Niels ten Oever

Human Rights Are Not a Bug

Upgrading Governance for an Equitable Internet

CONTENTS

III. CONSENSUS AND RESISTANCE

The internet infrastructure is governed through a process that is open, deliberate, and notoriously resistant to change.

IV. FUTURE PATHS

The same interdependence that makes the internet transformative and durable can enable cooperation that elevates human rights for all who depend on the internet's infrastructure.

Executive Summary

The internet is a complex infrastructure consisting of a myriad of interconnected devices, institutions, and standards. Together they allow information to move quickly and reliably across thousands of computer networks.

During the past year, as you searched for information on COVID-19, or tried to keep up with loved ones and work, you were relying on this infrastructure to deliver the web pages, video and phone signals that kept you connected.

Like the cables, protocols, and signals that carry your data, internet governance institutions go largely unnoticed, but the impact of their decisions is immense.

Like the cables, protocols, and signals that carry your data, internet governance institutions go largely unnoticed, but the impact of their decisions is immense. The speed, availability and privacy of online information all have human consequences, especially for those who are already subject to surveillance or structural inequities—such as an activist texting meeting times on WhatsApp, or a low-income senior looking for a vaccine appointment.

Although the stakes of internet governance are high for security, access to information, freedom of expression and other human rights, the standards and protocols developed by internet governance bodies remain largely voluntary. There is also no central authority to ensure that standards are implemented correctly, only members' shared motivation to keep the internet functioning. Internet governance bodies are open to all sectors, but they are dominated by the transnational corporations that own and operate much of the infrastructure. Our increasingly digital daily lives are defined by this unusual "stack" comprised of mostly voluntary norms, set by governance bodies, dominated by private corporations.

Internet governance organizations maintain a distinct governance philosophy: to be consensus-driven and resistant to centralized institutional authority over the internet. But these fundamental values have limitations that leave the public interest dangerously neglected in governance processes. In this consensus culture, the lack of institutional authority grants disproportionate power to the dominant corporate participants. While the governance bodies are open to non-industry members, they are essentially forums for voluntary industry self-regulation. Voices advocating for the public interest are at best limited and at worst absent.[1]

1 "The public interest" concerns the well-being of all individuals and groups in society. In this paper "human rights" is used in several places as a concrete proxy for "the public interest," based on the globally accepted, UN-codified norms that specify the rights of groups and individuals.

While the internet is often described as a public space or a public square, it is actually a mosaic of overwhelmingly privately owned infrastructure. The internet is more like a cluster of interconnected malls and garages than a public space.

Furthermore, the philosophy of internet governance inhibits and even denies opportunities to make inherent changes to the governance process itself. Human rights have not been the top priority for corporate actors. A legacy of narrow focus and the overarching objective to increase interconnection have produced a culture effectively dismissive of changes that could make consideration of the public interest a standard practice.

The internet's defining characteristics—its distributed architecture and its decentralized governance—offered the promise of improved access and greater freedom for everyone, but the internet has not exactly delivered on it. Instead, the very structures and practices established to maintain the internet widened the gap between the promise of a public good and the more complicated present-day reality.

This report examines the background and impacts of the internet's multistakeholder governance, and offers recommendations to civil society, corporations, governments, and academics for aligning internet governance—and internet infrastructure—with the public interest and human rights.

It recommends foremost that all actors support practices that consider the public interest impact of all technology and policy decisions, and that internet governance organizations adapt their processes and procedures to ensure the meaningful involvement of all those impacted by their decisions.

Those who develop and govern the internet's infrastructure can ensure its foundational safeguards against harm and inequity by adopting human rights impact assessments modeled on the UN's Guiding Principles as an inherent part of policy and technology development;[2] by broadening advocacy and methods for engagement between civil society and internet governance organizations; by lowering the barriers to participation for people outside the regions, companies and demographics that historically have dominated the governance bodies; and through longitudinal investment by donor organizations to help pilot and sustain new practices, among other steps described at the end of this report.

2 "UN Guiding Principles on Business and Human Rights," UN Human Rights, January 2012.

I. INTRODUCTION

The internet's infrastructure is better at connection than protection.

You're probably used to seeing "404" messages online when a web page is missing. The "Page Not Found" error is one of several dozen status codes—standard messages from web servers or service providers about what is available and what may be broken or disrupted.

You may not have encountered Status Code 451, though. A "451" error indicates that information is unavailable "for legal reasons," in other words, censored, disputed or subject to removal by a service or government.

