ARTICLE 19

Public interest, private infrastructure

An analysis of the barriers and drivers for adopting human rights standards in the Internet infrastructure industry

2018

ARTICLE 19
Free Word Centre
60 Farringdon Road
London EC1R 3GA
United Kingdom
T: +44 20 7324 2500
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

© ARTICLE 19, 2018

First published by ARTICLE 19, 2018

ARTICLE 19 is very grateful to Beth Goldberg for her contributions to this report.

We would also like to express our deep appreciation to all of the members of Internet infrastructure companies who shared valuable insights and time to the production of this report. We are grateful as well to experts at Yale Law School, Yale Jackson Institute for Global Affairs, and Center for Business and Human Rights for their feedback and review of this report.

This work is provided under the Creative Commons Attribution-Non-CommercialShareAlike 2.5 licence. You are free to copy, distribute and display this work and to make derivative works, provided you:

1) give credit to ARTICLE 19;
2) do not use this work for commercial purposes;
3) distribute any works derived from this publication under a licence identical to this one.

To access the full legal text of this licence, please visit: http://creativecommons.org/licenses/by-nc-sa/2.5/legalcode.
ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used.

Contents

Introduction 6

Background 8

What is Internet infrastructure? 8

Governance of Internet infrastructure 10

How does Internet infrastructure impact human rights? 10

The private sector's responsibilities 12

Research methodology 13

Findings: Key drivers of adoption of human rights standards 15

Primary driver of adoption: Reputational concerns 15

Secondary driver of adoption: Top-down accountability 17

Findings: Key barriers to adopting human rights standards 21

Primary barrier to adoption: Government demands 21

The paradox of government relations 22

Assessing the role of competition: A driver or barrier to adoption? 24

Economic analysis of the Internet infrastructure provider industry 24

Industry stakeholder analysis: Consumers, suppliers, and substitutes 25

Pro-social and negative competition 26

Recommendations for businesses 28

Recommendations for civil society 30

Areas for further research 33

Role of investors 33

Role of competition 33

Role of non-corporate providers 33

Appendix 1 35

End notes 36

Executive summary

The Internet has become a powerful vehicle for the exercise of human rights. At the same time, it is increasingly becoming a vehicle for the restriction of rights. The Internet's infrastructure — the cables, satellites, and spectrum that carry information between computers — provides a particularly effective bottleneck for governments and private actors alike to control the flow of information. Manipulation of Internet infrastructure can be used to surveil conversations, prevent journalists from reporting securely, or block users in a particular country or region from learning about political events, to name a few use cases. The majority of these chokepoints are owned and operated by private companies,[1] putting these companies in the position of having to mediate the tension between rights to free expression and individual liberty on the one hand, and economic incentives and government requests for user data on the other.[2] Although Internet infrastructure providers often claim to be "neutral pipes," increasing restrictions at the infrastructure level — whether imposed at the behest of governments or by the providers themselves — makes clear the politicized role they play.

Internet infrastructure providers have the technical power to safeguard the rights of end-users, or to facilitate human rights abuses through their services and technologies.[3] The power of these private companies derives from more than their technical function as operators of immense volumes of human communication. Industry analysis reveals that providers often function as regional monopolies with little pressure from buyers, sellers, or competitors, affording them an enormous amount of economic and political power. As providers gain more users, they become more enticing targets for governments to co-opt to enforce their control over citizens' Internet access and use. Such government intervention in Internet traffic is on the rise in dictatorships and democracies alike.[4] These infringements on users' human rights demand oversight, yet most Internet infrastructure providers avoid the public scrutiny given to more visible social media platforms or consumer devices by virtue of operating unseen in cables underground or under the sea.

While some Internet infrastructure providers have acknowledged their influence and established safeguards against abuse of their services, the majority have yet to align their policies and practices with international human rights standards. This is in part because infrastructure providers are generally localized, making them subject to local jurisdiction and regulations to an extent that Internet platforms typically are not. Furthermore, infrastructure providers often require local licenses to build and operate infrastructure, constraining their ability to negotiate with governments. Faced with the compounding challenges of government interference, lack of public scrutiny, and consolidation of market power, Internet infrastructure providers must institutionalize robust internal policies to help avoid complicity in human rights violations.

This report examines the most influential catalysts and barriers that shape Internet infrastructure providers' behavior regarding human rights. The report focuses on providers' adoption of the UN Guiding Principles on Business and Human Rights (UNGPs),[5] a widely accepted global standard defining responsibilities of businesses.

Adoption of the UNGPs serves as a valuable metric for understanding how companies are fulfilling their positive responsibilities to mitigate human rights impacts of their operations, publish transparency reports, and provide remedy for potential human rights violations.

Among Internet infrastructure companies that have developed strong human rights protections, the report describes two key drivers of these policies:

- Reputational concerns following revelations of human rights violations, or the specter of negative press for potential future violations.

- Top-down accountability from corporate leadership signaling that human rights are a priority for the company.

Primary barriers to Internet infrastructure providers adopting human rights standards were identified as:

- Government requests for companies to interrupt the free flow of information and serve demands for censorship, surveillance, or obstruction of communication.

- Perceived high cost and unclear benefits of UNGP adoption, particularly when companies are not public facing.

Competition between companies was identified as both a potential driver and barrier, inciting companies to meet higher standards set by peers, or inducing them to settle to the "lowest common denominator" of human rights protections among their competitors. As such, the role of competition — specifically within the Internet infrastructure industry — is analyzed separately.

The report concludes with specific measures that businesses and civil society organizations can take to protect human rights across the Internet's infrastructure. Recommendations address how businesses and civil society can partner to mitigate risks and embed accountability mechanisms for human rights impacts.

Introduction

Restricting open Internet access can have devastating consequences for citizens and businesses alike. The throttling or blocking of Internet access can shutter the doors to millions of e-commerce platforms and prevent ongoing business operations. More fundamentally, such restrictions violate the human rights that the Internet has uniquely enabled — freedom of expression, access to information, and privacy among them.[6]

Freedoms online are stifled in a range of forms: surveillance, censorship, throttled access speeds, limitations on encryption and anonymity, and Internet shutdowns make a free and open Internet an ideal far from reality. As recently as 2016, at least 64% of the world's population lived in countries with significant restrictions on their freedom online, and that number is only growing as governments and private actors cooperate to restrict the Internet: this is the seventh consecutive year Freedom House has measured a decline in freedom online.[7] Restrictions to free expression and access to information online are most frequently initiated by governments in the name of security, but privately owned Internet infrastructure companies are often complicit, whether begrudgingly or as willing facilitators.[8]

Although far less visible than regulation of content on social media platforms, the Internet's infrastructure is particularly vulnerable to negative human rights impacts because vast amounts of information travel through centralized infrastructure, creating potential chokepoints for censoring, surveilling, or shutting down access. Moreover, many Internet infrastructure providers operate as regional monopolies, giving consumers and governments little leverage to negotiate. As the industry is projected to further expand its market power, the question of how users will advocate for their human rights to be respected online becomes even more pressing.

In this context, it is vital to understand the behavior of corporations that operate Internet infrastructure, including the policy context in which they operate. Some governments, including the U.S., have taken a hands-off approach to regulating Internet development relative to other communications infrastructure on the basis that regulation would stifle innovation, and that market forces or antitrust mechanisms are sufficient[9] Self-regulation by companies is expected in the absence of governmental intervention. In particular, technology companies must balance competition and profits on the one hand with the fear of enabling "bad actors" through their service on the other hand. This creates an opportunity, and necessity, for businesses to find consensus on internal policies that enforce respect for human rights while levelling the playing field for competition. This is particularly important as the Internet becomes increasingly necessary to the exercise of basic economic, political, and social rights.

This report focuses on how this can be achieved through the application of the the United Nations Guiding Principles on Business and Human Rights ('the UNGPs') to Internet infrastructure providers. Published in 2011, the UNGPs are the product of six

years of consultations by the United Nations, civil society, and business stakeholders.[10] They represent the most widely accepted set of voluntary standards for business to respect human rights. As such, they have been applied to a wide range of industries, including oil and gas, mining, and textile manufacturing, among others.[11] Most recently, the UN Special Rapporteur on Freedom of Expression extensively referred to them in his landmark 2017 report on the role of the private sector in the provision of Internet access.[12] The first of its kind, the report detailed how Internet access entities should respect freedom of expression and privacy online, in conjunction with commercial interests. Building on the UNGPs, ARTICLE 19 also published a policy brief on the obligations of telecommunications and Internet service providers to protect and respect freedom of expression.[13]

This report also fills a gap in existing assessments of the telecommunications sector by focusing on equipment vendors, content delivery networks, and Internet service providers that operate backbone networks,[14] rather than the most visible firms that sell access to individual users.[15] While there are more than 282,000 wireless telecommunications companies and thousands more Internet service providers globally, the 20 companies in this study were selected because of their role as market leaders with significant market share in multiple regions.[16] Controlling a majority of digital communication in a region results in vast power over individuals' exchange of information. The report also provides analyses of the incentives, barriers, and catalysts that have shaped firms' behavior towards human rights.

Section 1 of the report begins with a background on Internet infrastructure, presenting the layers that comprise the Internet and the core components of the infrastructure layer. Next, Section 2 explores how Internet infrastructure impacts human rights and the responsibilities private actors have to respect and protect those rights, leading into a discussion of the UNGPs as the seminal standards on how businesses should protect human rights.

