The Digital Rights Double-Helix: Examining the Intertwined Roles of Business & Human Rights and Tech Governance

By Jason Pielemeier*

This essay is part of Shift's series marking the 15th anniversary of the UN Guiding Principles on Business and Human Rights.

Introduction

The modern information and communications technology (ICT) sector is built on mobile telephony and the Internet. These networks enable a range of mostly private, commercial providers to quickly spread digital services around the world. As the sector has expanded, unique features inherent to ICTs, which include the nonrivalrous nature and low costs of reproducing and transmitting data, have led to an explosion in the amount of information available to people, corporations, and governments everywhere – a boon to everything from education to surveillance. Meanwhile, the governance of these technologies has to date prioritized openness and interoperability, enabling the instantaneous, global sharing of news, memes, and viruses. The pace with which new tools, systems, and features are created and evolve has tested the capabilities of political systems, cultural norms, and human psychology.

In this essay, I use the history of the Global Network Initiative (GNI) to explain how the ICT sector is intertwined with the modern Business and Human Rights movement, examine the ways in which the UN Guiding Principles on Business and Human Rights (UNGPs) have impacted the sector's development, and consider lessons that might help guide future developments toward greater respect for and protection of human rights.

How ICT Influenced BHR

The UNGPs emerged during the later stages of turn-of-the-millennium globalization – a period still fueled by optimism, but tempered by the security concerns spawned by 9/11 and the emerging geopolitical tensions between China and the United States. It is impossible to understand the modern ICT sector without examining the dialectic tension between the forces of globalization and sovereignty.

These tensions were on full display in 2007, as Yahoo! CEO Jerry Yang withstood withering criticism from members of the US Congress for providing information that was used by authorities in the People's Republic of China to arrest and prosecute Shi Tao, a Chinese journalist and poet. At that hearing, Yang explained that the company was working with other companies and human rights organizations to develop a shared code of conduct, noting that "We're all focused on protecting and promoting free expression and privacy."

While that was likely little consolation to Shi's mother, who was in attendance, his commitment was sincere. The next year, the Global Network Initiative (GNI) Principles on Freedom of Expression and Privacy were launched and soon after a governance and oversight mechanism

emerged with participation from a small group of mostly American academics, civil society organizations, investors, and tech companies (including Yahoo). This new, multistakeholder initiative set out key expectations for tech companies, including around the conduct of human rights due diligence (HRDD) to manage risks to freedom of expression and privacy across their global operations. Importantly, it also provided a space for companies to confidentially share non-public information about how they were attempting to meet those expectations. Through these "assessments," non-company members were empowered to evaluate those efforts and make recommendations for continuous improvement.

The core elements of the GNI framework – its multistakeholder nature and commitment to HRDD, transparency, and continuous improvement – anticipated the broad structure of the UNGPs, which would be endorsed by the UN Human Rights Council in 2011. This was not a coincidence. Embedded in the negotiations that led to GNI's establishment were staff working for the Special Representative of the UN Secretary-General on Business and Human Rights, John Ruggie. Professor Ruggie presented his major report proposing the "Protect, Respect and Remedy Framework" that underpins the UNGPs to the UN Human Rights Council in 2008 – the same year that GNI launched.

In the almost two decades that have passed since then, the use of ICTs has exploded around the world, and government efforts to control that use and get access to related data have become more widespread and sophisticated. Meanwhile, GNI has continued to expand its membership and broaden its approach to guiding tech companies' efforts to respect freedom of expression and privacy. Today, over 130 leading tech companies, investors, civil society organizations, and academics from around the world come together through GNI to review company efforts, learn about emerging trends, and advocate for rights-respecting approaches to tech regulation.

GNI's endurance and growth are a direct result of two factors. First, the requirement to embed the GNI framework into company systems and policies, accompanied by periodic review and an expectation of improvement over time, has rooted these practices within corporate governance, making participation more enduring. Second, GNI's symbiotic relationship with the UNGPs: the UNGPs established the global reference point for understanding state duties and corporate responsibilities, while GNI has provided a forum for stakeholders to explore how those understandings play out in the ever-evolving tech sector.