Web users see few "451" errors not just because there are fewer censored pages than broken links, but also because the implementation of Status Code 451 depends on the individual practices of web hosts, and on the varied practices of governments for content removal and notification. While it's nice to imagine a world where censors and authoritarians give notice when they block access to material, in practice, such actions are more often taken unilaterally and unannounced.

Status Code 451 is unusual among the standards established by the Internet Engineering Task Force (IETF), both because it is named for a science fiction novel (Ray Bradbury's "savage and shockingly prophetic" tale of book-burning, *Fahrenheit 451*[3]), and because it was approved despite a

3 August Derleth, "Vivid Prophecy of Book Burning," review of *Fahrenheit 451* by Ray Bradbury, *Chicago Tribune*, October 25, 1953.

INTERNET INFRASTRUCTURE AND GOVERNANCE

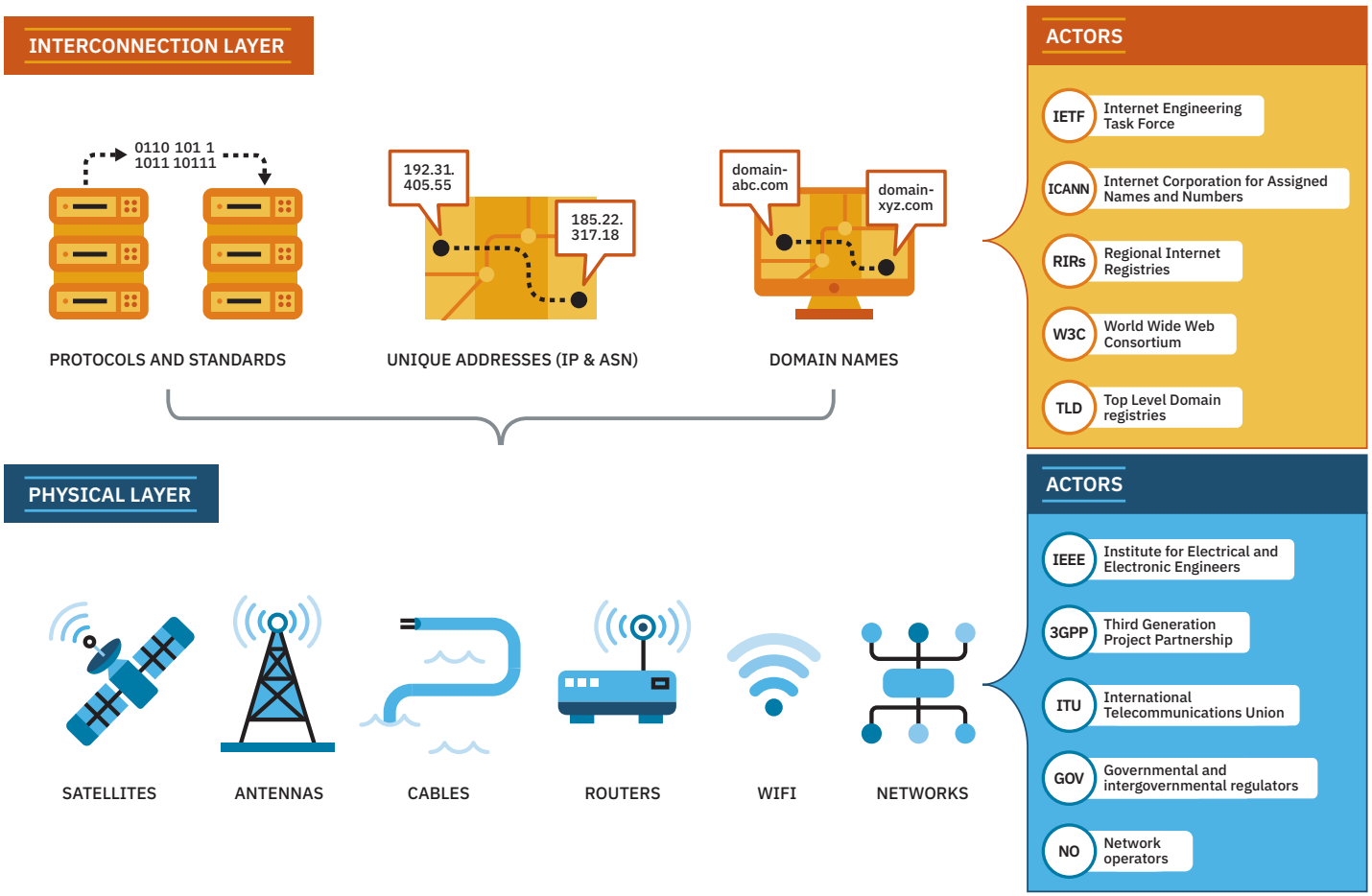

FIGURE 1.
Illustration by Nook Studios/ Greg Straight with 3 Bridges, licensed under CC BY-SA 4.0

longstanding debate about the proper role of the IETF as a guardian of human rights in the internet's infrastructure.