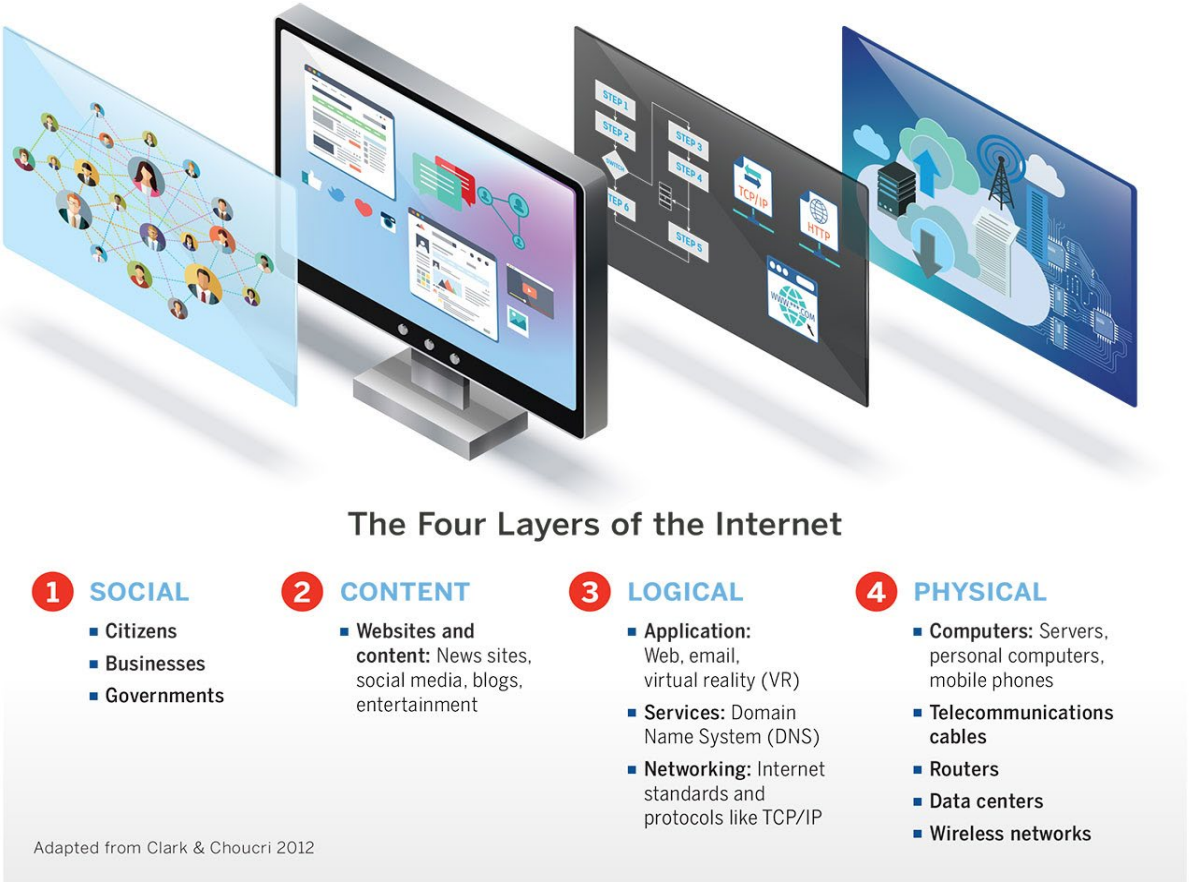
Section 3 outlines the research methodology behind this report, including a description of interviews conducted and desk research approaches. Based on this research, Section 4 presents findings, elaborating on two of the key drivers of companies adopting human rights standards. Specifically, reputational concerns regarding bad press and global public scrutiny drive UNGP adoption in many companies, while others are spurred to adoption by top leadership that has taken responsibility for human rights compliance. Next, turning to the majority of companies that have not yet adopted human rights standards, Section 5 explores the key barriers to adoption. Government demands were cited frequently as the primary barrier, but competition with non-compliant rivals also kept the bar low for many companies. Section 6 goes on to interrogate the role of competition in the Internet infrastructure industry, analyzing whether the degree and type of competition present is actually inducing greater adoption of human rights policies or preventing it. Finally, Sections 7 and 8 conclude with recommendations for civil society and businesses, respectively, that identify methods to overcome existing barriers and suggest pathways for more companies to adopt the UNGPs in their policies.

Background

What is Internet infrastructure?

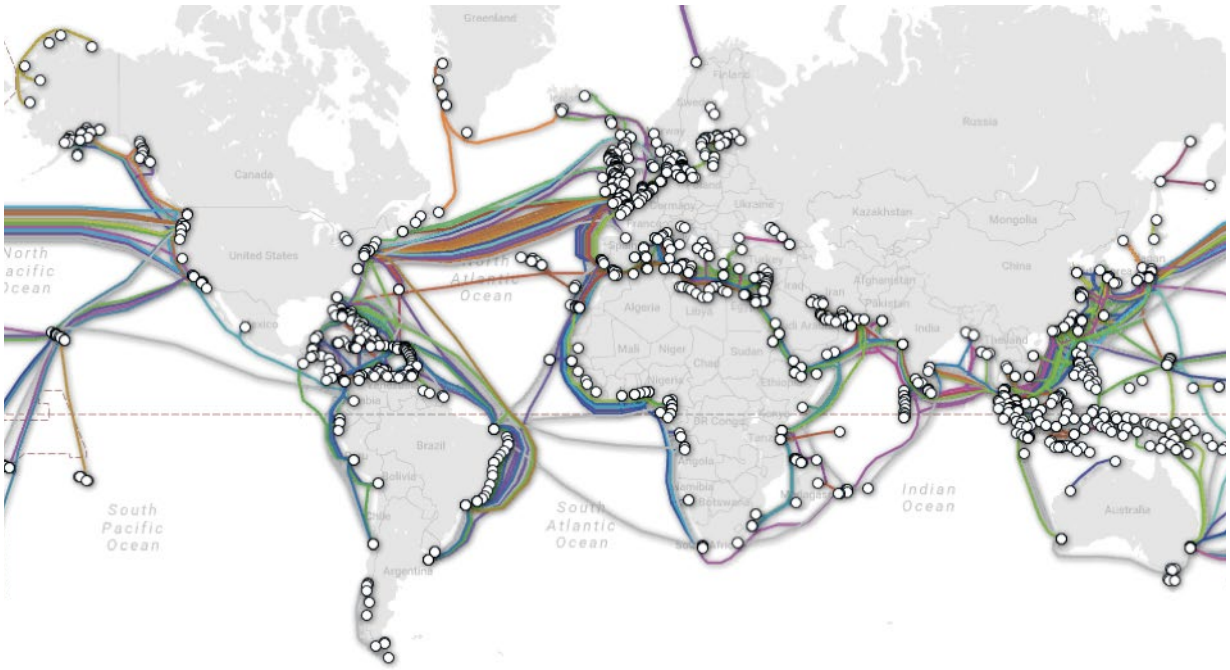
Internet infrastructure comprises the often-unseen physical and logical layers of the Internet that transport data to and from individual computers. This report focuses on physical infrastructure, the fourth layer in Figure 1, which spans the globe in an ever-expanding network of cables, satellites, towers, and data centers. Two particularly important elements of this infrastructure that deserve greater clarification are submarine cables and content delivery networks.

Figure 1



Submarine cables connect major ports through an expansive network of fiber optic cables stretched across ocean floors. These cables carry 99% of global Internet data by volume at any given time.[17] Controlling access to these networks therefore directly affects significant numbers of people. With the exception of military infrastructure, submarine cables are built, operated, and owned by consortia of private companies. While these companies are primarily telecommunications giants, large Internet companies like Google and Facebook are increasingly investing in infrastructure.[18] The submarine cable map in Figure 2 illustrates both the global breadth and unequal dispersion of cables as of October 2017.[19]

Figure 2: Submarine Internet cables



Content delivery networks (CDNs) improve the functionality of the physical layer of the Internet across distances. CDNs are distributed networks that improve the availability and speed of content delivery by locating proxy servers and data centers in relatively closer geographic proximity to end users, as shown in Figure 3. CDNs are paid by websites, media and e-commerce companies to deliver content to end users. In turn, CDNs partner with the Internet service providers and network operators to host servers. CDNs also provide a valuable security service to websites by securing a proxy of the web content from many types of outside attack, such as Distributed Denial of Service (DDoS) attacks. CDNs may make public commitments to be "content agnostic," meaning they remain neutral to the type of content they service, though this is not always the case (see: page 19). When CDNs exercise the power to pick and choose which websites to service, some websites receive protection and faster service, while unprotected sites are more vulnerable to takedown by malicious actors. For many contentious or political websites, the loss of protection by a CDN can enable censorship by those who disagree.

Internet service providers (ISPs) are companies that connect individuals with the complex infrastructure of wires, cables, and satellites that enable them to "go online." While emerging community providers represent an alternative form of digital inclusion, playing an important role in diversifying the Internet access pool and contributing to plurality and diversity of Internet connection models, the vast majority of Internet users connect through ISPs. As such, these providers act as a gateway between individuals and their enjoyment of human rights.

Governance of Internet infrastructure

Physical infrastructure is generally subject to local jurisdiction, similar to roadways or ports. There is no global body with binding legal oversight over Internet infrastructure. There are, however, four relevant global institutions that contribute to Internet governance—defined as shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.[20] The oldest is the International Telecommunications Union (ITU), a multilateral UN body dating back to 1865 when it was a telegraph union. The ITU facilitates much of the coordination on the physical layer between governments and businesses. Other Internet governance bodies have subsequently emerged to ensure interoperability of the various layers, standards, and protocols of the Internet, including the Internet Engineering Task Force (IETF) and the International Corporation of Assigned Names and Numbers (ICANN). These multistakeholder fora bring together governments, businesses, technical experts, and civil society to negotiate the future of the Internet. Unlike traditional governing bodies that work on strict majority voting practices, Internet governance bodies often run on "rough consensus" and voluntary adoption of norms.[21] This atypical governance model developed both culturally from the engineers who pioneered the Internet, and out of necessity to allow for experimentation and innovation.

How does Internet infrastructure impact human rights?

In the 21st century, the Internet has become indispensable to the exercise of fundamental human rights. The Internet is a gateway for freedom of expression, assembly and association, education, and access to information for nearly four billion people living in every country and territory on earth.[22] The Internet has also become a conduit for delivering essential public services from states to their citizens. Conversely, online expression is increasingly censored and access to information restricted through throttling or blocking. Meanwhile, privacy is under serious threat from government mass surveillance and the vast amounts of personal data collected by private companies.

