedoms in international law: practical steps to protect human rights online. Global Network Initiative.* https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

27 Bytes for All Pakistan. (2016, 15 April). Prevention of Electronic Crimes Bill 2016, yet another story of deception from democracy. https://content.bytesforall.pk/node/191

28 Keller, D. (2016, 27 January). The new, worse 'right to be forgotten'. *Politico*. www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy

29 Amnesty International. (2016). *Encryption: A matter of human rights*. www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

30 Cardozo, N., & Galperin, E. (2016, 29 February). Victory! State Department Will Try to Fix Wassenaar Arrangement. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2016/02/victory-state-department-will-try-fix-wassenaar-arrangement

INTERNATIONAL ACTION

At the international level, a number of state-based initiatives have addressed the role of business in human rights and ICTs. These include the Human Rights Council resolutions on the internet and human rights, which have been led by Sweden and a core group of states including the US, Tunisia, Turkey, Brazil and Nigeria. Following the Snowden revelations, Brazil and Germany championed two UN General Assembly resolutions on the right to privacy in the digital age, together with Austria, Lichtenstein, Mexico, Norway and Switzerland. Other intergovernmental organisation processes, such as the review of the World Summit on the Information Society (WSIS+10), have also touched upon key human rights issues impacted by ICTs without explicitly referencing the business and human rights responsibilities of technology companies.

Following the conclusion of the mandate of the SRSG for business and human rights in 2011, the Human Rights Council created a working group on the issue of human rights and transnational corporations and other business enterprises. At the time, critics warned that the working group, and the annual UN Forum on Business and Human Rights, lacked strong accountability mechanisms that would actually verify that companies respect rights, and contrasted it with the International Labour Organization treaty on domestic workers.[31] In 2013, the International Network for Economic, Social and Cultural Rights (ESCR-Net) claimed "the UN Working Group has shown a complete lack of leadership in addressing the root causes of corporate human rights violations."[32] In June 2014, the Human Rights Council extended the mandate of the working group for an additional three years. Although the working group has undertaken a number of important activities as part of its mandate, from country visits to collaborating with the Office of the High Commissioner for Human Rights on a report on improving access to remedy for victims of business-related human rights abuse, the group has also recently experienced significant turnover, with three resignations during the past year. With the commencement of treaty negotiations, the working group is under more pressure than ever. States that have supported the group and opposed a binding treaty on business and human rights should consider significantly enhancing the mandate of the working group when it expires in 2017.

EMERGING BEST PRACTICES

Despite the challenges of crafting laws and regulations on the internet, there are areas of innovation and creative approaches by states that can be built upon.

National Action Plans

The principal mechanism for articulating commitments and plans of action in response to the principles has been through national action plans (NAPs). The number of states publishing business and human rights NAPs has expanded rapidly in recent years, from the UK and the Netherlands in 2013, to eight published in 2015, with 25 more underway. In another six states, national human rights institutions and civil society organisations are undertaking "shadow" NAPs or other relevant work.[33] The process of creating and updating national action plans is as important as the plan itself. Government consultation processes can catalyse active participation by business interests. Civil society leadership, particularly through shadow NAPs and baseline assessments, can shape the agenda.

Few of the published NAPs address ICT sector issues in great detail. Sweden includes a paragraph on internet freedom in its report annex.[34] Finland proposed a roundtable on privacy and data collection with government, civil society, and ICT companies, but does not otherwise address ICT sector issues. Although six of the eight states that have published NAPs are members of the Freedom

31 Human Rights Watch. (2011). UN Human Rights Council: Weak Stance on Business Standards. https://www.hrw.org/news/2011/06/16/un-human-rights-council-weak-stance-business-standards

32 International Network for Economic, Social and Cultural Rights. (2013). Intervention at the CSO meeting prior to the UN Regional Forum on Business & Human Rights. business-humanrights.org/sites/default/files/media/documents/escr-net-statement-aug-2013.pdf

33 Business and Human Rights Resource Centre. business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-governments/by-type-of-initiative/national-action-plans

34 Government of Sweden. (2015). *Action Plan for Business and Human Rights.* www.government.se/information-material/2015/08/action-plan-for-business-and-human-rights/

Online Coalition (FOC), none incorporate their FOC membership into their NAP.[35]

The UK became the first government to release an update to its NAP in May 2016, which expands on some ICT sector issues, such as work through the Wassenaar Arrangement to combat the export of surveillance technology to governments engaged in human rights abuses, and the publication of guidance on cyber security export risks.[36] Expecting NAPs to incorporate sector-specific detail for every industry or sector of the economy would be unwieldy at best. But published NAPs do prioritise sectors of particular attention. Colombia, for example, identifies mining and energy, agribusiness and infrastructure.[37] The Netherlands features the agriculture and horticultural sectors, as well as the textile sector.[38] The lack of specific attention to ICTs – which through their increasing ubiquity have a huge impact on the realisation of rights across sectors – is conspicuous and reflects the siloing of business and human rights and technology policy within governments.

NAPs provide a means for articulating policy, a repository for guidance, and a process for consultation with stakeholders that will help ICT sector companies fulfil their own responsibilities. Stakeholders in the ICT sector should go out of their way to raise the profile of ICTs in future national action plans.

Reporting requirements

Non-financial reporting requirements provide a key means of ensuring that companies disclose information about how they are managing human rights risks. Europe has led the way by mandating that companies report non-financial information by 2017. Directive 2014/95/EU of the European Parliament and Council mandates that large companies "should prepare a non-financial statement containing information relating to at least environmental matters, social and employee-related matters, respect for human rights, anti-corruption and bribery matters," and points to the Guiding Principles as one of several frameworks reporting companies should rely upon.[39] Similar initiatives are gaining steam in other parts of the world. For example, the Singapore stock exchange has proposed requiring listed companies to review social, environmental and governance issues in annual sustainability reports.[40]

Diplomatic cooperation

Coalitions of governments, working through the Human Rights Council or through initiatives like the Freedom Online Coalition,[41] have achieved important victories, particularly widespread support for the resolution affirming "that the same rights that people have offline must also be protected online,"[42] shaping global norms that reflect a commitment to online rights. There is a continuing need for like-minded states to engage in international forums to prevent measures that would interfere with the responsibility of ICT companies to respect human rights.

GAPS

There are no shortage of gaps in state practice. In a collective submission to the report of the UN High Commissioner on Human Rights on the right to privacy in the digital age, NGOs, including APC, stressed, "we wish to state in the strongest terms that very few measures are being taken at national levels to ensure respect for and protection of the right to privacy."[43]

35 Government of Finland. (2014). *National Action Plan on Business and Human Rights.* www.tem.fi/files/41214/TEMjul_46_2014_web_EN_21102014.pdf

36 Good Business: Implementing the UN Guiding Principles on Business and Human Rights. Updated May 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/522805/Good_Business_Implementing_the_UN_Guiding_Principles_on_Business_and_Human_Rights_updated_May_2016.pdf

37 Columbia Avanza. Derechos Humanos y Empresa. Plan de Accion de Derechos Humanos y Empresas. www.ohchr.org/Documents/Issues/Business/NationalPlans/PNA_Colombia_9dic.pdf

38 business-humanrights.org/sites/default/files/documents/netherlands-national-action-plan.pdf

39 eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0095&from=EN

40 Han, W. W. (2016, 6 January). Sustainability reporting rules: SGX seeks views. *The Straits Times*. www.straitstimes.com/business/sustainability-reporting-rules-sgx-seeks-views

41 freedomonlinecoalition.com

42 A/HRC/RES/20/8, The promotion, protection and enjoyment of human rights on the Internet. Resolution adopted by the Human Rights Council, 16 July 2012.

43 www.ohchr.org/Documents/Issues/Privacy/PrivacyInternational.pdf

Freedom Online Coalition: Practising what is preached?

In the ICT sector, the principal government initiative focused on ICTs and digital rights is the Freedom Online Coalition (FOC), which has grown from 15 founding members to 29. But the coalition faces serious challenges in terms of legitimacy, lack of engagement, and questionable laws and legislative proposals. From a legitimacy perspective, the coalition conspicuously includes the "five eyes" governments, the signals intelligence alliance between the US, UK, Canada, New Zealand, and Australia.