How BHR Influenced ICT

Together, the UNGPs and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD Guidelines), which incorporate the HRDD approach set out in the UNGPs, provide a global framework that helps corporations navigate diverse jurisdictional realities. Like the GNI Principles, this framework relies on existing international human rights law (IHRL) principles to influence both tech company and government conduct. The global, "consensus" nature of these principles provides a degree of normative certainty and consistency that helps legitimize efforts to self-govern services and push back on overly broad government interventions.

Over the last 18 years, GNI company members have found themselves ordered to shut down telecommunications services during mass protests, facilitate mass surveillance, and restrict apps or entire platforms during elections, among many other compromising scenarios with serious human rights implications. In many of these cases, media reporting and public attention have understandably focused on the outcomes – network disruptions, privacy violations leading to other harms, or election interference – without exploring the full context of those scenarios, often because that context is not public.

At the same time, as case studies from GNI assessments illustrate, in many more instances that never make the news, companies find ways to avoid or mitigate compliance with these types of orders, quietly helping to protect freedom of expression and privacy.

Like the UNGPs, the GNI framework does not insist that companies must violate domestic laws, even where they are in tension with international ones. The GNI Principles on Freedom of Expression and Privacy also make clear that "the safety and liberty of company personnel who may be placed at risk" is a key aspect of responsible company decision-making. Through the GNI assessment process, members get the full stories behind these serious incidents — soldiers compelling network providers to act at gunpoint, secret service visits to company representatives' homes, or gag orders preventing companies from providing notice to their users. They also hear about the more successful cases where companies stand up against overbroad government demands, either by ignoring them, complying in only symbolic ways, or pushing back.

Of course, as new situations continue to arise, the challenges posed by government demands are becoming more complex and, in some cases, intractable. But over the course of almost two decades, these assessments and their resulting recommendations have helped guide corporate practices related to transparency reporting, the establishment of human rights policies and the empowerment of internal rights experts, the conduct of due diligence, and the provision of remedy. More recently, these expectations have begun to be encoded in laws like the EU's Digital Services Act and the UK's Online Safety Act, turning voluntary commitments into legal requirements.

Lessons for the Future

As ICTs become increasingly ingrained in our economies, societies, and political systems, the imperative to align these technologies and their governance with human rights principles only strengthens. Those working on responsible business conduct in the tech sector should continue to explore and propose how best to identify and address downstream risks, and seek innovative ways to ensure that responsibility and accountability continue to flow across the tech stack (the range of hardware, software, and protocols that underpin the modern digital ecosystem) and are appropriately embedded in relevant legal frameworks.

Moving forward, it will be important for tech companies and other stakeholders to come together to understand and unpack the ways that language models and agentic AI are scrambling conceptions of agency, liability, and safety. In so doing, they should continue to

honor the same inclusive, multistakeholder approach to governance that has helped keep the Internet open and interoperable, and use human rights to ground those discussions in lived realities in order to address the risks these technologies pose to the world's most vulnerable.

New questions are also arising regarding how the return of multipolar geopolitics, the demand for digital sovereignty, and the public alignment of some tech elites with particular political positions will impact the business case for responsibility. While it may be tempting to interpret these trends as a backlash against global norms, I would argue that they actually strengthen the case for companies to tether themselves to the tried-and-true principles of the UNGPs and their grounding in IHRL, which provide an enduring, global north star to help chart a course through these turbulent times.

---

*Jason Pielemeier is the Executive Director of the Global Network Initiative (GNI), a dynamic, multistakeholder, human rights collaboration, building consensus for the advancement of freedom of expression and privacy among technology companies, academics, human rights and press freedom groups and investors. Prior to joining GNI, Jason was a Special Advisor in the U.S. Department of State, where he led the Internet Freedom, Business, and Human Rights section in the Bureau of Democracy, Human Rights and Labor.