The Internet Engineering Task Force is one of the myriad organizations that drive the governance of the internet's infrastructure (see Figure 1). Most of these bodies lack any of the formal power held by states. Instead, they exercise a more informal power, setting voluntary norms that guide a transnational internet infrastructure industry made up largely of private companies. Unlike many historical communication networks—the telegraph, for instance, or the original ARPANET—the internet's infrastructure is run almost completely by corporations. The voluntary policies, standards, and specifications for industry behavior are developed in governance organizations such as the Internet Corporation for Assigned Names and Numbers, Regional

Internet Registries, the World Wide Web Consortium, and the IETF. It is these acronym-laden, industry-adjacent institutions who decide what our digital world looks like.

This report assesses the background and dynamics of internet infrastructure governance, with a focus on the Internet Engineering Task Force, and asks how internet governance processes could be updated to deeply embed the public interest in governance decisions and in decision-making culture.

The IETF sets the standards for the technical protocols that underlie and connect the internet—such as TCP, IP, and HTTP, all of which are in use when you browse the web—but IETF members are known for their insistence that, "We are not the protocol police," by which they mean that the IETF is not responsible for how their standards and protocols are implemented. For more than 25 years, the IETF has maintained a rigorous but narrow focus on one principle in its governance of the internet's infrastructure: to increase connectivity across the thousands of networks that comprise the internet.

Long-time participants in internet governance reiterate the importance of a narrow remit for standards bodies, and many rights-related topics such as privacy, free expression or exclusion are deemed "too political." In other words, engineers should not take up the role of nation-states, or meddle in their affairs. This objection is used to sidestep many issues that directly affect the lives and rights of millions of users. And even though work for the public interest is part of the mission statements of almost all internet governance organizations, there are no formal, required reviews for the societal implications of the technologies they standardize or the policies they set forth.

Since at least 2003, the Internet Engineering Task Force has faced calls to embed social impact assessment into the consideration of new policies and technologies.[4] But the IETF—like most of the internet's standards developing organizations—has been effectively unwilling to prioritize conversation about the implications of internet infrastructure for human rights or the public interest.

A version of this debate spilled into wider view in early 2021 in a charged public discussion about traditional internet vocabulary with racist connotations—such as "master" and "slave" (for a relationship between devices) and "whitelist" and "blacklist" (for how systems filter messages).[5] Like all standards and protocol changes, the proposal about racially charged words

4 John B. Morris Jr. and Alan B. Davidson, "Public Policy Considerations for Internet Design Decisions," posted June 2003.

5 Kate Conger, "'Master,' 'Slave' and the Fight Over Offensive Terms in Computing," *The New York Times*, April 13, 2021.

is subject to an IETF review process founded on "rough consensus" among members. The premise of the rough consensus approach is that extensive deliberation and negotiation will yield a better agreed solution, especially among stakeholders with varied interests.

Consensus-building has worked well for internet governance in particular because the primary shared objective among participants has been so strong: to increase the size of the internet through the interconnection of more networks and services. This is the value the participants in internet governance seek to create and the narrow focus they have sought to preserve.

The engineers who oversaw the emergence of the global internet believed that network growth always benefits the public interest. There was a deeply entrenched assumption that the internet is an engine for good—that interconnection and rough consensus naturally promote democratization and that the open, distributed design of the network can by itself limit the concentration of power into oligopolies.

This has not proved to be the case.

Increased connectivity, together with the rejection of centralized authority, has facilitated uneven power in internet governance organizations. The consolidation of the technology industry has granted some groups more influence than others over the internet's infrastructure, and provided them with greater means to introduce standards and to send representatives to participate in the processes.

The very thing that has made internet governance efficient—the tradition of a minimal mandate to increase interconnection and interoperation—has also thwarted a norm of collective action in the public interest.