Concern on the part of global civil society that the FOC was insufficiently focused on laws, policies, and regulations within member states helped spur the 2014 Tallinn Agenda, which together with the Founding Declaration and the Nairobi Terms of Reference forms the commitments to which members states are supposed to adhere. The Tallinn Agenda, in particular, commits member governments to "Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same."[44] In terms of engagement, the activities of the coalition to-date do suggest a need for greater government involvement. Multistakeholder working groups addressing cyber security, digital development and privacy and transparency now include geographically diverse participation by NGOs, academics and the private sector, but only very limited government participation and none by members from the "global South". Although the Privacy and Transparency Working Group has issued a report with recommendations on transparency for both governments and companies, it is not clear whether member governments will adopt its recommendations. More than half of the states in the coalition have neither hosted an FOC conference nor participated in one of the coalitions' working groups:

CHAIR/CONFERENCE HOST	GOVERNMENTS IN WORKING GROUPS	OTHERS
Netherlands	Netherlands (WG1)	Australia
Kenya	USA (WG1,WG2,WG3)	Austria
Tunisia	Canada (WG1)	Czech Republic
Estonia	Sweden (WG2, WG3)	Finland
Mongolia	Germany (WG2,WG3)	France
Costa Rica (2016)	Latvia (WG2)	Georgia
	Moldova (WG2)	Ghana
	UK (WG3)	Ireland
		Japan
		Lithuania
		The Maldives
		Mexico
		New Zealand
		Norway
		Poland
		Spain

Note: WG1 – An Internet Free and Secure, WG2 – Digital Development and Openness, WG3 – Privacy and Transparency Online. https://www.freedomonlinecoalition.com/how-we-work/working-groups

The coalition has recognised the need for self-reflection and commissioned a recently published independent evaluation of its activities.[45] The evaluation, based on interviews with FOC members and stakeholders, recommends that the coalition establish mechanisms through which stakeholders can raise concerns about member governments, and periodically review performance and commitments. A strategic review working group has been formed and tasked with reporting to the next meeting of the coalition in Costa Rica in October 2016.[46] Whether the coalition incorporates these recommendations into its operations will have a major impact on its future relevance.

---

44 www.freedomonline.ee/foc-recommendations

45 Center for Global Communication Studies. (2016). Clarifying Goals, Revitalizing Means: An Independent Evaluation of the Freedom Online Coalition. www.global.asc.upenn.edu/publications/clarifying-goals-revitalizing-means-an-independent-evaluation-of-the-freedom-online-coalition

46 Freedom Online Coalition. (2016). Freedom Online Coalition's Strategic Review Working Group Joint Statement on Independent Report by University of Pennsylvania. https://www.freedomonlinecoalition.com/wp-content/uploads/2016/05/06-05-FOC-Strategic-Review-WG-Joint-Statement-on-Independent-Report.pdf

Surveillance oversight and transparency

Until recently, the secrecy surrounding surveillance laws, policies, and their implementation made it very difficult for citizens to understand the extent of government and company collaboration as part of communications surveillance. Since the Snowden revelations, not only have the number of companies reporting on government requests for user data increased, but some telecommunications companies have begun to issue reports that summarise the surveillance laws they are subject to by jurisdiction, and to disclose which governments permit reporting. Vodafone issued the first such report in 2014, with other telecommunications companies following suit in recent years. These reports demonstrate the lack of transparency even by governments with stated commitments to online rights. In their most recent report Vodafone describes a continuing lack of clarity about whether it would be lawful to disclose statistics in Ghana.[47] In Ireland, despite extensive engagement with the government, Vodafone has been told they cannot disclose information about lawful interception. The legal position in Kenya continues to remain unclear as well.

Legislative backsliding

The recent legislative record of many governments that have made strong commitments to human rights online presents a serious cause for concern. Brazil has led international initiatives to rein in surveillance and revitalise multistakeholder engagement on internet governance, and its internet law, the Marco Civil, has been widely praised as pioneering for its protection of human rights online. But recent cyber crime legislative proposals have been widely criticised for provisions that would allow authorities to force intermediaries to remove allegedly illegal content without a court order.[48]

Legislation in FOC governments also reflects backsliding. Mobile network operator Telia Company (formerly TeliaSonera) has issued public statements expressing human rights concerns with proposed laws in Moldova and blocking of websites in Georgia.[49] France has widely expanded its surveillance powers since the 2015 terror attacks in Paris.[50] Despite the passage of the USA FREEDOM Act, the US has also passed controversial cyber security legislation that will enable greater sharing of data between government and companies with serious privacy implications.[51]

47 Vodafone. (2015). *Law Enforcement Disclosure Report 2015*. www.vodafone.com/content/index/about/sustainability/law_enforcement.html#

48 Ellerbeck, A. (2016, 21 April). Cybercrime proposals risk undermining Brazil's progress in securing free and open internet. *Committee to Protect Journalists*. https://cpj.org/blog/2016/04/cybercrime-proposals-risk-undermining-brazils-prog.php

49 www.teliacompany.com/en/newsroom/news/news/news-articles/2016/respecting-freedom-of-expression--telia-company-view-on-new-legislation-in-moldova and www.teliacompany.com/en/newsroom/news/news/news-articles/2016/freedom-of-expression--blocking-of-websites-in-georgia

50 Leghtas, I. (2015, 28 July). Dispatches: France – State Snooping is Now Legal. *Human Rights Watch*. https://www.hrw.org/news/2015/07/28/dispatches-france-state-snooping-now-legal

51 Brandom, R. (2015, 18 December). Congress passes controversial cybersecurity bill attached to omnibus budget. *The Verge*. www.theverge.com/2015/12/18/10582446/congress-passes-cisa-surveillance-cybersecurity

THE CORPORATE RESPONSIBILITY TO PROTECT: POLICIES AND PRACTICES

The corporate responsibility to respect human rights is not simply a "negative" obligation to avoid actively participating in human rights abuses. Instead, it is an operational framework of proactive responsibilities that helps companies assess, mitigate, and remediate human rights violations. Even Chris Albin-Lackey of Human Rights Watch, a vocal critic of the Guiding Principles, has acknowledged that "they bring us closer than we ever have been to a shared understanding of how businesses should think about at least some of their core human rights responsibilities."[52] This section surveys the state of play of ICT company implementation of the Guiding Principles, identifying how and where they have affected company behaviour.

KEY ISSUES FOR THE ICT SECTOR

The ICT sector ranges from tiny startups with only a handful of staff to vast multinational corporations with billions of users and offices strewn across the globe. It includes all aspects of the value chain and layers of infrastructure, devices, networks and applications that enable netizens to access the internet to conduct their digital lives. Telecommunications companies and mobile network operators are the primary providers of internet access across much of the globe. Equipment manufacturers, whether supplying telecom infrastructure or personal devices, are a key intermediary, as are web hosts and domain registrars and registries. The ICT sector includes not just companies but also multi-stakeholder processes and standard setting bodies. Increasingly, its issues pertain to other companies and industries, such as automotive and appliance industries as more vehicles and devices are connected to the internet.

Software and app developers, including companies like Airbnb and Uber, are building online platforms that drive offline behaviour with human rights implications, whether they are disrupting, avoiding or disregarding traditional regulations including labour protections. Such companies can quickly grow from early stage startups to multinational behemoths valued in the billions of dollars. The sooner such companies recognise that embracing human rights early can prevent serious violations, the better their chances of avoiding costly crises and brand damage down the road.

EMERGING BEST PRACTICES

There is a growing body of guidance for companies seeking to implement human rights policies in the ICT sector. This includes the GNI Principles and Guidelines, the Telecommunications Industry Dialogue, and the EU ICT Sector Guidance on implementing the United Nations Guiding Principles, all of which have been recommended as minimum standards by UN Special Rapporteur David Kaye.[53]

Human rights due diligence and impact assessments

Companies operationalise their policy commitments to the Guiding Principles through due diligence processes that "identify, prevent, mitigate, and account for how they address their human rights impacts."[54] ICT initiatives, from the GNI and Telecommunications Industry Dialogue Principles to the European Commission-sponsored sector guidance, have begun to offer specific steps on how to conduct due diligence, but details remain lacking. The actual conduct of due diligence, including human rights impact assessments, is often obscured by the imperatives of speed and secrecy that drive business decisions in the sector.

The GNI implementation guidelines specify that impact assessments should be undertaken when reviewing

52 Albin-Lackey, C. (2013). *Without Rules: A Failed Approach to Corporate Accountability.* Human Rights Watch: New York. https://www.hrw.org/sites/default/files/related_material/business.pdf

53 Kaye, D. (2015) Report on encryption, anonymity, and the human rights framework. www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

54 United Nations. (2011). Op. cit.

internal procedures, entering new markets, considering potential partners, investments and suppliers, or designing and introducing new technologies and services. The Telecommunications Industry Dialogue offers less detail in their principles, but explicitly align with the Guiding Principles, which were finalised after the launch of GNI and before the creation of the Industry Dialogue.