Internet access is increasingly mediated by private companies. Many nationalized networks or parastatals with government control have been privatized since 1990. While private ownership has had positive effects for many Internet users, expanding access and modernizing networks to increase speed, end-users do not have power to hold these private actors accountable as they might an elected government. The private owners of network infrastructure have the power to determine when users can "go online", or not, and what content users can see. As one company representative noted, "If you sell networks, you also, intrinsically, sell the capability to intercept any communication that runs over them."[23]

Infrastructure is particularly vulnerable to abuse because of its invisibility, allowing manipulation by private actors and governments alike. Findings from interviews with experts and corporate executives revealed that threats to users' rights most often arise from governments requesting access to personal data or ordering restrictions

on access to content that private providers are forced to comply with. Increasingly, however, private providers unilaterally restrict rights by filtering online content by default, mishandling private user data, charging different prices for different content, or throttling the speed of access for certain users.[24] These violations come in a wide variety of forms, as described by the UN Special Rapporteur for Freedom of Expression in his June 2017 report:

> "What governments demand of private actors, and how those actors respond, can cripple the exchange of information; limit journalists' capacity to investigate securely; deter whistleblowers and human rights defenders. Private actors may also restrict freedom of expression on their own initiative. They may assign priority to Internet content or applications in exchange for payment or other commercial benefits, altering how users engage with information online. Companies that offer filtering services may influence the scope of content accessible to their subscribers."[25]

There is ample evidence of such limitations in India, where the Internet was shut down 54 times between January 2016 and September 2017.[26] Rather than being due to technical failure, most of these shutdowns were initiated by governments calling on regional ISPs and telecommunications companies ("telcos") to shut off or otherwise limit access to the Internet until further notice. These government orders are not always written or formalized: when an Indian journalist interviewed a private ISP about their process for engaging with shutdown orders in Kashmir, the ISP representative replied "we just get a call. All an operator needs to do is push a button and the signal strength goes down."[27] Private companies justify their compliance as simply following local law — if they do not, they risk losing their license to operate. Ironically, the state-owned Internet and telecommunications provider in India has much more rigorous due diligence to complete before their network is disabled, making it the more reliable network provider of choice for many businesses.

Governments most frequently justify intervening in Internet infrastructure for reasons of "public safety" and "stopping rumors", according to a study by Access Now.[28] In practice, shutdowns often occur when there is a risk of political instability, such as around an election or high-profile court case. Ongoing violations such as network surveillance and censorship are also justified on vague national security and/or public safety grounds.

There are four important points of differentiation to consider when assessing human rights violations that happen on Internet infrastructure:

1. **The instigator** — government or private actor — and point of origin will determine where and how to best address the violation.

2. **The type of violation** can vary between a full shutdown of the Internet, throttling of access speeds, blocking of certain websites or IPs, prevention of the use of encryption or anonymity, or more advanced censorship and filtering of certain content.

3. The speed with which an order is executed varies greatly, and due diligence processes or the requirement of formal court orders may provide valuable time to contest these decisions.

4. The willingness of the private actor to comply with a government request can signal opportunities for collective action or legal challenges. While some companies are willing participants, others acquiesce with a degree of protest or ignore parts of the request.

The private sector's responsibilities

Businesses operate under highly varied local laws, which may be relevant to human rights. For example, many jurisdictions, including the European Union, African Union, and much of Latin America, have adopted data protection laws; more than 50 countries have signed the Data Protection Convention of 1981.[29] At a global level, however, businesses are not legally bound to meet the standards of international human rights laws or treaties. While there have been numerous attempts over the last five decades to make such texts legally binding, these met with failure due to misaligned priorities between businesses, governments, and human rights advocates.

Given this history of gridlock, the degree of consensus built around the United Nations Guiding Principles on Business and Human Rights (UNGPs) in the last decade is remarkable. Unlike a legally binding treaty, the UNGPs are a set of voluntary universal standards for states and businesses. The UNGPs are significant because they define the first, authoritative set of international standards for businesses regarding human rights.[30]

The development of the UNGPs was led by Professor John Ruggie, who was appointed Special Representative to the Secretary General of the UN in 2005 to recommend a compromise for transnational corporations and human rights. By 2008, Ruggie developed the "Protect, Respect, Remedy" framework that defines the UNGPs. This tripartite framework proposes (i) state duty to protect human rights, (ii) corporate responsibility to respect human rights, and (iii) the need for both to collaborate in the provision of remedy for victims of human rights abuses.[31] The UNGPs garnered unprecedented support from the business community through almost 50 consultations and collaboration on the development of the text. There is high-level political support as well; the UN Human Rights Council unanimously endorsed the UNGPs in 2011. Since then, 19 states have published National Action Plans to implement their duties under the UNGPs in national legislations with another 30 in progress.[32] Simultaneously, hundreds of companies have formally committed to uphold their responsibilities under the UNGPs. While the evidence on translating the UNGPs into beneficial human rights impacts is inconclusive at best, the widespread nature of their adoption has generated greater awareness and momentum towards corporate reforms.[33]

Research methodology

The findings in this report are based on primary and secondary qualitative research conducted between September and December 2017. To establish context on Internet infrastructure governance standards and human rights impact assessments, a series of interviews were conducted with experts from academia, civil society, and international organizations that contribute to Internet governance. Based on expert recommendations, the scope of this study was limited to three important components of Internet infrastructure: internet service providers, content delivery networks, and network equipment vendors. This included telcos that operate significant amounts of broadband infrastructure. These physical components of the Internet are often overlooked in conversations about human rights, which have focused on the content or application layer of the Internet. These three infrastructure components were selected amongst the many infrastructure actors — hosting and domain providers, Internet exchange points, registrars, registries, etc. — because they have particularly high levels of privatization and consolidation, whereby private companies have significant influence over end users.[34]

A sample of 20 companies was chosen based on selecting "influencers" or market leaders whose actions would be most likely to influence their peers. Characteristics considered when identifying "influencers" included geographic breadth, market capitalization, and number of customers served. A few were selected for exhibiting what were hypothesized to be "market leading" characteristics or best practices in the field of human rights, including adoption of the UNGPs and implementation of Human Rights Impact Assessments (HRIAs).

Desk research was conducted to analyze publicly available corporate policies, annual reports, economic performance metrics, and human rights compliance data released by the 20 corporations. Findings were arranged into a matrix to facilitate comparison and pattern identification. Next, interviews were conducted with executives from 10 of these corporations to gather more nuanced perspectives on corporate decision-making, internal drivers, and perceived barriers. Interviews were structured depending on the type of infrastructure provided and included discussion of corporate human rights policies and practices, due diligence processes, privacy, freedom of expression, and access to remedy. Finally, process tracing was used to analyze corporate actions and decisions along a linear timeline. The tracing correlated the timing of a company undertaking human rights policy development — an announcement of compliance with the UNGPs, conducting an HRIA, publishing a transparency report — with the timing of a major external event — an Internet shutdown, a new national security law, or a major disruption of service. Relevant external events may have affected multiple companies, such as the passage of a law, or a single occurrence affecting one company. External events also included public advocacy in the form of civil society campaigns or private communication that raised reputational concerns for the company.

The findings from the process tracing, interviews, and desk research are purely illustrative observations and are not intended to demonstrate statistical significance or represent company positions. Information published in this report has been obtained with the free, prior and informed consent of all participating stakeholders. For a complete listing of companies studied, please reference Appendix 1.

Findings: Key drivers of adoption of human rights standards

Adoption of human rights standards by corporations has unequivocally increased in recent years. Understanding the drivers, or catalysts, of this phenomenon is valuable to human rights advocates who seek to expand adoption to the millions of businesses who have not yet sought to incorporate human rights standards into their policies and practices. "Adoption" is defined for the purposes of this study as the initial announcement by a corporation of compliance with an international human rights standard in publicly accessible corporate policies. This study measured adoption of the UNGPs, in particular, as foundational guidelines for respecting human rights in business.

The quality of adoption, an important consideration, was gradated on the basis of how each human rights standard was embedded into corporate policies, the transparency of the policy and practices, accountability in carrying out policies through executive oversight or external mechanisms, and the day-to-day integration of the standard into corporate practices. For example, a press release declaring adoption of a standard without subsequent evidence of the standard in corporate policies or practices did not count as adoption. Conversely, recognition of standards within multiple corporate policies and updates on performance vis a vis these standards in company annual reports signaled strong commitment. The highest quality of adoption was demonstrated when corporate practices, such as internal hiring practices or due diligence processes, were designed in accordance with international standards and audited regularly by independent third parties.

Primary driver of adoption: Reputational concerns

Observations from this study suggest that corporate policy changes are triggered when a combination of reputational considerations and motivated internal champions are activated by a catalyzing event. Corporate decision- and policy-making are often complex, layered procedures requiring a significant commitment of time and broad input, making it nearly impossible to attribute one primary driver of a policy. This is particularly true for large multinational telecommunications corporations where policy-making can span many departments, continents, and years. The key question for human rights advocates is: what are the most common catalysts that contributed to positive policy changes?

This study considered a number of factors influencing corporations, including stock prices, investor pressure, board relations, subsidiary autonomy, competitor behavior, organizational structure, primary consumer population, and media attention. Two clear patterns emerged from the data.[35]

First, corporations tend to react quickly and decisively to public scandals and negative attention in the media. A strong correlation was observed between the publication of

a scandal regarding a human rights violation and companies adopting human rights standards. Regardless of the type of violation, publishing a new privacy policy or commitment to human rights standards signals corporate intentions to avoid a repeat misstep. The correlation between scandals and human rights adoption was made even clearer in some instances where a particular violation was addressed with a targeted policy that involved partial adoption of the UNGPs. For example, after the Snowden disclosures in 2013 exposed collaboration by ISPs and telcos with the U.S. National Security Agency (NSA) that violated users' privacy rights, all U.S.-based ISPs and telcos in this study began publishing transparency reports within the next year.