As a result, the very thing that has made internet governance efficient—the tradition of a minimal mandate to increase interconnection and interoperation—has also thwarted a norm of collective action in the public interest. The habit, the reflex, of inquiry for any proposal remains to ask if it might hamper interconnection across networks. Historically, proposals to consider the societal impacts of a technology or policy have been met with resistance along these lines.

Such resistance has not only been a matter of principle, it has also defined the style and culture of the Internet Engineering Task Force debate over proposals tied to societal impacts (and indeed over most topics). Anything not seen to be in the interest or worldview of a significantly represented group is unlikely to move forward. The lack of demographic or regional diversity in most internet governance institutions has only compounded this dynamic. Participants' narrow focus on interconnectedness has too often become narrowness regarding other topics and other voices; this challenge is attributable both to logistical and socioeconomic realities and to social and cultural issues.

The practice of internet governance has produced the information architecture of the internet, but it has also defined the governance philosophy:

The engineers who oversaw the emergence of the global internet believed that network growth always benefits the public interest. There was a deeply entrenched assumption that the internet is an engine for good—that interconnection and rough consensus naturally promote democratization and that the open, distributed design of the network can by itself limit the concentration of power into oligopolies.

This has not proved to be the case.

consensus driven and resistant to centralized institutional authority. Both of these fundamental characteristics have limitations and risks that threaten the public interest and human rights. While all views and perspectives are supposedly equal in the consensus-building process, the lack of central authority helps enable disproportionate power for the dominant private actors. Meanwhile, the philosophy of internet governance inhibits opportunities for changes that are not in the interest of those dominant parties.

Despite the promise of innovation and transformation that is wired into the internet's infrastructure, internet governance has not delivered on that promise in its stewardship of human rights and the public interest. And the systems and people who could address that failure may be limited by the same structures that enable the internet's governance and growth.

To make the societal impact of technologies and policies an inherent consideration in internet governance processes it is important to contemplate what changes might look like, how they could work in practice, and where the barriers and opportunities are among those potential changes.

There are several ways that the institutions of internet governance, companies, governments, and advocates can build considerations of the public interest into the operations and culture of internet standards development organizations. Some of the recommendations offered at the conclusion include:

> That **internet governance organizations** incorporate human rights impact assessments into their regular work, using the United Nations Guiding Principles for Business and Human Rights as a template, and that they adopt new practices that engage more vulnerable, impacted communities in decision-making.
>
> That **civil society and researchers** seek to broaden their spectrum of engagement with internet governance bodies and private companies, and partner to identify opportunities for cross-sector collaboration and advocacy.
>
> That **advocates, academics, and other non-techies** volunteer and participate in governance bodies, to better understand the processes and incentives underlying internet governance, and to help improve the bridges between expert communities.
>
> That **governments** evolve their own use of the UN Guiding Principles on Business and Human Rights to promote more responsible, accountable technology through governance, procurement, and cross-sector collaboration.

That **technologists and technology companies** implement stronger practices for human rights impact assessment, forge deeper partnerships between engineers, CSOs, and communities, and adopt the UNGP as their counterparts in the finance, telecommunications and garment sectors have done.

That **donor groups and agencies** fund accountability programs with cycles of 5 to 10 years instead of 12 to 18 months, to align with the real-world pace of governance decisions and standards development and ensure sustained investment in shifting cultures and practices.

These potential interventions and others are summarized in Section IV, under "Opportunities."

1. The internet's creators aspired to technologically distribute power to the edges of the network, but economic consolidation of the sector has centralized power in the hands of a few corporations.

The early internet engineers believed that the growth of a global communication network would benefit society. The design of the network and its governance reflect their conviction that any increase in interconnection would be in the public interest. The major governance organizations herald the public interest and social good in their charter statements. The bylaws of ICANN identify "core values" including "broad, informed participation reflecting the functional, geographic, and cultural diversity of the internet" a "bottom-up, multistakeholder policy development process [used] to ascertain the global public interest."[6] The IETF mission statement states that "The Internet isn't value-neutral, and neither is the IETF," citing openness, fairness, "edge-user empowerment and sharing of resources," as "core values of the IETF community."[7]

In internet governance organizations, the tradition of decisions through "rough consensus" reflects this belief in decentralized power, and the prime directive to increase the size of the internet by enabling the connection of more networks and services. Each network or service added creates more value for the internet as a whole and thus all for all the connected networks.

However, the continued expansion of the internet has happened alongside continued consolidation in the technology sector, which has a significant

6 "Bylaws for Internet Corporation for Assigned Names and Numbers," ICANN, accessed January 15, 2020.