The public report on the GNI assessments of Google, Microsoft, and Yahoo reflects challenges implementing due diligence, noting that "new acquisitions present significant challenges for companies."[55] An anonymised case example from the report detailed how a company identified free expression and privacy risks during an acquisition and developed an implementation plan to adjust data storage in a high-risk jurisdiction. But details about how companies assess and mitigate such risks are generally few and far between. Ericsson, the first ICT company to use a new Guiding Principles reporting framework, noted it had conducted impact assessments in Myanmar, Iran, and Ethiopia during 2014 and 2015 as part of its due diligence.[56] Ericsson has also published details about its approach to due diligence in the sales process as part of an updated sales compliance policy and directive.[57]

These examples demonstrate the degree to which companies operating in different segments of the ICT value chain face very different risks. Identifying risks and implementing mitigation strategies, particularly when those strategies have serious impact on revenue, requires support from across the company, particularly at the highest levels.

The concept of human rights due diligence, and the tools and tactics that ICT companies have used to address freedom of expression and privacy can also be applied to a much wider set of human rights risks. From technology-related violence to discriminatory impacts on economic, social and cultural rights, companies should be actively using the tools at their disposal to assess and mitigate these risks.

For example, former US Federal Trade Commission technologist Ashkan Soltani has noted that companies can use big data analysis to correct hidden biases in algorithms: "You look at Google, where there was a big debate around glass ceilings and gender bias. They ran big data studies on their own hiring practices and found that they did, in fact, have gender biases in their hiring, and so they could essentially tune or correct for that."[58]

Transparency reporting

There has been some movement toward more granular guidance for ICT companies on privacy and surveillance, especially since the Snowden revelations. Transparency reporting has demonstrated the constructive potential for competition among companies to drive innovation, as companies have introduced new features and components with each release. In 2010, Google became the first company to report on government requests, followed by Twitter in 2012. By 2014, more than 40 companies around the world had released transparency reports, with telecommunications companies and ISPs joining internet companies in doing so.[59]

New iterations of transparency reports have introduced reporting on content removal, copyright removals, and search removals in Europe following the Court of Justice of the European Union ruling in Google Spain v. AEPD and Mario Costeja Gonzalez. Facebook's most recent report has introduced case studies on content removal, providing more detail on certain government censorship and user data requests. As transparency reporting has been taken up by an increasing number of companies across the sector, standardised guidance has been developed, but current iterations are focused on transparency reporting with respect to US law.[60] Nonetheless, significant gaps persist, notably around reporting on removal of content under terms of service

55 Global Network Initiative. (2014). *Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo*. globalnetworkinitiative.org/content/public-report-independent-assessment-process-google-microsoft-and-yahoo

56 www.ericsson.com/thecompany/sustainability-corporateresponsibility/conducting-business-responsibly/human-rights

57 Ibid.

58 Zara, C. (2015, 9 April). FTC Chief Technologist Ashkan Soltani on Algorithmic Transparency and the Fight Against Biased Bots. *International Business Times*. www.ibtimes.com/ftc-chief-technologist-ashkan-soltani-algorithmic-transparency-fight-against-biased-1876177

59 Losey, J. (2015). Surveillance and Communications: A Legitimization Crisis and the Need for Transparency. *International Journal of Communication, 9*. ijoc.org/index.php/ijoc/article/viewFile/3329/1495

60 New America Foundation/OTI transparency reporting project.

violations. As Ranking Digital Right reports, none of the companies ranked disclosed "any information whatsoever about the volume and type of user content that is deleted or blocked when enforcing its own terms of service."[61]

Civil society rankings and ratings

Civil society organisations, academics and activists have filled gaps in company disclosures through rankings and ratings that incentivise companies to compete with each other in rights-enhancing ways. The Electronic Frontier Foundation (EFF) has been giving out "gold stars" to companies that adopt positive privacy practices with respect to government access to user data since 2011. In 2015, the EFF adjusted the report criteria by increasing expectations of companies, most of which had become industry standards in the meantime. Although this approach was initially very focused on domestic US law, this model has has been adapted and replicated through partnerships with several digital rights groups in Latin America, with reports issued for Colombia and Mexico.[62]

In 2016, the EFF released a new version of the report focusing on the practices of "sharing economy" companies.[63] However, by focusing solely on privacy with respect to government requests, the report offers an incomplete view of the full responsibilities of those companies to respect human rights, particularly at a time when the labour practices of the sharing economy are facing scrutiny from global regulators.

The Ranking Digital Rights 2015 Corporate Accountability Index was developed with an international approach from the start, and assesses a global mix of ICT companies, including internet and telecom companies based in China, France, India, Korea, Malaysia, Mexico, Russia, South Africa, UAE, the UK and the US.[64]

Socially responsible lobbying

Companies are obliged to respect national laws in the jurisdictions where they operate. But their responsibility to respect rights "exists over and above compliance with national laws and regulations protecting human rights."[65] In situations where governments compel companies to violate human rights, companies have several options at their disposal, from challenging the government in court (see: Remedy section), to lobbying for legislative reforms that would enable them to fulfil their responsibility to respect human rights.

For example, GNI participants commit to "engage governments and international institutions to promote the rule of law and the adoption of laws, policies and practices that protect, respect, and fulfil freedom of expression and privacy."[66]In a press release responding to the first GNI assessments of Google, Microsoft, and Yahoo, Human Rights Watch noted that such assessments "should examine whether the companies are advocating reform of overreaching surveillance laws."[67]

In response to the Snowden revelations, companies have ramped up lobbying on surveillance reform, particularly through the formation of the Reform Government Surveillance coalition, consisting of AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo.[68] Other industry associations have joined broader company-civil society collaborative advocacy in the US, including the i2Coalition of internet infrastructure companies, the Internet Association and startup association Engine Advocacy.[69]

Companies have also engaged extensively with surveillance legislation initiatives in the United Kingdom, providing evidence on the Communications Data Bill and the more recent Investigatory Powers Bill both

61 Ranking Digital Rights. (2015). Op. cit.

62 Colombia: dondeestanmisdatos.info/ Mexico: https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isps-stand-their-users

63 Electronic Frontier Foundation. (2016). *Who Has Your Back? Protecting Your Data From Government Requests.* https://www.eff.org/who-has-your-back-2016

64 https://rankingdigitalrights.org/index2015

65 United Nations. (2011). Op. cit.

66 Global Network Initiative Principles on Freedom of Expression and Privacy. globalnetworkinitiative.org/principles/index.php

67 Human Rights Watch. (2014, 9 January). United States: Internet Companies Assessed on Rights Policies. https://www.hrw.org/news/2014/01/09/united-states-internet-companies-assessed-rights-policies

68 https://www.reformgovernmentsurveillance.com

69 https://static.newamerica.org/attachments/2579-nsa-coalition-letter/NSA_coalition_letter_032515.pdf

individually as part of GNI as well as through industry associations.[70]

Multistakeholder initiatives, discussed in more detail below, are important but are not the only means of engagement. Trade associations, think tanks and academia offer other venues and mechanisms, but companies need to be sure that initiatives they are involved with do not contradict their commitments to human rights. For example, the Asian Internet Coalition, which consists of Facebook, eBay, Google, LinkedIn, Yahoo, Apple, Salesforce and Twitter, has been an active voice on public policy and legislation in Hong Kong, Thailand, Vietnam, Singapore and India. However, it rarely comments specifically on human rights and has a track record of collaboration with other trade groups rather than civil society.[71] The Asociación Latinoamericana de Internet (ALAI), formed in 2015, aims to play a similar role in Latin America and the Caribbean.[72]

Engineering rights by design

Some of the most innovative approaches to human rights in the tech sector entail efforts to incorporate rights into the engineering of the internet and other ICTs.[73] Among the oldest and best known is privacy by design, which originated during the 1990s in a set of principles developed in Canada by Ontario's Information and Privacy Commissioner Dr Ann Cavoukian. Privacy by design is "an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures."[74] It has been widely supported by data protection and privacy authorities worldwide. Although not all ICT firms have formally embraced privacy by design, its spirit is reflected in the recent move toward enabling encryption by default for both data at rest (e.g. smartphones and hard disks) and data in transit (e.g. secure messaging and communications tools).