The Nokia Siemens Networks (NSN) scandal in Iran offers a clear illustration of negative press driving corporate policy change. In 2009, The Wall Street Journal found that NSN was complicit in the Iranian government's violent crackdown on peaceful protesters and journalists in the Green Revolution.[36] Following the story, many consumers worldwide boycotted Nokia products.[37] NSN responded by noting it had provided "lawful interception» capabilities to the country's operators but acknowledged that it should not have sold monitoring centers to Iran, halting all work in that area and then divesting that part of its business. Subsequently, NSN became one of the first companies to adopt the UNGPs when they were published in 2011 and has included details on operations in authoritarian states in its annual report every year since 2011.[38] Nokia now has a dedicated Human Rights Group and is a leader amongst its peers for robust human rights policies and practices.

In some cases, a scandal on its own is insufficient to compel adoption. In many of these cases, heightened media attention and public scrutiny by civil society after a scandal can induce companies to be more sensitive to reputational damage. The majority of cases observed involved a human rights abuse overseas in a corporate subsidiary or partner, which subsequently triggered public outcry in the region of the corporation's headquarters. Sustained attention in public media and demands for changes by civil society appear to influence corporations' calculus regarding the costs and benefits of adopting human rights standards. Thus, while public scrutiny and media attention do not always lead to changes and certainly not in isolation, they are often important drivers.

To preempt bad press and reputational damage, many companies join industry groups to ensure their policies and practices match the level of commitment of their peers. In 2009, the Global Network Initiative (GNI) was formed to enhance collaboration on accountability between technology companies, universities, and civil society organizations in order to protect freedom of expression and privacy online.[39] Both Internet content providers (e.g. Google, Facebook, Yahoo) and telecommunications companies (e.g. Telia, Orange, Vodafone) took part in the organization's creation. Once the terms of membership became set, including a biannual intensive third-party audit, all participating telcos declined to join, while Internet content providers did. Based on conversations with both groups of companies, the decision to join GNI appeared to hinge on the amount of public attention directed at the company's actions. Content platforms in the U.S. — which were starting to come under intense scrutiny for hate

speech, violence, and other forms of content permitted by 2009 — all joined while telcos in Europe outside the public spotlight did not join.

This began to change in 2011 when the UNGPs were adopted and a number of influential telcos came under fire for violations by their global subsidiaries during the Arab Spring uprisings. In January 2011, Vodafone facilitated the shutdown of the Internet in Egypt for five days during the Tahrir Square protests through Vodafone's Egyptian subsidiary.[40] Vodafone also complied with requests to send its Egyptian customers pro-government messages on its network. There was a surge of condemnation from civil society and the public in the media for this act of complicity in suppressing free expression and access to information. Vodafone reacted by meeting with civil society advocates, changing its executive leadership, and developing human rights-oriented policies.[41] Since the Arab Uprisings, other major telcos have also attracted increased scrutiny regarding policies and practices in their global subsidiaries, and many followed suite by publishing transparency reports and joining the Global Network Initiative, which represent steps towards full UNGP adoption.

Notably, the effect of scandals and negative attention on driving UNGP adoption was only consistently observed for companies with a customer base comprised primarily of individual consumers, or business-to-consumer ("B2C") companies. Conversely, negative attention did not appear to have a consistent effect on companies whose primary customers are other businesses, or business-to-business ("B2B") companies. For this study, B2B companies include backbone ISPs, CDNs, and network equipment vendors that sell primarily to other businesses.

B2B companies in this study that were implicated in a human rights scandal were significantly less likely to adopt changes to company policy than B2C companies, even when there was significant negative media coverage. For example, Cisco has continued to deny allegations since evidence was leaked in 2008 detailing how Cisco network routing equipment was designed specifically for use by the Chinese government to prosecute Falun Gong members. To date, Cisco has not publicly changed course because of this scandal and continues to fight the allegations in the courts. This correlates with the understanding that public-facing companies are more sensitive to reputational concerns because consumer trust is more critical to their business model than to companies who primarily sell to other businesses and governments. Policy-makers in some B2B companies with less public visibility noted that their hesitation to draft new policies was a lack of "public impetus."[42]

Secondary driver of adoption: Top-down accountability

When leaders in the C-suite[43] and corporate boardroom tackle a problem (or have their own jobs on the line for a problem), solutions can come quickly. In the case of addressing potential human rights abuses, top leadership can be a decisive driver for adopting robust policies and practices. Responsible top leadership alone is generally insufficient to drive policy adoption, but the critical role of champions at the top has been demonstrated as a significant pattern. Champions have proven valuable for both reactive decisions to adopt human rights — translating criticism after a scandal

into momentum for change — and proactive decisions to reduce corporate risk before scandals occur by embedding human rights protections into corporate policy and practice.

It is not surprising that internal champions for change in positions of power can make a big difference — this has long been substantiated in public policy literature.[44] The contribution of this report is the role that organizational structure can have on driving policy change and implementation. This is different from the mere endorsement of a policy by an executive. Findings show that it matters instead who in the organization is ultimately responsible for developing and enforcing the policy, and where in the organizational structure they sit. A policy overseen by top executives in the C-suite was found to have a significantly stronger impact on corporate practices than a policy hived off into an administrative branch such as Human Resources or decentralized to local subsidiary offices. The weakest level of human rights policy development was found in companies with human rights oversight committees that only met periodically. NTT Communications in Japan has a human rights education committee that meets biannually, and while this committee reports directly to the board, its efficacy and responsiveness is limited by this organizational design.[45]

In one laudable example, the CEO of MTN, a South Africa-based global telco and ISP, institutionalized a subcommittee on the Board of Directors committed to social and ethical concerns. In 2013, the subcommittee approved a human rights policy that is based on the UNGPs and UN Declaration on Human Rights. The subcommittee had a human rights impact assessment conducted in 2016, subsequently establishing an annual risk assessment specific to digital human rights risks and a human rights toolkit developed with guidance from the Access Now Telco Action Plan, the Global Network Initiative, the Institute for Digital Human Rights and Business, and the Business and Human Rights Resource Centre, among others. The toolkit includes a decision tree for handling third-party or government requests in balance with human rights obligations. MTN has since moved to embed the policy and risk assessment recommendations by changing MTN's organizational structure, hybridizing responsibility for managing human rights incidents between a senior centralized team and country-level Issue Management Councils comprised of the country CEO, Chief of Corporate Services (Legal), and head of business risk management, among others.[46]

The importance of top leadership involvement makes sense intuitively; when a company consistently dedicates valuable executive time and clout to an issue, it signals the importance of the issue to its employees. It also suggests that violating such a policy would be costly. For human rights policies or compliance checks coming from lower levels of authority, or from groups that meet only periodically, the signal sent is that this issue — human rights — is not a company priority.

Leadership support for new policies can also be a double-edged sword. Changes from the top can move quickly and sometimes occur before thorough consideration of the unintended consequences or analysis of precedent. The case of Cloudflare, a leading American CDN, demonstrates the double-edged sword of leadership taking unmitigated responsibility for human rights.

At Cloudflare, policies and procedures for sensitive issues like government takedown requests tend to be kept informally in the heads of executives and the legal team. Given its size and stage of development,[47] Cloudflare expressed a fear that codifying evolving practices into company policy would mean losing flexibility to approach problems on a case-by-case basis. The desire for flexible decision-making is common amongst early-stage companies, particularly in industries that reward rapid experimentation. While flexible decision-making does not imply arbitrary decisions, in a privately-held organization it does imply that ultimate decision-making power and accountability lie in the hands of the leader. The public blog posts of Cloudflare's CEO laid out the company's stance on issues like content neutrality,[48] in lieu of formal policies or commitment to international standards. Without the checks of formal policy or processes, however, such flexibility can also enable unchecked executive decisions that can affect the rights of millions of end users.

This is precisely what happened in August 2017 when Cloudflare made headlines for a seemingly arbitrary reversal on its content neutrality stance. Cloudflare had long differentiated itself from competing CDNs for being staunchly content neutral, with Cloudflare's co-founder and CEO, Matthew Prince, vocally defending the company's principles in blog posts. In a post on freedom of expression in 2013, Prince wrote, "A website is speech. It is not a bomb," and concluded that, "no provider has an affirmative obligation to monitor and make determinations about the theoretically harmful nature of speech a site may contain."[49] Four years later in May 2017, a ProPublica exposé revealed that under the auspices of content neutrality, Cloudflare had hosted websites of terrorist groups and neo-Nazis, sparking internal discussions on content neutrality.[50] However, it was the white supremacist "Unite the Right" rally in Charlottesville on August 12, 2017 that marked a turning point in corporate positioning, as Cloudflare and other Internet infrastructure providers faced mounting public pressure to stop servicing websites of neo-Nazi organizations.

Cloudflare's CEO faced a Catch 22 dilemma confronting many Internet infrastructure providers today.[51] He ultimately decided to revoke service for the Daily Stormer, mirroring the decision made by a number of other companies, including the domain registrar GoDaddy.[52] While this seems to many an ethical decision, Prince acknowledged that this choice to limit speech, even if neo-Nazi speech, "sets a dangerous precedent when a company that most have never heard of is effectively deciding what can and cannot be on the Internet."[53] What made Cloudflare's decision more troubling, however, is that it did not rely upon an internal policy, terms of service agreement, or international norms to guide its response to the violent speech. Rather, the decision was grounded in the personal whims of its executives.

In an internal letter to Cloudflare employees the day of the decision, Prince wrote, "Let me be clear: this was an arbitrary decision… Literally, I woke up in a bad mood and decided someone shouldn't be allowed on the Internet." In anticipation of the critique of this decision, Prince noted, "No one should have that power."[54]

Internet company executives are increasingly forced into unenviable positions to make complex ethical decisions. Accountability mechanisms for executive discretion to set de facto policies can lower the stakes, making the decision less unilateral and personal. Published corporate policies can also make executive actions more predictable and transparent for the public, limiting backlash over unexpected decisions. Most importantly, publishing an explicit, transparent policy allows those with grievances a clearer understanding of what they violated and how they may seek redress. It is imperative that Internet infrastructure companies, particularly a company as powerful as Cloudflare, which handles 10% of all Internet requests on their network, limit the unchecked discretion of leaders over human rights to avoid decisions driven by personal values. Instead, companies should navigate challenging ethical decisions with the consistent guidance of a human rights policy grounded in international standards. Civil society also has a vital role to play in building consensus to define what it means for an infrastructure provider to act ethically in contexts where human rights norms appear to be in conflict.