7 "A Mission Statement for the IETF," Internet Engineering Task Force RFC 2935, October 2004.

impact on power relations in consensus processes. Some groups now wield much greater power than others over the internet infrastructure, and have more resources to produce technology and send people to participate in the governance process.

Market consolidation can be seen at all the layers of the internet infrastructure. In all significant submarkets, such as networking equipment vendors, "Top-Level Domain" registries, and network operators, a few large corporations are dominant. This dynamic is also reflected in the number of corporate-affiliated governance participants.

The commercialization and privatization of the internet that began in the 1990s was expected to bring about innovation and competition. In practice, it has led to the emergence of oligopolies.[8] Though some have hailed the internet as a "generative network," an engine for innovation, and a tool for democratization,[9] others have pointed out that the dominant role of (mainly American) companies in internet companies could be seen "as a mechanism for the reinforcement of existing power dynamics."[10]

Historically, global communication systems like the telegraph or the telephone were owned, operated, and governed by nation-states or their subsidiaries. International connectivity was standardized and regulated in intergovernmental bodies. The internet is the first global communication network where private corporations play a more important role than governments.

The internet is the first global communication network where private corporations play a more important role than governments.

While the distributed nature of the internet infrastructure, combined with voluntary standards and decentralized decision-making, were supposed to be an enabling environment for grassroots participation, these same features have turned out also to be a bug, a root cause of the internet's economic centralization and consolidation of power.

2. With few exceptions, internet governance has resisted efforts to make user empowerment and the greater public interest a priority.

Discussions about the privacy, legal and social risks of the internet date back to its very earliest development in 1969, the same year as the moon landing.[11] But, like the space race, the internet has unleashed a world of risks and unintended consequences. Everyday users cannot easily manage their data, or

8 Cowhey, Aronson, and Richards 2009; Van Schewick 2012.

9 Zittrain, 2008; Van Schewick, 2012; Castells, 2009.

10 Carr, 2015.

11 Braman, 2009; 2010; 2012.

understand who can access or control it. The rise of the online attention economy has rewarded misinformation and propaganda tactics that help spread fear, violence and, most recently, the COVID-19 virus. And nation-states have new robust toolkits for surveillance, repression, and persecution.

Because of the private and voluntary nature of internet governance and the independence of the networked systems, there is no central authority that can be held accountable for violations against the public interest or human rights that are perpetrated through the internet infrastructure. Physical infrastructure standards are traditionally built to minimize harm—steam engines have a minimum boiler thickness, roads have guardrails, cables are insulated—but the internet's standards regime is not designed around protection from its dangers or around assessment of the potential societal impact of the standards and policy process.

Even the well-understood risks such as surveillance and data security have not been systematically addressed in governance processes. Researcher Nick Doty shows in his analysis of standard-setting that since 1989 the Internet Engineering Task Force has required a "Security Considerations" section in all the important technical and policy submission documents called "Requests for Comments" (or more commonly RFCs). These considerations are meant to anticipate how proposed technologies could impact security for users and the overall internet. However, not all "Security Considerations" sections are as long or thorough as one would hope or expect.[12]

In 2017, human rights advocates, including the author, published a Request For Comments suggesting guidelines for human rights considerations to be used for protocols.[13] Two years later, when an RFC on password security included a section on human rights considerations (the first and only one to date), the section's language resembled gun rights rhetoric more than a conventional discussion of human rights.[14] The new security measures "can be used as arms, kept and borne, to defend oneself against all manner of attackers," the document reads, "criminals, governments, lawyers, etc." This reflects the prevailing attitude about rights within internet governance organizations (a view akin to American libertarianism), and the way the governance culture diverges from wider public discourse or treaties on human rights and the potential societal impacts of technology.

12 Doty, 2015.

13 ten Oever and Cath, 2017.

14 "Secure Password Ciphersuites for Transport Layer Security (TLS)," Internet Engineering Task Force RFC 8492, February 2019.

Physical infrastructure standards are traditionally built to minimize harm—steam engines have a minimum boiler thickness, roads have guardrails, cables are insulated—but the internet's standards regime is not designed around protection from its dangers or around assessment of the potential societal impact of the standards and policy process.