Civil society organisations have broadened this concept in recent years, calling for "human rights by design" in statements and contributions to international policy processes. At the same time, multistakeholder processes in the technical community have begun to consider a similar approach. These include the Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights (CCWP-HR) which considers the corporate and social responsibility of the Internet Corporation for Assigned Names and Numbers (ICANN), as well as the Internet Research Task Force's Human Rights Protocol Considerations Research Group.

ICT companies, whose employees are active participants in the Internet Engineering Task Force (IETF) and other multistakeholder processes, should consider buttressing these initiatives with organisational support, and integrating such efforts into their overall human rights policies and due diligence processes.

GAPS

A la carte policy commitments

The starting point for company implementation of the Guiding Principles is the adoption of a human rights policy commitment. Although a small but increasing number of ICT companies have adopted comprehensive human rights policies that embrace and are explicitly aligned with the guiding principles, implementation of human rights policies and procedures in the sector reflects the tendency of companies to respond to those issues that have triggered serious scrutiny and reputational risk. The Business and Human Rights Resource Centre maintains a list of company policy statements that reflects this tendency in the sector.[75]

The majority of ICT firms with human rights policies remain hardware manufacturers, for whom supply chain risks, such as labour conditions in factories or sourcing

70 Global Network Initiative. (2016, 8 January). GNI submits written evidence to the UK Joint Committee scrutinizing the Investigatory Powers Bill. globalnetworkinitiative.org/news/gni-submits-written-evidence-uk-joint-committee-scrutinizing-investigatory-powers-bill; other submissions available at www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/?type=Written#pnlPublicationFilter

71 Recent statements and publications from the AIC are available at www.asiainternetcoalition.org/recent-activities

72 alai.lat

73 For background, see: Doria A., & Liddicoat, J. (2012). *Human rights and internet protocols: Comparing processes and principles*. APC. https://www.apc.org/en/pubs/human-rights-and-internet-protocols-comparing-proc

74 https://www.ipc.on.ca/english/privacy/introduction-to-pbd

75 business-humanrights.org/en/company-policy-statements-on-human-rights

of raw materials from conflict regions, have motivated action.[76] For internet and telecommunications companies where freedom of expression and privacy risks have loomed largest, human rights responses have been initiated through participation in the multi-stakeholder Global Network Initiative (GNI) and the Telecommunications Industry Dialogue on Freedom of Expression and Privacy, which are on track to combine with seven telecommunications companies becoming observers of GNI in 2016.

Although GNI members make public commitments to freedom of expression and privacy, backed by rigorous independent assessments of implementation, only Microsoft has framed its GNI commitments within a broader human rights policy that explicitly includes all human rights per the Guiding Principles.[77] In contrast, Google's code of conduct deals in detail with free expression and privacy, but does not use the words "human rights".[78] APC research on the policies of companies around the world on women's rights found that only two of 22 reviewed companies had a formal commitment to human rights.[79]

Corporate culture has an impact on how companies implement and communicate their human rights approach. Internet companies, who see themselves as innovators and disruptors of established industries, can be sceptical of stodgy corporate social responsibility programmes and annual sustainability reports. In some cases they have pioneered new tools, such as transparency reporting, or have led efforts to lobby governments to pass legislation that protects and promotes human rights, or challenged government action in courts. These are valuable steps and more companies should follow suit. But by picking and choosing which issues to frame as part of human rights commitments, and by focusing narrowly on governments and sidestepping concerns with the implications of their own corporate practices, these companies are missing an opportunity to reestablish a foundation of trust with users around the world.

Enforcing terms of service

Companies are reluctant to view content moderation undertaken to enforce their terms of service (TOS) as a human rights issue. While companies should have broad discretion to set content policies that reflect the services they provide, the lack of transparency and accountability for how those policies are enforced can lead to human rights risks.[80] According to Ranking Digital Rights, "No company in the Index discloses any information whatsoever about the volume and type of user content that is deleted or blocked when enforcing its own terms of service." The distinction between content removed at the behest of governments and that removed for TOS violations, or between consumer privacy and privacy with regard to government requests is evident in company policies and procedures, as well as in multistakeholder initiatives such as the GNI principles and implementation guidelines.

But decisions made by companies about content restriction, account deactivations, and other TOS enforcement clearly have huge impacts on user rights. First, governments are increasingly making use of company TOS in order to pursue their own content control priorities. The UK government created a Counter Terrorism Internet Referral Unit that receives reports from the public about alleged "illegal terrorist or extremist content" that channels requests to internet companies to remove content, and in July 2015 Europol launched a European Union Internet Referral Unit that is taking up this practice.[81]

Second, greater transparency, better established due process, and other procedural enhancements to company practices would greatly improve their ability to respect human rights, and should be considered a part of company human rights due diligence.

Third, some companies are beginning to report limited data on TOS content removals. In its most recent transparency report, Google reported that 3,638 of 5,728 items removed from YouTube as a result of government

76 For example, see: HP, Intel and the Electronics Industry Citizenship Coalition.

77 https://www.microsoft.com/about/csr/human-rights

78 https://abc.xyz/investor/other/google-code-of-conduct.html

79 Athar, R. (2015). *From impunity to justice: Improving corporate policies to end technology-related violence against women*. APC. www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf

80 See https://onlinecensorship.org for more information.

81 More information about the UK referral unit is available at www.npcc.police.uk/NPCCBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx; the Europol initiative is at https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

requests were found to be violations of YouTube's community guidelines.[82] Twitter has also begun reporting the number of legal requests where content was removed due to TOS violations. Because these numbers only reflect government requests or legal process where content was removed for TOS violations, they only reflect one small part of the content moderation that occurs. For example, from July through December 2015, Twitter reported 2,265 accounts impacted by legal requests where content was removed due to TOS violations.[83] But this pales in comparison to the 125,000 accounts that Twitter reported suspending during the same period for "threatening or promoting terrorist acts, primarily related to ISIS."[84] Similar data is not available for other TOS violations, such as the suspension or deactivation of accounts that violate real name policies, engage in hate speech, or harassment.

In contrast to the absence of information about how companies implement most content moderation, there is a great deal of information and frequently used procedures to handle one particular issue, the removal of copyright infringing content. As APC research has documented, this is almost entirely due to US copyright law and the Digital Millennium Copyright Act (DMCA), as well as similar notice and takedown legislation that has expanded to other jurisdictions through trade agreements and other mechanisms.[85] Some companies report on copyright removal requests or disclose them to Lumen, an academic initiative that tracks such orders.[86] Other governments seeking to control particular types of online content have recognised that United States copyright law is a powerful extraterritorial tool. Ecuador, for example, has habitually used DMCA takedown requests to suppress content critical of the Ecuadorian government.[87]

Advisory groups

In recent years, several ICT companies have established outside advisory bodies such as Twitter's Trust and Safety Council, or participated in working groups such as the industry working group on cyber hate hosted by the Anti-Defamation League.[88] Critics have pointed to procedural and substantive concerns with such initiatives, particularly the lack of balanced participation by organisations representing affected communities around the world, as well as questions about how these ad hoc initiatives have been put together.[89] Companies should strongly consider situating these groups as parts of their overall human rights due diligence programmes, and ensure that their processes meet emerging standards for multistakeholder inclusion developed by civil society organisations active in internet governance.[90]

Sharing economy companies have also recently begun to engage in multistakeholder dialogue with experts, NGOs and labour unions, setting forth principles for means of ensuring that social safety net benefits and protections encompass workers in this sector.[91] Although a commendable step, this initiative risks focusing disproportionately on the US context and missing the urgent need for a truly global conversation about the impact of sharing economy business models on labour rights. For example, given the increasing number of markets where companies like Uber have faced outright bans, legal restrictions, or operate amid uncertainty or through legal loopholes, more international dialogue on this topic is urgently needed.[92]

82 https://www.google.com/transparencyreport/removals/government

83 https://transparency.twitter.com/removal-requests/2015/jul-dec

84 Twitter. (2016, 6 February). Combatting Violent Extremism. https://blog.twitter.com/2016/combating-violent-extremism

85 Athar, R. (2015). Op. cit.

86 https://lumendatabase.org/pages/about

87 Masnick, M. (2016, 28 January). Ecuador Continues To Use US Copyright Law To Censor Critics. *Techdirt*. https://www.techdirt.com/articles/20160126/18061933438/ecuador-continues-to-use-us-copyright-law-to-censor-critics.shtml

88 Anti-Defamation League. (2014, 23 September). ADL Releases "Best Practices" for Challenging Cyberhate. www.adl.org/press-center/press-releases/discrimination-racism-bigotry/adl-releases-best-practices-challenging-cyberhate.html?referrer=https://www.google.com/#.VyklmxUrL6Y