Findings: Key barriers to adopting human rights standards

The majority of Internet infrastructure providers have not adopted policies that meet even basic international norms for protecting human rights. While the primary barrier to adoption was found to be government interventions, other common barriers from a business perspective include the costs of instituting new compliance mechanisms, competitive pressures, and a lack of expertise in determining the relevance of human rights to corporate business practices, let alone the appropriate response to violations. Organizationally, companies may also face internal barriers related to employee attitudes, a lack of understanding of the relevance of human rights abuses to company operations, or weak change management.[55]

Primary barrier to adoption: Government demands

As data from digital communications becomes an ever more prevalent element national security operations led by law enforcement and intelligence agencies, governments are increasingly demanding sweeping access to user data. Under the threat of losing licensing agreements, companies are often compelled to sign agreements with governments to share private user data, pressured to comply with court orders to block or remove content, or obligated to meet other unwritten government requests. Governments have also forced Internet infrastructure companies to comply with Internet shutdown or blocking requests, directly restricting users' access to information and freedom of expression. Troublingly, such government demands are increasingly coming from authoritarian regimes and democracies alike. Prominent recent cases of government demands violating the rights of users came from democratically elected governments in India,[56] Bangladesh,[57] and the United States.[58]

When companies face the choice between complying with binding local laws or losing their business license in efforts to uphold international human rights standards, the economic calculation is clear. By and large, businesses comply with local government requests or legislation, even when national law directly violates international human rights law. Governments understand a company's priority is to retain businesses licenses and remain in operation, which allows leverage to enact controversial measures such as provisions permitting government discretion over shutting down the Internet, businesses often comply with local government request.[59]

In some cases, however, when local governmental abuses are severe enough that they could cause reputational risk, or the economic profitability of operating in a given country is unclear, businesses may elect to violate local law or pull out of the country altogether. In the case of Telia, a global telco based in Sweden, they faced over $1B in fines to regulatory authorities in the Netherlands, Sweden, and the US for complicity in Eurasian government corruption. Telia subsequently decided to pull out of seven Eurasian markets. In efforts to prevent a repeat occurrence and comply with international human rights standards, Telia contracted an independent third party to

conduct a series of intensive human rights impact assessments (HRIAs) on all of its operations. While the challenge of complying with problematic local laws in Eurasia did not trigger reflection on their own, the financial repercussions and public scrutiny after the pullout led Telia to prioritize international human rights standards when in conflict with national laws. Today, Telia is a market leader in the telecommunications space for their robust implementation and transparent reporting of HRIAs conducted independently by a third party.[60]

The paradox of government relations

Executives acknowledge that they face a paradoxical relationship with governments. On the one hand, corporations need government mechanisms to limit abuse by nefarious actors and to restrain unfair competition. On the other hand, governments pressure companies at times to facilitate government ambitions to surveil, censor, or block networks. While most often couched as law enforcement, such requests often violate the rights to privacy and freedom of expression.

Compounding this tension, government requests to Internet infrastructure companies may come with a "gag order." Gag orders are court orders preventing the company from telling anyone about the existence of the government request for a given period of time. Companies argue that gag orders limit their ability to report their actions transparently and comply with human rights standards. Governments, meanwhile, contend that gag orders are necessary to investigate criminal suspects without tipping them off.[61]

In response to this paradox, Internet companies studied have developed three types of responses, ranging from the most accommodating of government requests to the most resistant:

i. Privacy policy exception clause: In efforts to comply with government data requests, while also maintaining a reputation among customers for respecting privacy, many companies have developed privacy policies with an exception clause. This clause warns users that the company will comply with government requests for data, even in cases when they violate user rights to privacy and compliance with UNGPs. The exception clause has been developed as a mechanism to signal the company's intention to meet international standards by having a privacy policy, while not challenging local law.

ii. Transparency Reporting: Since the Snowden disclosures, companies are increasingly using transparency reports to communicate what user data has been requested and by whom. By exposing the origin of surveillance requests, companies can shift the responsibility for surveillance to governments. Many companies now publish biannual reports listing all requests for information from governments.[62]

iii. Active management approach: Some companies choose to confront government requests that violate international norms. Such challenges may be also discrete, manifesting during contract negotiations with the government. Companies have successfully negotiated clauses to deter dual use of technologies for unethical ends or conducted strict due diligence processes to prevent human rights abuses by acquisitions. For example, Nokia includes the clause "Nokia will not knowingly provide technology or services for the purpose of limiting political discourse, blocking legitimate forms of free speech, or otherwise contributing to activities that are not consistent with internationally recognized human rights standards" in its annual report.[63]

Governments can make or break a company's efforts to adopt the UNGPs. To understand the significance of government policies on corporate human rights compliance, it is illustrative to compare the European General Data Protection Regulation (GDPR) with the United States NSA Surveillance Program. Since the passage of the GDPR in 2016, companies around the world have modernized data systems, changed data retention processes, and sought legal counsel in an effort to comply with the new legislation. Yet despite the millions of euros upgrading internal data processing processes has cost companies, many still express support for the GDPR as a welcome harmonization of privacy and cybersecurity provisions.[64] In contrast, the enactment of the NSA surveillance program in 2001 requested that US companies place surveillance equipment in their devices and telecommunications junctions to conduct deep packet inspection of customers' private communications. Companies were also requested to hand over call metadata without a warrant, both requests that would severely violate users' right to privacy and degrade corporate commitments to human rights.[65] In each case, government requests to companies — whether legally mandated or coerced — changed companies' behavior significantly in relation to human rights commitments.

When governments require corporate complicity for human rights infringements, the UNGPs can be partially adopted at best. To operate in countries where governments place significant demands on corporations to restrict rights, it is all but impossible to embed the UNGPs in a meaningful way. Companies have traditionally responded to such pressure by putting the UNGPs into practice only where company interests align with best practices. For Internet companies, the UNGPs are most often referenced in corporate policies regarding freedom of expression or supply chain transparency, two issues where Internet companies' brand reputation and quality assurance align with upholding human rights.

Assessing the role of competition: A driver or barrier to adoption?

Analyzing the economic characteristics of an industry can offer insights into past company decision-making and future trajectories. An individual firm's behavior is shaped by its field of competitors, buyers, suppliers, and threats from substitutes and new entrants. An analysis of these factors below clarifies why the competition in the Internet infrastructure provider industry is so intense, and what intense competition means for the likelihood of human rights policy adoption.

Economic analysis of the Internet infrastructure provider industry[66]

The Internet infrastructure provider industry (hereinafter "the industry") is in a high growth period. Because economic analyses do not typically group these companies together, this analysis takes in aggregate companies such as telcos, ISPs, and network services industries. ISPs grew 6.7% in 2016 and accelerated to 8.2% growth in 2017. Because organic demand is driving growth, profits rose to 13.7% of revenue in 2017.[67] This high profitability and growth means it is an attractive industry for new entrants.

The main reason behind the industry's booming growth rates and profitability is demand from emerging markets. With 52% of the world still without consistent Internet connection, there is rapid expansion in markets in South Asia and Africa especially, as well as continued expansion in Southeast Asia and Latin America. The growth in more developed markets is driven by demand for high-end technologies including fiber and high-speed broadband.

Geography matters immensely for competitiveness of physical infrastructure. While the industry is not consolidated on a global scale, regional oligopolies control the vast majority of infrastructure worldwide, preventing optimally competitive markets. Price competition has declined in the most developed, highly concentrated markets as they become saturated and Internet access becomes a commoditized service. Price competition is dampened by companies offering differentiated data packages, bandwidth speeds, and commercial service offerings. Some companies are choosing to compete through integration and consolidation of different forms of communications services, such as wired and wireless Internet, telephony, and television. Such bundling can cut costs while consolidating the company's power relative to consumers and its competitors, raising competition within regional oligopolies.

A degree of differentiation, and subsequently heightened competition, is propelled by rapid technological advances in the industry. These advances have enabled increasing volumes of data to travel faster, fueling consumer preferences for higher speed streaming with more reliable services such as fiber to the premises. On the other hand, focusing on differentiation through high-end services is exacerbating the digital divide. High income, densely populated regions are serviced by ever-faster, more advanced

Internet technology, while operators in emerging markets often choose to avoid infrastructure-intensive solutions in favor of slower mobile broadband coverage.

Some governments, like South Korea, have invested in internet infrastructure to prevent the social and economic inequalities perpetuated by a digital divide. South Korean Internet is still big business, but a strong relationship between the industry and the government means that subsidies, low-interest loans, and funding packages have incentivized ISPs to ensure otherwise neglected communities across the country meet high-speed minimums without incurring losses.[68] Critics point out that these costs have been passed on to international ISPs that are required to pay non-market rates to interconnect with South Korean ISPs, driving some to route around South Korea and slow traffic.[69]

Around the world, the number of players in the industry is increasing at a rate of 3.2% per year, including an estimated 11,441 global Internet providers in 2017, and 12,924 projected by 2022. This growth is primarily in emerging markets where barriers to entry are particularly low. In some countries, recent privatization of nationalized telecommunications has meant companies have the advantage of acquiring existing infrastructure and customers. Despite a high degree of consolidation in some developed markets,[70] emerging technologies like fiber have made space for new entrants like Google Fiber. The performance of new entrants is a serious threat to the existing dominant players; economic analysts project that the four largest players globally will all see declining market share due to new entrants over the next five years.[71]

Industry stakeholder analysis: Consumers, suppliers, and substitutes

Unfortunately for end users, the glut of demand — combined with regionally concentrated oligopolies — means individual consumers have very little power. Consumers in many markets face a single, monopoly Internet provider or a few oligopolists. This is particularly true in the ISP industry in North America and East Asia. In the United States, more than 40% of the country has only one ISP option for Internet access, and there are even fewer options at higher speeds.[72] Because a home or office does not need multiple Internet connections, once the first provider connects the building, there is a high cost associated with switching the physical infrastructure to a different provider. This low ability for the consumer to shop between providers, results in "lock-in", where the first provider has significant power for a period of time over the consumer. This results in natural monopolies where companies are less affected by consumer pressure because consumers cannot credibly threaten to change providers.