Nevertheless, discussions about human rights are not entirely absent among these governance institutions. In 2013, after Edward Snowden revealed massive US spying programs secretly monitoring internet traffic, the internet governance community came together to issue the "Montevideo Statement," declaring "strong concern over the undermining of the trust and confidence of Internet users," amid reports of "pervasive monitoring and surveillance." Despite the distinct roles of each governance body, and the strong culture of autonomy and decentralization, alarm over these privacy abuses became "a way for a lot of different agendas to meet," as one expert put it.[15] It's worth noting, though, that even this collective action was born out of a particular conception of human rights, grounded in preserving uninterrupted connectivity between corporations and their customers.

The fact that there is no central rule maker for the internet does not mean that there is no power and authority at all—on the one hand, no one can single-handedly switch off the whole internet, but on the other hand, changes can be hard to make. Even when a change is agreed that does not guarantee it will be implemented. For instance, the new version of the internet Protocol, dubbed IPv6, was standardized in 1998 to open up exponentially vast numbers of internet addresses as internet-connected devices proliferated. But, like any number of new agreed standards, full implementation remains uneven and incomplete, nearly 25 years on, and even though IPv4 addresses have long since run out. This slow adoption has led to quick fixes, such as Network Address Translation (NAT), that have made the internet less transparent and increased the power imbalance between users and service and content providers.[16]

This complicated reality makes it even harder for non-corporate actors, such as civil society, academics, and governments, to participate in the governance process, because they have no direct control over how decisions are implemented. The least-resourced internet users, and those most subject to structural inequity or political discrimination, also lack a voice in these processes. The cycle of development and implementation takes a long time and demands a high level of knowledge and expertise. Processes also differ per governing body, which reinforces the influence of veteran participants with greater fluency and larger social networks.

Largely because of these limitations of intervention and redress, there remain too many instances where internet infrastructure has been used to

15 Robinson Meyer, "What Does It Mean for the U.S. to 'Lose Control of the Internet?'," *The Atlantic*, October 16, 2013.

16 ten Oever, 2021.

harm human rights or has failed as a bulwark against abuse and inequality. States and private companies have ample opportunities to conduct surveillance or censorship, for instance, and infrastructural power grows ever more concentrated in a few transnational corporations.

Even as the internet's omnipresence increases, its infrastructure and governance are showing signs of wear and tear that suggest an urgent need for an update. Many crucial security fixes have not been implemented, resulting in a range of attacks and unaddressed dependencies. But even as the need for updates has increased, the opportunity for non-corporate actors to roll out new protocols is scant. For example, Google's QUIC protocol—a secure, high-speed connection method central to Google's approach to data transfer—was launched and widely adopted over the last five years, even while many other organizations have been unsuccessful in launching or disseminating their own new protocols in the past.[17]

Since at least 2002, there have been calls to incorporate social impact assessments into the governance process for new internet policies and technologies. Up to now, this has not been realized. As we explore whether the existing internet governance regime can manage the world's information infrastructure in the public interest, we must consider that the main objective for most governance participants remains the expansion of interconnectivity and interoperation among networks and services, not the creation of limitations in the name of human rights.

17 ten Oever, 2021.

Internet governance encompasses physical, interconnection, and collaborative layers.

Internet infrastructure encompasses more than the technologies such as hardware, networks, and software and logical layers. The complex of relationships, institutions, agreements, and documents that enable the infrastructure to function are also an inherent part of it.

1. Wires and cables, communication standards and protocols, make up the internet's physical and "interconnection" layers.

The internet consists of more than 70,000 linked communication networks connecting billions of devices. The role of internet standards and protocols is to ensure interoperation not just between these networks and devices, but also between the products and services of countless providers. Often, when you do see a connection fail, it's the lack of standardization, or the lack of a properly implemented standard, that's the reason. Without these standards, applications would not work properly in some browsers, and not all devices or brands of computer could get online.

The wide range of networks get connected in different ways: through satellite or radio signals, copper or fiber cables, over electrical cable or even barbed wire. These wires and signals and various devices constitute *the physical layer* of the internet.

The steps to join all these networks together into one network happen at *the interconnection layer*—or the "logical" layer—of the internet (see Figure 1, pg. 6). The interconnection layer forms the preconditions for these divergent networks and different devices to both join and extend the internet. The interconnection layer includes three main functions:

1. Define protocols for the devices and network to talk to each other—such as IP for addressing, TCP for enabling devices to connect for data transfer, HTTP for delivering content to browsers, etc.)
2. Assign unique numbering addresses to all networks and devices so they can contact each other
3. Translate numbered addresses (IP addresses) to unique human-readable addresses, also called domain names, such as example.com (this happens through the DNS, or Domain Name System)

These functions are the pre-conditions for the physical layer to deliver information as it should. The infrastructure is managed through coordination and negotiation among several governance organizations (see Table 1, pg. 18).