89 Puddephatt, A. (2016, 14 February). Just another 'black box'? First thoughts on Twitter's Trust and Safety Council. *openDemocracy*. https://www.opendemocracy.net/digitaliberties/andrew-puddephatt/just-another-black-box-first-thoughts-on-twitter-s-trust-and-safet

90 bestbits.net/meaningful-stakeholder-inclusion-presentation /

91 Portable Benefits. https://medium.com/the-wtf-economy/common-ground-for-independent-workers-83f3fbcf548f#.22i799cuj

92 Khosla, E. (2015, 8 April). Here's everywhere Uber is banned around the world. *Global Post*. www.businessinsider.com/heres-everywhere-uber-is-banned-around-the-world-2015-4

Access initiatives and economic, social and cultural rights

ICT companies rarely frame their activities in the context of economic, social and cultural rights, but many use explicit human rights language as part of initiatives to increase internet access around the world. In the white paper that introduced the Internet.org initiative in August 2013, Facebook founder and CEO Mark Zuckerberg wrote, "I believe connectivity is a human right, and that if we work together we can make it a reality."[93] In 2012, Vinton Cerf, internet pioneer and vice president and chief internet evangelist at Google, published a widely read New York Times op-ed that took a contrary view, that internet access is not itself a right, but that implored internet engineers to uphold human rights in their work.[94] Nonetheless, Google's extensive global internet access initiatives, including the balloon-powered Project Loon among others, do not use a human rights frame.[95]

There is no doubt that most ICT companies, particularly social media companies, view their products and services as a means of fulfilling universal human rights, from the right to education to the right to take part in cultural life. But companies rarely engage with the international institutions established as part of human rights treaties, or the UN system in general.

The stereotypical Silicon Valley mentality, summed up in Facebook's former motto for its developers, "move fast and break things,"[96] is far removed from the slow pace of international cooperation and multilateral diplomacy of the UN and its human rights system. The desire of companies to leapfrog existing access initiatives through "moonshot" projects and innovative use of technology is understandable, but problematic for a number of reasons.

First, major internet companies have been cavalier about conflating altruistic intentions with commercially beneficial market acquisition strategies. As Facebook product VP Chris Daniels told Buzzfeed, "Once people come online they discover and seek more services that they can use online. And it is also good for Facebook, there's no question about that. When more people come online, those are more potential Facebook users."[97] This conflation has been a major factor in the backlash against Internet.org that has been most prominent in India, where regulators banned zero-rating services in 2016. In that case, Indian regulators found the competitive risks of an initiative that would make Facebook a de facto gatekeeper for a walled garden of a limited set of applications and services outweighed the potential benefits of Free Basics.[98] Second, by insufficiently involving the communities most affected by a lack of internet access, they are missing opportunities to both improve their products and services and develop initiatives with genuine

93 The white paper, written in the first person, is not available on Internet.org and can only be read when logged into Facebook. Zuckerberg, M. (2013, 23 August). Is Connectivity a Human Right? *Facebook*. https://www.facebook.com/isconnectivityahumanright

94 Cerf, V. (2012, 5 January). Internet Access is Not a Human Right. *The New York Times*. www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html

95 www.google.com/loon

96 Kelly, S. (2014, 30 April). Facebook Changes Its 'Move Fast and Break Things' Motto. *Mashable*. mashable.com/2014/04/30/facebooks-new-mantra-move-fast-with-stability/

97 Kantrowitz, A. (2016, 21 January). How Facebook Stumbled On Its Quest To Give Internet Away for Free. *Buzzfeed*. https://www.buzzfeed.com/alexkantrowitz/how-facebooks-plan-to-give-the-world-free-mobile-internet-we?utm_term=.pqWvRwK9k#.faVJveEoD

98 Bhatia, R. (2016, 12 May). The inside story of Facebook's biggest setback. *The Guardian*. https://www.theguardian.com/technology/2016/may/12/facebook-free-basics-india-zuckerberg

buy-in. Internet.org launched with lofty rhetoric about involving NGOs, academics and experts, but its founding partners were other tech companies, such as Ericsson, Nokia, Qualcomm and Samsung – many of whom are no longer affiliated with the initiative. Rather than "move fast and break things," ICT company access initiatives should recognise the paramount importance of the leadership of affected communities, or as disability activists and other global activists have said, "nothing about us without us."[99] ICT companies should use their products, resources and personnel to obtain feedback from the ground about how best to achieve universal internet access.

Third, such initiatives cannot avoid engagement with regulators. Although the most obvious example of this is the Telecom Regulatory Authority of India's decision to ban zero-rating services, other industry access initiatives are also running into regulatory conflicts. Although Project Loon initially planned to purchase proprietary space on the radio spectrum to operate independently of existing networks, recent news from India, Sri Lanka, and Indonesia suggests that the initiative will instead work through local mobile network operators' spectrum.[100]

In recent months, there are signs that internet companies are revamping their approach to increasing access. In September 2015, Mark Zuckerberg made an unprecedented visit to the UN, where he addressed the General Assembly's Sustainable Development Summit. In his remarks and in an op-ed co-authored with Bono, Zuckerberg called for internet access as a component of the newly agreed Sustainable Development Goals.[101] At the same time, the company announced changes to Internet.org intended to allay civil society concerns, rebranding its zero-rating component as Free Basics.

High level meetings and op-eds with celebrities may generate buzz, but they will not meet the goal of helping to achieve the Sustainable Development Goals in a rights-respecting manner. ICT companies with global operations should give thought to how they engage on the ground, incorporating economic, social and cultural rights into human rights impact assessments and expanding such assessments to include access initiatives. Such assessments should guide how they participate in ventures such as the Global Connect Initiative[102] and the Alliance for Affordable Internet.[103] However companies choose to engage, they should be sure that their efforts are informed by, and coordinated with, the communities that they seek to benefit, as well as governments' existing access policies.

99 Abdul Raheem, T. (2005, 9 June). Nothing about us without us. *Pambazuka*. www.pambazuka.org/pan-africanism/nothing-about-us-without-us

100 Steel, W. (2016, 29 March). An update on Google's Project Loon. *Cleanleap*. cleanleap.com/update-googles-project-loon

101 Bono, & Zuckerberg, M. (2015, 26 September). To Unite the Earth, Connect It. *The New York Times.* www.nytimes.com/2015/09/27/opinion/sunday/to-unite-the-earth-connect-it.html

102 https://share.america.gov/globalconnect/

103 a4ai.org

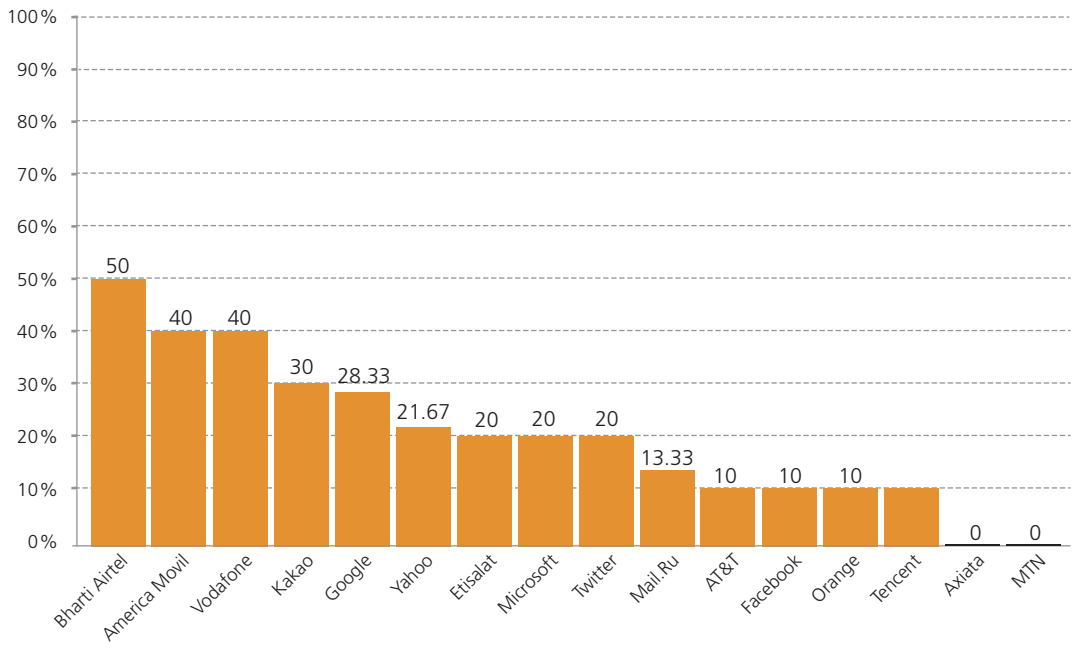
REMEDY – STILL THE FORGOTTEN PILLAR?