Natural monopoly power in the ISP industry is enabling companies to consolidate regionally or expand into related industries. Corporate consolidation further diminishes consumers relative power. This is more than an effect of size; Harvard Business Review finds that "it's the combined effect of size, concentration, and, importantly, incumbent-friendly regulation on the healthy competition" that hurts end users.[73]

The suppliers of Internet infrastructure providers are much more competitive by contrast. Suppliers include hardware and wire manufacturers that build the physical components of network equipment or telecommunications infrastructure. These are much less consolidated industries than Internet infrastructure, comprising many small manufacturers or commodity providers. This fragmentation allows powerful ISPs and telcos to exercise leverage over suppliers.

Substitutes, particularly mobile broadband providers, pose strong competition. In many places, mobile broadband is a complementary service provided at increasingly competitive prices alongside Internet subscriptions. The proliferation of mobile devices, as compared to lower growth for laptops and desktop computers that rely on internet, is a threatening sign for the future of the internet industry. Moreover, as mobile broadband providers move away from the fixed-term subscriptions that internet service providers are sticking with, the mobile providers will likely win over consumers who wish to escape the "lock-in" effect of fixed-term contracts. A handful of the largest players are integrating across sectors, such as Verizon, operating both mobile broadband and Internet service provision, in a move that could significantly limit competition. Because of the intensity of competition and the importance of geography, two different forms of competition have emerged and influenced the development of human rights policies in two divergent trajectories.

Pro-social and negative competition

The psychological concept of "pro-social behavior" comprises the broad category of actions that help other people. While there is a debate as to whether motivations underlying the behavior must also be altruistic, there is growing consensus that organizations and businesses can also act "pro-socially", or for the benefit of others. Applied to competition, this means that one competitor's pro-social behavior induces its competitors to reciprocate, or compete, by also engaging in pro-social behavior. For example, one business may commit to increase scrutiny throughout its supply chain, inducing its competitors to also introduce new due diligence measures. Such mirroring occurs when an industry has intense rivalry and when one competitor makes a credible commitment to engage in pro-social behavior. A commitment becomes credible when it is public and costly to reverse, such as publishing a policy, investing in a new corporate social responsibility initiative, or signing a contract publicly with an industry group.

The findings from this study suggest that clusters of pro-social competition can emerge where a group of competitors all improve their human rights practices at around the same time as one another. For example, a group of seven telcos in Europe adopted the UNGPs and joined GNI at approximately the same time; transparency reports were published by the largest ISPs in US in 2014 together. When rivalry is intense, participation in private industry groups increases private information flows, decreasing the risk of a company acting alone, and increasing the ability for companies to act pro-socially in tandem.

On the other hand, negative competition manifests when one influential corporation sets a norm of non-compliance that permits, or induces, its competitors to follow suit. This can result in a race to the bottom, where standards in the industry revert to the "lowest common denominator." For example, when a particularly influential competitor openly cooperates in surveillance practices, it sets expectations that surveillance is a normalized, acceptable practice to maintain power in that industry segment.

In the market for network equipment, the American technology company, Cisco, questioned the need to adopt specific human rights norms after noting that their main competitor is Huawei, a notoriously non-compliant Chinese network equipment vendor. This effect was observed both for large rival corporations with dominant market share, as well as for smaller players.

The recommendations section below analyzes how strategic corporate decisions, including transparent reporting and third-party accountability measures, can catalyze an industry from negative competition toward pro-social competition around human rights responsibilities.

Recommendations for businesses

1. **Pair strong, transparent Terms of Service with strong, transparent implementation.** Terms of Service and other policies regarding users' rights should be rooted in international human rights standards. It is much easier to write a human rights-compliant policy, however, than to enforce one, and companies often find a gap between the ambition for responsible action and the capacity to enforce it. Companies should proactively allocate staff time and resources to implementing policies at the time they are written, ensuring bandwidth alongside other cyclical company functions. Leadership at the top should signal that the terms of service are meaningful by dedicating time to reviewing annual assessments of their effectiveness and transparently addressing violations of their terms.

2. **Partner with civil society organizations on HRIAs.** HRIAs can be affordable — they do not need to be conducted by expensive auditing or consulting firms to be credible. A number of nonprofits specialize in conducting human rights impact assessments. ARTICLE 19 and the Danish Institute for Human Rights (DIHR) have collaboratively developed a model for conducting HRIAs with Internet infrastructure providers which entails an internal questionnaire and guided interviews with relevant organizational points of contact.

3. **Embed HRIAs in corporate compliance practices with executive-level oversight.** Reporting for reporting's sake is a drain on resources. Instead, reporting should be streamlined as part of ongoing compliance practices and the results should feed directly into corporate decision-making and review processes. When companies embed human rights protections and HRIAs into regular practices, akin to an annual financial audit, they significantly reduce risk of a violation. Specifically, HRIAs can be embedded alongside robust legal compliance and due diligence processes. Embedding also entails having personnel responsible and accountable for the company's human rights performance. Specificity is important: rather than simply having "sustainability" or "legal" personnel, data shows it is more effective to have specific human rights compliance officers.

   Market leaders observed in this study made human rights an executive-level priority. Reporting for human rights impacts was overseen by a C-suite executive or council. To ensure accountability, they established either a Human Rights Oversight Committee on the Board of Directors or a cross-department Advisory Panel that meets quarterly to review human rights compliance. However, these practices are the exception, not yet the norm—the majority of companies in this study, as well as companies across sectors studied by the Shift Project, fail to clearly identify who is responsible for human rights accountability.

4. **Apply HRIAs annually throughout value chain and global subsidiaries.** Corporate compliance or legal teams often sit in headquarters and rarely have the capacity,

expertise, or executive buy-in to apply HRIAs across the entire company, even when violations of human rights have been identified in global subsidiaries. Just as companies conduct thorough due diligence prior to a merger or acquisition, internal human rights due diligence should be conducted thoroughly across all holdings globally, not only in corporate headquarters, and on an annual basis. Civil society organizations can assist by training staff on conducting due diligence or identifying appropriate third parties globally.

5. **Publish assessments publicly for benchmarking against competition.** Transparent reporting of human rights assessments, policies, and methods allows for more accurate benchmarking. Publishing publicly not only strengthens companies' own accountability, but it also helps the industry as a whole to have benchmarks. Transparent reporting of HRIAs helps avoid the "whitewashing" effect whereby corporations signal compliance rhetorically while failing to apply or meet substantive indicators in practice. Market leaders can also gain recognition from publicly describing their activities and implementation of human rights safeguards. Findings from this study suggest that publishing HRIA results can set a valuable precedent for the industry, and may spark pro-social competition that leads to improved practices by competitors. Currently, competitive industry benchmarking is hindered by the lack of transparent reporting after human rights due diligence occurs. While certain information collected during due diligence must be kept private to protect intellectual property, there is no reason an entire HRIA must be kept private. The benefits of publishing findings transparently outweigh the costs.

6. **Phase in human rights compliance to build internal buy-in.** Market leaders today often developed progressively more robust due diligence over the course of a few years. Typically, the first step is conducting private internal reviews of operations, before next contracting a third-party to conduct an official HRIA. The first assessment is often limited to the company's primary geography or headquarters, before subsequent assessments are conducted for global subsidiaries and supply chains.

7. **Ensure anonymous access to remedy for all stakeholders.** UNGP adoption is incomplete without its third pillar: redress for victims of human rights abuses. Even so, this essential ingredient is often forgotten. Corporations have not only the ability, but the responsibility to provide non-judicial remedies and anonymous grievance mechanisms for all stakeholders to voice concerns. "Stakeholders" comprise a category broader than shareholders and customers to include any individual or entity that a company impacts, including its neighbors and surrounding community, employees, and the natural environment. Provision of remedy is the most sorely lacking UNGP commitment, with only two of 20 companies studied offering anonymous remedy mechanisms for all stakeholders. Providing more comprehensive mechanisms for redressing grievances not only mitigates risk of complainants generating bad press, but it empowers users and improves customer relations.

Recommendations for civil society

Findings from this study present an optimistic outlook for the role of civil society by identifying both a need and specific avenues for engagement with corporations on human rights. Given the diversity of corporate human rights practices in the Internet infrastructure sector, civil society should employ a combination of carrots and sticks depending on each company and context. While some companies have demonstrated interested in meeting human rights standards and may simply require assistance in strengthening processes, others may require a push to understand the relevance and significance of end users' human rights at the level of Internet infrastructure.

1. **Monitor and reach out to corporations directly.** Numerous civil society organizations have proven the effectiveness of operating strategically in a "watchdog" role by monitoring corporate activities for abuses. In most cases of abuse, it is best for civil society actors to first engage corporations directly and privately once evidence of abuses is collected. Corporations have a strong interest in avoiding negative press or public scandal. Civil society can therefore have significant positive influence on corporate human rights practices by sending letters or meeting with corporations to identify violations and suggest corrective measures. Multiple companies in this study noted how private letters from Privacy International, Greenpeace, the Anti-Defamation League, and others had a strong catalytic impact, sparking internal dialogues that led to changes in corporate practices and policies. These letters were most effective when coupled with robust evidence of human rights violations, or potential thereof, and a willingness to either go public and publish or partner with the company in efforts to redress grievances.

2. **Partner with companies on defining human rights goals and identifying gaps.**

   There is a lack of clarity and consensus about how infrastructure companies should balance competing human rights interests. In cases such as the Daily Stormer removal, companies would benefit from clear guidance on how to address the tension between freedom of expression and moderating hate speech. Civil society can play an important role in helping to determine how human rights standards apply to different Internet actors and advocating for consensus around those positions.

   In practice, the process of human rights identification and prioritization is often conducted at the discretion of corporate executives and the process may not be transparent. This leads to concerns that corporate identification of salient human rights, while well intentioned, may be arbitrary, or at worst, purposefully obscuring more severe human rights issues.