The Internet Engineering Task Force defines the protocols that enable connection across the internet. The human-readable addresses are set and managed by the Internet Corporation for Assigned Names and Numbers, and the unique numbering addresses for networks and devices are distributed through five Regional Internet Registries (or RIRs).[18] (Meanwhile, for your browser, the World Wide Web Consortium (W3C) sets the standards; browser developers cooperate in the W3C to make sure you can view a website or stream a program as easily in Firefox as you can in Chrome or Safari.)

These organizations and the logical and physical layers they oversee comprise the internet's governance regime. This section provides background on how this physical and collaborative infrastructure came into being and identifies some of its defining characteristics. This will set the stage for the subsequent discussion of its limitations and how they might be addressed.

18 ARIN for the United States, LACNIC for Latin America, AFRINIC for Africa, APNIC for the Asia-Pacific region, and RIPE NCC for Europe, the Middle East and the former Soviet Union.

INTERNET INFRASTRUCTURE: KEY GOVERNANCE ACTORS

TABLE 1.

INSTITUTION	ROLE
INTERCONNECTION LAYER	
IETF **Internet Engineering Task Force**	Standards Developing Organization for internet protocols (such as IP, TCP, HTTP, and QUIC)
ICANN **Internet Corporation for Assigned Names and Numbers**	Organization that develops policies for the distribution of Top Level Domains and addresses
RIRs **Regional Internet Registries**	Five regional organizations that distribute network address (ASNs) and Internet Protocol (IP) addresses to ensure that all numbers used on the internet are unique
W3C **World Wide Web Consortium**	Standards Developing Organization producing web standards (for example, for HTML, APIs, or accessibility)
TLD **Top Level Domain registries**	Organizations that administer Top Level Domains (such as .com, .net, .gay, .amsterdam, etc.)
PHYSICAL LAYER	
IEEE **Institute for Electrical and Electronic Engineers**	Professional association that sets standards for networking (such as WiFi and Ethernet)
3GPP **Third Generation Project Partnership**	Umbrella organization for regional groups that facilitate the development of telecom standards (such as those for 3G, 4G, and 5G)
ITU **International Telecommunications Union**	United Nations body regulating and standardizing radio and telecommunications
GOV **Governmental and intergovernmental regulators**	National and supranational regulators that develop and enforce laws and rules passed by governments
NO **Network operators**	Organizations building and maintaining the physical and virtual networks that facilitate communication

2. Internet governance organizations have distributed functions and govern by distributed processes.

The protocols and designations for connections across the internet are determined by the Internet Engineering Task Force (IETF). Standards are set to allow different networks to talk efficiently with each other. However, a standard is not the same as its implementation. For instance, all web browsers will display a website looking basically the same way, even though browser technology varies per product (such as Chrome, Explorer, or Safari) and operating system. When each system follows the standard specifications, they should all interoperate smoothly and traffic will continue to flow, despite the varied implementations.

The IETF created the six protocols that ensure an email can travel from sender to recipient through a series of authenticated, secure steps that keep senders and receivers safe from surveillance and impersonation. When email became one of the most successful and enduring applications of the internet, so did the risks associated with it. Phishing, eavesdropping, and fraud are critical threats that most could not have imagined when people began sending "electronic letters." But the system that manages and secures your email only works if your email provider has implemented all of the core protocols, and many providers have lagged behind, claiming that full implementation adds overhead and cost.[19] Furthermore, authentication and validation create added complexity because they depend on multiple actors across the internet ecosystem.

Because humans are notoriously bad at remembering long numbers, the Domain Name System (DNS) is used to help connect us to our favorite sites and services. This system translates the complicated IP addresses, e.g., 2001:db8:0:0:0:0:2:1, into human-readable domain names like "example.com." The Internet Corporation for Assigned Names and Numbers (ICANN) determines who manages the services for each "Top-Level Domain" and what the preconditions are for operation.

Domain management may seem like a simple function for common domains such as .com, .org, or .uk, but governance choices about who can offer services and on what terms have big implications for access, privacy, and freedom. Consider the potential harms or conflicts in decisions about domains ending .gay or .islam, for example. A significant debate has also emerged over the

19 Such as STARTTLS, SPF, DKIM, DANE, DMARC, and DNSSEC. You can learn more and test the security of your own email here: https://internet.nl/test-mail/.