The right to remedy when companies are involved in human rights abuses is an essential component and the third pillar of the Guiding Principles. Despite increasing adoption of the Guiding Principles by tech sector companies, access to effective remedy is less established in the ICT sector compared to other industries that have faced serious human rights scrutiny, including extractive industries and manufacturing. In those sectors, human rights defenders and civil society are pressing companies to ensure grievance mechanisms meet effectiveness criteria laid out in the Guiding Principles. In the ICT sector, just getting companies to establish any sort of grievance mechanisms framed explicitly in Guiding Principles terms has proven challenging.[104] Company performance on the remedy indicator in the Ranking Digital Rights index was easily the worst in the "commitment" category, with all companies scoring 50% or less (see Figure 1). [105]

The Guiding Principles note that unless governments "investigate, punish, and redress business-related human rights abuses" the state duty to protect "can be rendered weak or even meaningless."[106] However, the close relationship between governments and companies involved in many abuses in the ICT sector complicates the provision of effective remedy.

The landscape of remedy consists of state- and non-state-based mechanisms that are either judicial or non-judicial.[107] This section will briefly survey some of the most notable cases in the landscape of remedy for the ICT sector, identifying gaps and opportunities for improvement.

FIGURE 1. Grievance and remedy mechanisms: Overall company performance



Source: Ranking Digital Rights. https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf

104 Micek, P., & Landale, J. (2013). *Forgotten Pillar: The Telco Remedy Plan*. New York: Access Now. https://www.accessnow.org/cms/assets/uploads/archive/docs/Telco_Remedy_Plan.pdf

105 Ranking Digital Rights. (2015). Op. cit.

106 www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

107 Shift. (2014). *Remediation, Grievance Mechanisms and the Corporate Responsibility to Respect Human Rights*. New York: Shift. shiftproject.org/publication/remediation-grievance-mechanisms-and-corporate-responsibility-respect-human-rights

JUDICIAL REMEDY

Domestic courts

Domestic legal remedy for ICT-related rights violations remains a work in progress, with legal challenges by companies against governments having been more productive in recent years than challenges against companies for their own offences.

In the case of privacy violation stemming from state surveillance, excessive secrecy has stalled litigation, particularly in the US and UK.[108] In early 2006, following news reports about US National Security Agency (NSA) mass surveillance and after receiving documents from AT&T technician Mark Klein, EFF brought a class action lawsuit against AT&T on behalf of its customers for collaborating with NSA mass surveillance.[109] But the passage of the 2008 FISA Amendments Act provided immunity for telecoms companies if the government certifies, in secret, that surveillance was legal or authorised by the president. Another early suit filed by the American Civil Liberties Union on behalf of a coalition of NGOs, journalists, lawyers and academics was dismissed because the plaintiffs could not prove they had been subject to NSA spying. But in the wake of the Snowden revelations, a wide range of litigation is moving forward.

In addition to lawsuits brought against companies for complicity with state surveillance, there are also cases where companies have challenged surveillance as unconstitutional. In 2008, Yahoo challenged the authority of the predecessor to the FISA Amendments Act in the Foreign Intelligence Surveillance Court. The challenge and its appeal were denied, and Yahoo's role in the challenge was classified until 2013, but Yahoo did successfully sue to declassify documents from the case.[110] A group of US tech companies previously filed suit against the government seeking the right to publish more information about national security requests in their transparency reports, reaching a settlement in early 2014.[111] Twitter has an active suit and Microsoft recently filed a new challenge against non-disclosure provisions that impose perpetual secrecy on government requests to access user data.[112]

Claims have also been filed against the UK Government and its signal intelligence agency, Government Communications Headquarters (GCHQ). Privacy International and Bytes for All, Pakistan filed a claim against mass surveillance with the Investigatory Powers Tribunal (IPT) – another instance of a secret tribunal that does not make its proceedings public – that UK spying has been "neither necessary nor proportionate."[113] Privacy International also worked with a global group of seven internet service and communications providers – GreenNet (UK), Riseup (US), Mango Email Service (Zimbabwe), Jinbonet (Korea), Greenhost (Netherlands), May First/People Link (US), and the Chaos Computer Club (Germany) – to challenge GCHQ's computer network exploitation, or government hacking. Although the IPT ruled against the providers, the proceedings led to GCHQ's first public admission of engaging in hacking both internationally and domestically, and has informed advocacy on this issue in the Investigatory Powers Bill.[114]

Beyond challenges against US and UK mass spying, other domestic legal cases have investigated ICT sector involvement in human rights abuses. In October 2011 in France, human rights groups filed a criminal complaint against the company Amesys, a subsidiary of Bull, for complicity with acts of torture in Libya undertaken in connection with communications surveillance equipment they supplied to the Libyan government.[115] That case is still pending in a Paris tribunal that specialises in war crimes, crimes against humanity and genocide, but demonstrates obstacles to accessing judicial remedy, from the challenges of collecting evidence in a conflict setting, to challenges getting the prosecutor's office to take up the case.[116]

---

108 Public interest journalism organisation ProPublica has a comprehensive tracker of National Security Agency (NSA) surveillance lawsuits: https://projects.propublica.org/graphics/surveillance-suits

109 https://www.eff.org/nsa/hepting

110 https://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence

111 Timberg, C., & Goldman, A. (2014, 27 January). U.S. to allow companies to disclose more details on government requests for data. *Washington Post.* https://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html

112 Nakashima, E. (2014, 7 October). Twitter sues U.S. Government over limits on ability to disclose surveillance numbers. *Washington Post.* https://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html

113 https://www.privacyinternational.org/node/66

114 Kim, S. (2016, 12 February). Investigatory Powers Tribunal Rules GCHQ Hacking Lawful. *Privacy International*. https://privacyinternational.org/node/729

115 FIDH. (2011, 19 October). FIDH and LDH file a complaint concerning the responsability of the company AMESYS in relation to acts of torture. https://www.fidh.org/en/region/north-africa-middle-east/libya/FIDH-and-LDH-file-a-complaint

116 FIDH. (2014). *Business and Human Rights: Enhancing Standards and Ensuring Redress*. Paris: FIDH https://www.fidh.org/IMG/pdf/201403_briefing_paper_enhance_standards_ensure_redress_web_version.pdf

In India, ICT companies played a prominent role in efforts to overturn notorious provisions of India's IT Act, including Section 66a, which was used to arrest individuals for allegedly "offensive" content, and strengthening protections for intermediaries in section 79 of the IT Act, which had been shown to lead companies to broadly censor content in over compliance with the provision. Indian e-commerce site MouthShut and the Indian Internet and Mobile Industry Association filed separate challenges that were merged with suits by a range of public interest groups and which resulted in a landmark ruling in March 2015.[117]

Regional mechanisms

At the international level, regional human rights courts have played a prominent role shaping jurisprudence for the ICT sector. Human rights organisations have challenged GCHQ's mass surveillance initiatives at the European Court of Human Rights in cases that are currently pending, and recent judgments concerning Hungary and Russia have ruled that national security surveillance must be individualised, holding out the promise of establishing that mass surveillance is a violation of the right to privacy.[118] Not every ruling by the ECHR has necessarily advanced human rights protections in ICTs. In Delfi AS v. Estonia, the ECHR ruled that holding an online news outlet liable for defamation for user-generated comments did not violate freedom of expression under Article 10 of the European Convention on Human Rights.[119]

Internet and ICT-related issues are also beginning to surface at the other regional human rights systems, which are composed of commissions and courts, although they have yet to address the role of the private sector in detail. In Latin America, the Inter-American Commission on Human Rights (IACHR) has taken an interest in freedom of expression and the internet. In 2013, IACHR Special Rapporteur on Freedom of Expression and Opinion Carolina Botero published a report on Freedom of Expression and the Internet.[120] In April 2016, Brazil organised a hearing at the IACHR on cultural rights and the internet, in which the role of internet intermediaries was highlighted as a key concern by both the Brazilian government and civil society organisations, including APC.[121] In Mexico, where a coalition of journalists, human rights groups and students have challenged telecommunications data retention mandates for their lack of legal safeguards, a domestic court recently ruled against the challenge and activists have indicated they will file new litigation before the Inter-American Court of Human Rights.[122]

At the African Commission for Human and Peoples' Rights (ACHPR), "the issue of Internet rights is still almost completely absent from the agenda," according to the Secretariat of the African Declaration on Internet Rights and Freedoms.[123] For this reason, organisations that helped to create the declaration have engaged with the commission to drive recognition of the internet and its role as an enabler of human rights. The African Court on Human and Peoples' Rights, which works together with the commission, delivered its first judgement in 2009 and has finalised only 25 cases thus far. The rising number of instances of network shutdowns during elections and other politically sensitive periods on the African continent is an emerging issue, with a group of NGOs writing to the African Union and encouraging the ACHPR to resolve that internet shutdowns violate freedom of expression.[124] Such action will lay the groundwork for eventual action by the African Court.