   For example, AT&T self-publishes a materiality assessment, charting the perceived relevance of various human rights risks in relation to the company's

operations.[74] Unfortunately, no information is published about the process by which AT&T reached those conclusions or how it uses that assessment in its operations. Formalized, professional HRIA processes assist with identification and prioritization of salient rights as well as a process to identify and analyze gaps in internal policies. Civil society organizations with expertise in HRIA processes should partner with corporations to assist them with designing HRIAs credibly and ensure that they are addressing not just the most convenient, but the most pressing issues.

3. **Proactively offer companies assistance in conducting independent assessments.** Corporations rarely have in-house expertise on human rights, so offering to partner on the development of robust policies can benefit both parties. Some companies may lack an understanding of the importance or relevance of an HRIA for their business. For technology companies in particular, there is significant attention paid to upstream supply chain issues concerning conflict minerals and child labor, but much less understanding of downstream human rights issues. Civil society can play a vital role in clarifying why issues of privacy, freedom of expression, and access to information are vital considerations to be protected and assessed regularly by companies.

   Civil society can remind companies that enlisting an independent partner to conduct human rights assessments is vital both to enhance the credibility of the process and ensure that a subject-matter expert is engaged to mitigate risk. This can also raise the quality of the assessment. Where cost is a concern, civil society should clarify how the long-run benefits of human rights due diligence and reputational protection outweigh the costs of the assessment.

4. **Speak to corporations in their language**. The cultural divide between the human rights community and business community is expressed linguistically, meaning that messages from civil society may inadvertently convey negative connotations, go unheard, or be misunderstood. While civil society must not erase human rights concepts from their language, it is imperative they learn to code switch and meet companies where they are. For example, the meaning of "individual rights holders" is more familiar to a civil society member than a corporate executive and can be effectively reframed as "end users" or "customers." Though not an exact translation, "human rights" can sometimes be referred to as "minimizing harm" in order to start conversations about impacts. To communicate the relevance of human rights in a corporate setting, the language of "intrinsic values" or "universal dignity" may not resonate as well with corporate decision makers as the framing of "risk mitigation" and "legal compliance." Similarly, in order to convey the idea that protecting the rights of end users is within the scope of an infrastructure provider's responsibility, it is important that responsibility is carried throughout a corporation's value chain.

5. **Organize collective policy advocacy campaigns with corporations.** Given that government intervention present the most significant barrier to UNGP adoption, civil society can partner on policy advocacy to limit government interventions. Civil

society organizations have expertise to offer in the area of movement building and policy advocacy around human rights protection. Nokia, Google, and others noted that a significant draw of industry groups like the Global Network Initiative (GNI) is the ability to gain collective bargaining power in negotiations with governments.

Areas for further research

Role of investors

Investors hold significant influence over the actions taken by many corporations. In the past, investors have demonstrated the ability to positively influence companies to improve human rights practices. In 2015, a group of 84 investors managing over $4.8 trillion in assets publicly expressed support for the UNGP Reporting Framework for corporate disclosure on human rights. The investors explained that, "[o]ne of the drivers for this investor action is the growing risk of reputational damage to investors themselves if their risk management and due diligence procedures for assessing human rights risk are perceived to be weak."[75] While this is a laudable trend, these investors are still in the minority.

This study looked at the effect of human rights incidences on companies' prices in the New York Stock Exchange, where the majority of companies in the study are listed. The findings were inconclusive, suggesting that there is not a significant portion of investors who are responsive to corporate human rights violations. What role could investors play in driving corporate commitment to human rights? Is it possible that other stock exchanges already have a higher proportion of investors than the NYSE who are sensitive to corporate human rights violations? How can influential investors come to understand their influence on corporate human rights practices?

Role of competition

The dynamics of competition within an industry are complex, obscuring simple one-to-one correlations between measures of competition and internal corporate decision-making. However, evidence shows that the intensity and directionality of competition is a significant factor in the formulation of company policies. In the United States, 55% of Internet consumers have access to only one Internet service provider while a further 30% have a choice between only two. This extremely limited competition impacts the behavior by companies benefiting from monopoly or duopoly conditions.

It would be worthwhile to compare human rights adoption by companies with duopoly or monopoly control of a majority of service provision against those operating in more competitive markets to inform antitrust enforcement in the sector.

Role of non-corporate providers

This report focused on three influential internet infrastructure providers — network equipment vendors, content delivery networks, and Internet service providers. However, not all providers are this big or operate as private businesses. Smaller, non-corporate providers may offer alternative approaches to human rights compliance or incorporation of the UNGPs. Do organizations with a foundational commitment to sustainability and ethics — such as Greenhost, Riseup, 1984 and others — comply with the UNGPs better or worse than their corporate counterparts? Is differentiation

in compliance directly correlated with organizational design and a commitment to generate profit? A similar thread of inquiry could investigate how the type of infrastructure provided, whether a mass-market product like Internet broadband or individual add-ons like VPNs, correlates with UNGP adoption and compliance.

Appendix 1

List of companies in the study

a. AT&T
b. Bharti Airtel
c. BT Group
d. CenturyLink
e. Cisco
f. Cloudflare
g. Deutsche Telekom
h. Ericsson
i. Google
j. Huawei
k. Incapsula
l. MTN Group
m. Nokia
n. NTT Communications
o. Orange
p. Telefonica
q. Telia Company
r. Verizon
s. Vodafone

End notes

[1] Internet infrastructure providers include a variety of actors, including Internet Service Providers (ISPs), registries, registrars, hosting providers, Internet exchange points, and content delivery networks, to name a few. These will be described in depth in the background section.

[2] DeNardis, Laura. "The Global War for Internet Governance." Yale University Press, 2014, p. 2.

[3] Klonick, Kate. "The New Governors: The People, Rules, and Processes Governing Online Speech." Harvard Law Review, Vol. 131, April 10 2018, p. 1598-1669.

[4] Access Now. "Pulling the Plug on Free Expression: The Rise of Internet Shutdowns to Silence Dissent," 16 January 2018. https://www.accessnow.org/pulling-plug-free-expression-rise-internet-shutdowns-silence-dissent/

[5] "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect, and Remedy' Framework." Office of the United Nations High Commissioner for Human Rights, April 2011. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[6] These obligations are enshrined in Article 19 of the International Covenant on Civil and Political Rights (ICCPR). They explicitly affirm a commitment to uphold these rights at home and abroad, and across any form of media. 169 countries, including the United States, have ratified the ICCPR. The mandate of the UN Special Rapporteur promotion and protection of the right to freedom of opinion and expression describes these rights, which can be retrieved from: http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL.USA.24.08.17.pdf

[7] Internet Freedom is measured as the prevalence of different censorship methods including obstacles to access, limits on content, and violations of user rights across using 100 indicators. "Freedom of the Net 2017 Report," Freedom House, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017

[8] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." United Nations Human Rights Council, 30 March 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement

[9] DeNardis, Laura. "The Global War for Internet Governance," Yale University Press, 2014, p.123

[10] "Guiding Principles on Business and Human Rights," United Nations Human Rights Office for the High Commissioner, April 2011. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[11] "Human Rights Reporting: Are Companies telling Investors what they need to know?" Shift Project, May 2017. https://www.shiftproject.org/media/resources/docs/Shift_MaturityofHumanRightsReporting_May2017.pdf

[12] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion." United Nations General Assembly, Human Rights Council, 6-23 June 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement

[13] ARTICLE 19. "Getting connected: Freedom of expression, Telcos and ISPs," 2017. https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf

[14] Internet Backbone refers to large strategic data routes interconnecting other networks, similar to arteries of the body connecting veins. Backbone is also referred to as "trunk" network.

[15] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion." United Nations General Assembly, Human Rights Council, 6-23 June 2017, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement; "Telecommunications and Human Rights: An Export Credit Perspective," Institute for Human Rights and Business, February 2017, https://www.ihrb.org/uploads/reports/IHRB%2C_Telecommunications_and_Human_Rights_-_An_Export_Credit_Perspective%2C_Feb_2017.pdf; "Reforming Telecommunications in Burma: Human Rights and Responsible Investment in Mobile and the Internet," Human Rights Watch, May 2013, https://www.hrw.org/report/2013/05/19/reforming-telecommunications-burma/human-rights-and-responsible-investment-mobile

[16] Total companies count is based on companies within the OneSource Global Universe database. "Global Telecommunications Industry Report." OneSource, 2018. https://app.avention.com/industry/c24f0b81-2243-3f91-8934-e7ea15bce707#report/industry_summary

[17] Main, Douglas. "Undersea Cables Transport 99 percent of international communications." Newsweek. 2 April 2015. http://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072

[18] Burrington, Ingrid. "What's Important about Undersea Cables." The Atlantic, 9 November 2015. https://www.theatlantic.com/technology/archive/2015/11/submarine-cables/414942/

[19] "Submarine Cable Map." PriMetrica Inc., 5 May 2018, https://www.submarinecablemap.com/

[20] World Summit on the Information Society. "Tunis Agenda for the Information Society." International Telecommunications Union, 18 November 2005, http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[21] Cath, Corinne, et al. "Media Development in the Digital Age: Five Ways to Engage in Internet Governance." Center for International Media Assistance, 22 May 2017. https://www.cima.ned.org/publication/media-development-digital-age-five-ways-engage-internet-governance/

[22] ARTICLE 19 has articulated how the right to freedom of expression must be protected by telecommunications companies in its policy brief: "Getting connected: Freedom of expression, Telcos and ISPs ," June 2017. https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf

[23] Deep, Aroon. "How do Internet Shutdowns happen, and do they work?" MediaNama, 17 December 2017. https://www.medianama.com/2017/12/223-namapolicy-Internet-shutdowns-happen-work/

[24] ARTICLE 19, 2017, ibid.