117 Singh, M. (2015, 25 March). India High Court: No Takedown Requests on Social Sites Without Court, Gov't Order. *Centre for Internet & Society*. cis-india.org/internet-governance/news/bloomberg-bna-march-25-2015-madhur-singh-india-high-court-no-takedown-requests-on-social-sites-without-court-govt-order

118 St. Vincent, S. (2016, 13 January). Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe? *CDT*. https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe

119 https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia

120 Inter-American Commission on Human Rights. (2013). *Freedom of Expression and the Internet*. Office of the Special Rapporteur for Freedom of Expression. oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf

121 Levine, R. (2016, 9 April). Cultural Rights and the Internet in Brazil. *Human Rights Brief*. hrbrief.org/hearings/cultural-rights-and-the-internet-in-brazil/

122 Bogado, D. (2016, 6 May). Mexico's Supreme Court Won't Halt Data Retention: Activists Plan to Take Case to International Court. *EFF Deeplinks Blog*. https://www.eff.org/deeplinks/2016/05/mexicos-supreme-court-wont-halt-data-retention-activists-plan-take-case

123 Mlonzi, Y. (2016, 14 April). Making Internet rights visible at the African Commission on Human Rights. *African Declaration on Internet Rights and Freedoms*. africaninternetrights.org/updates/2016/04/article-628/

124 Joint letter on internet shutdown in Uganda. https://www.indexoncensorship.org/2016/02/joint-letter-on-internet-shutdown-in-uganda/

Remedy and technology-related violence against women

The other area where domestic legal remedy for business involvement in rights abuses is developing at a fast pace is regarding technology-related violence, especially against women. Research undertaken for APC's "End violence: Women's rights and online safety" project explored legal frameworks in seven countries and found that even countries that are CEDAW signatories and which have constitutional prohibitions on gender discrimination have serious deficiencies in their legal frameworks that reflect structural failures, power imbalances, and a culture of impunity when it comes to violence against women.[125] Frustration with inaction by tech companies to respond appropriately to technology-related violence, has led to increasing calls to hold companies liable when they fail to take appropriate action to protect users, and legislation that imposes varying burdens on intermediaries, from requiring them to respond to requests for information about the identity of a harasser, to deactivating accounts or removing content.[126]

This is a difficult area. Online violence against women chills free expression and suppresses speech, including for journalists, bloggers and human rights defenders. As Snježana Milivojević writes, "Gendered harassment and online sexual abuse cause a very distinct form of chilling effect. In the age of 'here comes everybody' many women choose to blog, tweet, write or speak hiding under a (male) pseudonym. Others keep isolated, remain silent or just leave the cyberspace. Thus the chilling effect of abuse may spread beyond the female journalistic community."[127] At the same time, holding intermediaries liable for user-generated content risks further constraining these rights by incentivising companies to over-comply with content removal requests to avoid liability. More thoughtful engagement between legislators, regulators, company representatives, and communities directly affected by online violence against women is required to craft both legislation and corporate policies that begin to deter and respond to technology-related violence.

To that end, Carly Nyst has proposed "moving from an approach that focuses on the liability of intermediaries, to one which focuses on the responsibility of intermediaries."[128] Meanwhile, Sarah Jeong writes that "the odd thing about the new era of major social media content moderation is that it focuses almost exclusively on deletion and banning," while putting forward a taxonomy of additional approaches, such as filtering, editing, annotation, amplification and diminution, as well as banning users, IP bans, suspension, and accountability processes.[129]

ICT companies should embrace the concept of intermediary responsibility and work together with other stakeholders to craft policies and procedures, including enhancing their own operational grievance mechanisms, to address this issue. Legislation in this arena should comply with the Manila Principles on Intermediary Liability, which provide human-rights based standards for intermediaries and were developed by global civil society organisations.[130]

---

125 Women's Legal and Human Rights Bureau. (2015). *End violence: Women's rights and safety online project - From impunity to justice: Domestic legal remedies for cases of technology-related violence against women*. APC. https://www.apc.org/en/pubs/impunity-justice-domestic-legal-remedies-cases-tec-0

126 Nyst. C. (2014). *Technology-related violence against women: Recent legislative trends*. APC. www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_ln.pdf

127 Milivojević, S. (2016). *More platforms, less freedom: How new media reproduce old patriarchal structures*. www.osce.org/fom/220411?download=true

128 O'Brien, D. (2015, 2 October). Breaking Section 230's Intermediary Liability Protections Won't Fix Harassment. *EFF Deeplinks Blog*. https://www.eff.org/deeplinks/2015/10/breaking-section-230s-intermediary-liability-protections-wont-fix-harassment; see also Nyst, C. (2013, 26 November). Towards Internet Intermediary Responsibility. *GenderIT.org*. www.genderit.org/feminist-talk/towards-internet-intermediary-responsibility

129 Jeong, S. (2015). *The Internet of Garbage.*

130 https://www.manilaprinciples.org

NON-JUDICIAL REMEDY – EMERGING INSTITUTIONS AND MECHANISMS

State- and non-state-based non-judicial mechanisms are also beginning to consider the ICT sector.

State-based non-judicial mechanisms include the national contact points (NCPs) of the Organisation for Economic Co-operation and Development (OECD), an implementation mechanism for governments that adhere to the OECD Guidelines for Multinational Enterprises.[131] NCPs, who are usually seated within the foreign ministry or other government agency, receive reports of specific instances of alleged violations of the OECD guidelines, investigate the specific instances and provide dispute resolution.

Since the 2011 update to the OECD guidelines that brought them into alignment with the Ruggie principles, which also introduced reference to internet freedom, complaints to NCPs concerning ICTs have increased, with complaints filed in the UK, Germany and Mexico concerning ICT involvement in corruption, illegal surveillance and facilitating drone strikes. NCPs are an important resource that cover alleged violations by companies based in adhering states operating abroad, and include not only the 34 members of the OECD, but also another 12 governments that subscribed to the OECD Declaration on International Investment and Multinational Enterprises.[132]

Governments have broad leeway when it comes to implementation of the NCPs. Some house the NCP within an existing government agency, such as the Peruvian Investment Promotion Agency or the US State Department, while others such as Norway have institutionalised their NCP as an independent government agency.[133] At the same time, the enforcement powers of NCPs are limited, amounting to what is effectively a "name and shame" system, and which is used robustly only by some NCPs. The US in particular has been vocally criticised by NGOs for overly strict confidentiality provisions, procedural weaknesses, and obstacles to access that "prevent it from serving as an effective remedial mechanism for corporate human rights abuses."[134]

International financial institution mechanisms

Non-state-based mechanisms include the accountability mechanisms of international financial institutions, industry and multistakeholder initiatives, and company grievance mechanisms. Examples include the World Bank Inspection Panel[135] and the International Finance Corporation Office of the Compliance Advisor/Ombudsman.[136] Complaints to these mechanisms have historically concerned the social and environmental impacts of development finance investments in extractives and infrastructure. But given the high degree of international financial institution investment in telecommunications networks, including in operating environments where both corruption and human rights risks run high, they could prove to be a much-needed instrument for accountability.

Industry and multistakeholder initiatives

Industry associations and multistakeholder institutions in the ICT sector are behind the curve when it comes to grievance mechanisms. The Guiding Principles state that the legitimacy of such initiatives may be put at risk if they do not provide mechanisms to ensure that affected parties can raise concerns if they believe such organisations are not fulfilling their commitments. The challenge of putting in place such systems for the ICT industry, which operates at a vast scale, is a significant one. GNI has committed to creating a complaints and grievance mechanism, but has run up against the challenge of working with participants who serve billions of users.[137] The telecommunications industry dialogue has examined "options for implementing grievance mechanisms," but did not implement a system prior to combining with GNI. The newly enlarged GNI, with telecommunications company observers, has an opportunity to move from laggard to leader on grievance and ICTs by focusing its shared learning activities on this challenge and putting a system into place.

131 www.oecd.org/investment/mne/ncps.htm

132 mneguidelines.oecd.org/oecddeclarationanddecisions.htm

133 Details on each NCP are available at mneguidelines.oecd.org/ncps

134 Accountability Counsel NAP submission: www.accountabilitycounsel.org/wp-content/uploads/2012/05/1.15.2015-Accountability-Counsel-NAP-submission.pdf

135 ewebapps.worldbank.org/apps/ip/Pages/Home.aspx

136 www.cao-ombudsman.org

137 Contact points to raise concerns about GNI implementation by company members are available on GNI's contact us page: https://www.globalnetworkinitiative.org/contact

Company mechanisms

Even those ICT companies that have explicitly adopted the Guiding Principles are early in the process of developing grievance mechanisms that meet the effectiveness criteria set out in the guiding principles. According to the Ranking Digital Rights index, "the company scoring highest points for remedy in the Index was Bharti Airtel of India, while the highest-scoring Internet company on remedy was Kakao of South Korea. In both cases these companies' strong performance is largely due to legal requirements in their home markets."[138] Interestingly, both South Korea and India score only "partly free" according to the Freedom House 2015 Freedom on the Net report.[139] This suggests an opportunity for global telcos to learn from regulations in their operating markets and develop or augment their group-wide mechanisms to improve their systems across the board.

Grievance mechanisms are yet another area where companies would benefit from integrating issues like online harassment into a holistic human rights-based approach. Companies' customer service, content moderation, and ethics and compliance hotlines and reporting channels are already handling large quantities of complaints with human rights implications, and these processes should be able to identify human rights-specific concerns as such and handle them appropriately. Put simply, there is no reason why companies with the resources and ingenuity of internet and telecom sector leaders should not have grievance mechanisms that meet or exceed the effectiveness criteria in the Guiding Principles. Leaders in other industries, such as the adidas Group, not only have developed such mechanisms, they regularly report on their use.[140]

138 Ranking Digital Rights. (2015.) Op. cit.

139 https://freedomhouse.org/report/freedom-net/freedom-net-2015

140 Disclosure of Third Party Complaints Received by the adidas Group in 2014. www.adidas-group.com/media/filer_public/1f/38/1f38f565-9b7b-4577-a66f-246e9ab9b3d6/disclosure_of_third_party_complaints_received_by_adidas_group_in_2014_aug31.pdf

CONCLUSION AND RECOMMENDATIONS

In a blistering open letter announcing his resignation from the UN Working Group on Business and Human Rights, Puvan Selvanathan wrote:

> I suggest that if states wish for businesses to respect human rights then what that constitutes must be made mandatory. Otherwise it is just voluntary. Legally required standards compel compliance in business operations to a meticulous degree. Business respects boundaries and business craves clarity. Companies are our own social creations and reflect our own values. They are defined by the rules that we choose to lay down. We hope they create wealth, drive economies and are not "evil". But if they are because there are no rules or consequences, then we are responsible.

In theory, a legally binding treaty would be the best way to impose mandatory legal requirements on companies operating around the world. In practice, the path to such a treaty is long and full of obstacles. But leaving corporate accountability for human rights as a purely voluntary initiative is both inadequate and a misreading of the promise of the Guiding Principles.

It would be unhelpful to conclude that everyone with a stake in how human rights are applied in the ICT sector should simply do more and do better. But digital rights advocates do need to drive a deeper debate about the details of how governments and companies implement the Guiding Principles while at the same time broadening discussions about a new business and human rights treaty to incorporate ICT-specific concerns.

The same rights that people enjoy offline apply online. The obligations of ICT companies to respect those rights must extend across both online and offline environments around the world. As more and more aspects of life are mediated by digital interactions, all human rights are digital rights. The sooner that both governments and companies recognise and act upon this, the better.

FOR GOVERNMENTS

- Refrain from compelling companies to violate human rights. Any restrictions on rights that involve private companies should be justified as necessary and proportionate under international human rights law.
- Formalise commitment to the responsibility to respect through national action plans that specifically address ICT sector policies and initiatives.
- Make company human rights due diligence mandatory. There are myriad ways to implement mandatory due diligence, from the creation of non-financial reporting requirements as in the EU, requiring companies to conduct human rights due diligence and impact assessments, or developing issue specific requirements.
- Review legal requirements for grievance mechanisms for ICT companies and consider explicit human rights requirements for grievance mechanisms in line with the right to remedy under the Guiding Principles.
- OECD National Contact Points should engage in joint peer-learning focused on responsible business conduct in the ICT sector, which could be used to consolidate and update sector specific guidance for company due diligence.
- Non-OECD states should sign up to the OECD Declaration on International Investment and Multinational Enterprises and establish NCPs.

FOR INTERGOVERNMENTAL INSTITUTIONS AND INITIATIVES

- The Human Rights Council should define the scope of the open-ended intergovernmental working group on a legally binding instrument, including a review process following the elaboration of elements of the draft treaty. This should be presented for consultation at the Forum on Business and Human Rights, providing a robust opportunity for stakeholders to weigh in on how the treaty process should proceed.
- The UN Working Group on Business and Human Rights should be tasked with preparing a report assessing implementation of the Guiding Principles during its mandate and with recommendations for the treaty process, soliciting input from diverse stakeholders, including the ICT sector.
- The Freedom Online Coalition should adopt a peer review process that monitors member governments track record, and involves external stakeholders.

FOR NATIONAL HUMAN RIGHTS INSTITUTIONS

- Engage with the private sector, civil society and the government to strengthen the online and offline protection and promotion of human rights impacted by the ICT sector.
- Consider ICTs as a cross-cutting issue that should be incorporated across efforts to promote and protect human rights.
- Invest in technology. Very few national human rights institutions employ basic digital security such as encrypted websites, end to end encrypted email, and other information security tools and resources.

FOR COMPANIES

- Formalise policies that commit to respect for all human rights, consistent with the Guiding Principles. They should broaden their analysis of what are the most salient human rights issues, those that pose the greatest risk to people, rather than risks to the company. Although freedom of expression and privacy continue to be critical issues for the ICT sector, companies should broaden their analysis to include other salient rights, and incorporate existing resources, tools and reporting into a human rights framework compliant with the guiding principles.
- Company and industry advisory initiatives should incorporate emergent best practices for multistakeholder inclusion, increase transparency about their activities and work to increase their diversity. The establishment of regional or national level advisory groups could help to ensure greater global participation in such initiatives.
- Increase their engagement on public policy in support of human rights, and cease lobbying activities and affiliations that may be at odds with their human rights policies.
- Incorporate explicit human rights components into existing customer service and ethics-related grievance mechanisms, such as hotlines that are accessible to users, so that they meet the effectiveness criteria in the Guiding Principles.

FOR CIVIL SOCIETY

- Digital rights and free expression organisations should continue their dialogue with organisations working to combat technology-related violence, especially against women, and hate speech. Building off the Manila Principles on Intermediary Liability, these organisations should work together to develop implementation guidance for regulators and companies that helps address harassment. The checklist developed by APC for intermediaries to address violence against women in compliance with the Guiding Principles could provide a starting point for this effort.[141]
- Explore national level advocacy campaigns targeting companies who are lagging behind industry standards on human rights. This could build upon the global advocacy that organisations like Access Now are undertaking using the Ranking Digital Rights 2015 Corporate Accountability Index.
- Consider principled engagement with companies. This should entail working together with companies through structures like the GNI and other multistakeholder advocacy and learning, while continuing to speak out against ICT company actions that negatively impact human rights.

141 Athar, R. (2015). Op. cit.

Internet and ICTs for social justice and development

APC is an international network of civil society organisations founded in1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs).

We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org info@apc.org

Graphic Design: MONOCROMO

THIS ISSUE PAPER FORMS PART OF APC'S GLOBAL POLICY ADVOCACY WORK, AND WAS PRODUCED WITH THE SUPPORT OF CORE FUNDING FROM THE SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY (SIDA).

BUSINESS AND DIGITAL RIGHTS: TAKING STOCK OF THE UN GUIDING PRINCIPLES FOR BUSINESS AND HUMAN RIGHTS IN THE ICT SECTOR
June 2016

ISBN 978-92-95102-64-4 APC-201604-CIPP-I-EN-DIGITAL-255