[25] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion." United Nations General Assembly, Human Rights Council, 6-23 June 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement

[26] "Launching Stop: The Shutdown Tracker." Access Now. 16 November 2017 https://www.accessnow.org/keepiton-shutdown-tracker/

[27] Deep, Aroon. "How do Internet Shutdowns happen, and do they work?" MediaNama, 17 December 2017. https://www.medianama.com/2017/12/223-namapolicy-Internet-shutdowns-happen-work/

[28] "Launching Stop: The Shutdown Tracker." Access Now. 16 November 2017. https://www.accessnow.org/keepiton-shutdown-tracker/

[29] "Convention for the Protection of Individuals with regard to Automatic Processing of

Personal Data," Treaty 108, Council of Europe, January 1981. https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

[30] "Commission Staff Working Document on Implementing the UN Guiding Principles on Business and Human Rights - State of Play." European Commission, Brussels, 14 July 2015, https://ec.europa.eu/transparency/regdoc/rep/10102/2015/EN/10102-2015-144-EN-F1-1.PDF

[31] "Guiding Principles on Business and Human Rights," United Nations Human Rights Office fo the High Commissioner, April 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[32] "National Action Plans on Business and Human Rights." Business & Human Rights Resource Centre, 2018. https://www.business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-governments/by-type-of-initiative/national-action-plans

[33] "Human Rights Reporting: Are Companies telling Investors what they need to know?" Shift Project, New York, May 2017. https://www.shiftproject.org/media/resources/docs/Shift_MaturityofHumanRightsReporting_May2017.pdf

[34] It should be noted that a degree of consolidation is also present among registrars and regional Internet registries.

[35] Evaluation of potential catalysts involved gathering insights from corporate executives, then comparing external events in a timeline beside improvements in corporate human rights policies and practices. This process tracing procedure was used to identify which events may have correlated with or contributed to adoption of the UNGPs.

[36] Rhoads, Christopher and Loretta Chao. "Iran's Web Spying Aided by Western Technology." The Wall Street Journal, 22 June 2009. https://www.wsj.com/articles/SB124562668777335653

[37] Zetter, Kim. "Consumer Boycott Nokia, Siemens for selling to Iran." Wired Magazine, 23 June 2009. https://www.wired.com/2009/06/nokia-siemens-boycott/

[38] Nokia Annual Report 2016 (Form 20-F). p. 138 https://www.nokia.com/sites/default/files/files/nokia_20f16_full_report_en.pdf

[39] "About GNI." Global Network Initiative, 2018. https://www.globalnetworkinitiative.org/about/index.php

[40] Garside, Juliette. "Vodafone under fire for bowing to Egypt pressure." The Guardian, 26 July 2011. https://www.theguardian.com/business/2011/jul/26/vodafone-access-egypt-shutdown

[41] "Vodafone." Business & Human Rights Resource Centre, 2018. https://business-humanrights.org/en/vodafone-0

[42] Interviews on file with ARTICLE 19. Conducted November 19, 2017.

[43] "C-Suite" refers to "Chief" level executive positions, including the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, among others.

[44] Fernandez, S. and Rainey, H. G. "Managing Successful Organizational Change in the Public Sector." Public Administration Review, 66, 2006, p. 168—176.

[45] "NTT Communications Sustainability Report 2016." NTT Communications, 2016. http://www.ntt.co.jp/csr_e/pdf/sustainability_report_2016e.pdf

[46] "Digital Human Rights" MTN Group, 2018. https://www.mtn.com/en/mtn-group/sustainability/sustainable-societies/Pages/digital-human-rights.aspx

[47] Cloudflare is different from most other Internet infrastructure companies in this study because it was founded relatively recently in 2009 and is a privately held company with approximately 650 employees.

[48] Content neutrality is a policy in which a provider remains agnostic to the type of content, hosting or transmitting content

regardless of its potentially vile or uncivil nature.

[49] Prince, Matthew. "Cloudflare and Free Speech." Cloudflare Blog, 9 Aug 2013. https://blog.cloudflare.com/cloudflare-and-free-speech/

[50] Schwenke, Ken. "How One Major Internet Company Helps Serve Up Hate on the Web." ProPublica, 4 May 2017, https://www.propublica.org/article/how-cloudflare-helps-serve-up-hate-on-the-web

[51] Cloudflare CEO Matthew Prince attempted to differentiate personal decisions from company policy in an interview with the Verge, stating, "This was my decision, I don't think it's CloudFlare's policy and I think it's an extremely dangerous decision in a lot of ways." Russel, Brandom. "The Daily Stormer just lost the most important company defending it." The Verge, 16 August 2017. https://www.theverge.com/2017/8/16/16157710/cloudflare-daily-stormer-drop-russia-hate-white-nationalism

[52] Shu, Catherine. "GoDaddy tells white supremacist site Daily Stormer to find a new domain provider," TechCrunch, 14 August 2017. https://techcrunch.com/2017/08/13/godaddy-tells-white-supremacist-site-daily-stormer-to-find-a-new-domain-provider/

[53] Larson, Selena. "Cloudflare CEO questions his decision to terminate neo-Nazi website," CNN Money, 24 August 2017. http://money.cnn.com/2017/08/24/technology/business/cloudflare-ceo-interview-daily-stormer/index.html

[54] Conger, Kate. "Cloudflare CEO on Terminating Service to Neo-Nazi Site: 'The Daily Stormer Are Assholes'." Gizmodo, 16 August 2017, https://gizmodo.com/cloudflare-ceo-on-terminating-service-to-neo-nazi-site-1797915295

[55] Post, James and Barbara W. Altma. "Managing the Environmental Change Process: Barriers and Opportunities." Journal of Organizational Change Management, Vol. 7 Iss 4, 1994. p. 66. http://dx.doi.org/10.1108/09534819410061388

[56] Global Voices. "India's Latest Internet Shutdown Hits Haryana and Punjab," 31 August 2017. https://globalvoices.org/2017/08/31/indias-latest-internet-shutdown-hits-haryana-and-punjab/

[57] Sridharan, Vasudevan. "Bangladesh: Government briefly shuts down Internet," International Business Times, Nov 8, 2015, https://www.ibtimes.co.uk/bangladesh-government-briefly-shuts-down-internet-mobile-services-1529316

[58] Timberg, Craig and Ellen Nakashima, "Agreement with private companies protect U.S. access to cables' data for surveillance," The Washington Post, 6 July 2013. https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html?utm_term=.c66a55fde284

[59] "Launching Stop: The Shutdown Tracker." Access Now. 16 November 2017. https://www.accessnow.org/keepiton-shutdown-tracker/

[60] "Human Rights Impact Assessment" BSR, conducted on behalf of Telia Company, 2017. https://www.teliacompany.com/en/sustainability/reporting/human-rights-impact-assessment/

[61] Perlroth, Nicole and Katie Benner, "Subpoenas and Gag Orders Show Government Overreach, Tech Companies Argue," The New York Times, 4 October 2016. https://www.nytimes.com/2016/10/05/technology/subpoenas-and-gag-orders-show-government-overreach-tech-companies-argue.html

[62] This excludes information requests covered by gag orders. Many Internet content providers, and increasingly infrastructure providers, use warrant canaries to communicate transparently with the public about when they receive gag orders. Warrant canaries are method to inform users when a court order is issued preventing that company from revealing the existence of a government request. The warrant canary remains visible until a court order

is issued, and then the canary is removed; if the canary is not replaced in a specified period of time, users are meant to assume that the company has been served a gag order. This passive method of signaling government intervention significantly improves transparency. More information available in "Warrant Canary FAQ." Electronic Frontier Foundation, April 2014. https://www.eff.org/deeplinks/2014/04/warrant-canary-faq

[63] Nokia Annual Report 2016 (Form 20-F). p. 138 https://www.nokia.com/sites/default/files/files/nokia_20f16_full_report_en.pdf

[64] Kaye, Kate. "Telefonica gives Consumers Control over (some) Data," Adage, 5 May 2017. http://adage.com/article/datadriven-marketing/telefonica-consumers-control-data/308925/

[65] "NSA Spying: How it Works," Electronic Frontier Foundation, https://www.eff.org/nsa-spying/how-it-works

[66] The scope of the industry for this study goes beyond traditional analyst definitions to encompass Internet Service Providers, Wireless Telecommunications Carriers, and Hardware Equipment Vendors as part of the "Internet infrastructure provider" industry ("the industry").

[67] See IBISWorld "Global Internet Service Providers" and "Global Wireless Telecommunications Carriers." IBIS World Global Market Research Report, April 2018 and July 2017, respectively. https://www.ibisworld.com/industry-trends/global-industry-reports/telecommunications/

[68] Laravea, Merrick. "South Koreas Internet infrastructure shows the FCC how net neurality should be done," Forbes, 26 January 2018. https://www.forbes.com/sites/outofasia/2018/01/26/south-koreas-internet-infrastructure-shows-the-fcc-how-neutrality-should-be-done/#31f41897581b

[69] Parrish, Kevin. "South Korea Fines Facebook $300K for allegedly throttling its services." Yahoo! News, 21 March 2018. https://ph.news.yahoo.com/south-korea-fines-facebook-300k-233407165.html

[70] Much of the EU is an exception to this trend having instituted a telecommunications law in 1999 oriented towards protecting competition from new market entrants and preventing a high degree of consolidation.

[71] "Global Internet Service Providers." IBIS World Industry Report, May 2017, p 4.

[72] Beede, David. "Competition Among US Broadband Service Providers." US Department of Commerce, Office of the Chief Economist, OCE Issue Brief #1-14, December 2014, http://www.esa.doc.gov/sites/default/files/competition-among-us-broadband-service-providers.pdf ; Kaleigh, Rogers. "More than 100 Million Americans Can Only Get Internet Service from Companies That Have Violated Net Neutrality." Vice Motherboard, 11 December 2017. https://motherboard.vice.com/en_us/article/bjdjd4/100-million-americans-only-have-one-isp-option-internet-broadband-net-neutrality

[73] Wessel, David. "Is lack of competition strangling the US economy?" Harvard Business Review, March 2018. https://hbr.org/2018/03/is-lack-of-competition-strangling-the-u-s-economy

[74] "AT&T Materiality Assessment." AT&T CSR Sustainability Reporting, 2017. http://about.att.com/content/dam/csr/sustainability-reporting/PDF/2017/Materiality_Map-print.pdf

[75] "UN Guiding Principles Reporting Framework Investor Statement." Shift Project and Mazars Consulting, February 2017. http://www.ungpreporting.org/early-adopters/investor-statement/