.amazon domain and who should own and operate it—the Amazon corporation or the governments of the countries along the Amazon River.

As internet traffic moves from device to network, and from network to device, other systems support the connections—and points of potential failure—in the data flow. The Regional Internet Registries, for instance, provide subsets of regional IP addresses to individual networks, which communicate via Internet eXchange Points and pass internet traffic down to the IP addresses of individual devices. This all happens within milliseconds.[20]

The consequences of governance through an open, multistakeholder, industry-centric process instead of a government-driven multilateral process are not simply good or bad. It's complicated.

Taken together, these protocols, dependencies and decisions become a labyrinthine infrastructure, crowded with actors and even more so with risks. Meanwhile, the process of internet standard-setting remains largely voluntary. Sometimes standards are agreed to in governance bodies, sometimes a technology is developed and adopted so that it becomes a de facto standard—without or before any formal process. Examples of voluntary but formally set standards include widely used internet protocols such as HTTP, DNS, IP, and TCP, among many others. Examples of de facto standards include BitTorrent—developed 20 years ago by a programmer frustrated with file transfer speeds—and MP3, which began in the 1980s in an academic project focused on compressing the size of digital files.

Internet governance organizations develop their standards and policies through email lists, video conferences, and in-person meetings. While each organization's procedures are distinct, in general the contours of the decision-making process are similar: New issues or proposals require a venue, i.e., is there a group already working on the topic or must a new working group be established? After a group begins working on a topic, there is usually a period of document drafting and revision until a consensus is reached. Once consensus is reached, the document goes through different phases of review before it can become an official policy. In IETF, it takes an average of three years for a Request for Comment to become a fully developed policy. The ICANN policy process takes a year on average. Even after a new policy or technical document is fully developed, full implementation is in no way guaranteed.

20 The Regional Internet Registries (RIRs) assign unique addresses to independent networks known as Autonomous Systems (AS). Each AS in turn distributes unique IP addresses to the devices on their networks. This enables data to find its way from IP address to IP address until it reaches its destination address.

3. Decentralization—and resistance to new approaches—have been hard-coded into internet governance since the beginning.

In the 1970s, before there was the internet as we know it now, one could safely assume that standard-setting for transnational communication networks would be done in bodies such as the International Telecommunications Union or the International Organization for Standardization (ISO). By the end of the 1970s, the ISO was developing an architecture that would overhaul all previous communication networks, the so-called Open Systems Interconnection (OSI).[21] In many computer science textbooks this 7-layer OSI model is still used to explain how modern digital information networks work; the OSI architecture itself, however, never saw the light of day.

By the beginning of the 1990s, there were two competing information architectures: OSI and TCP/IP, a newer protocol developed by the Internet Engineering Task Force, which was by then about five years old. As engineers planned for the development of a new internet protocol, the decision effectively became a contest between ISO, an organization that drew all its members from national standards setting or, and the IETF, an organization in which anyone can freely participate. When IETF engineers suspected that the members of their own oversight body had struck a deal with OSI to put the new version of the Internet Protocol under OSI's control, the IETF members staged a mutiny and removed their oversight body from the standards process. TCP/IP went on to become the most used connection protocol. The IETF had outplayed state-centered organizations.

This seems like a story of how a merit-based, multistakeholder, consensus-based body outperformed an unwieldy, old-fashioned, government standards body. While it is true that ISO was defeated and OSI was never fully developed, the TCP/IP protocol suite published by the IETF—cannot be called a total success. For instance, the IPv6 protocol, an evolution deemed crucial for the internet since the 1990s, is still not in use on two thirds of the web's most popular sites.

4. The internet governance regime and the laws and policies of nation-states have always been in a dialogue.

Outside the technical and organizational layers of the internet's governance regime sit the institutions whose policies continue to shape the development

21 Russell, 2006.

As policy shapes new technologies, new technologies in turn demand new processes of standardization and governance.

Those processes create norms that inevitably find their way into policy practices.

and regulation of technology. And while the particular culture and processes that govern the present-day internet may seem entirely fixed, this is far from the case. The governance of communication networks has informed the development of technologies, regulations, and institutions since 1865, when the International Telegraph Union was established to regulate and standardize transnational telecommunications. As policy shapes new technologies, new technologies in turn demand new processes of standardization and governance, and those processes create norms that inevitably find their way into policy practices, and sometimes into challenges from courts and legislatures.

The interplay between government initiatives and multistakeholder governance is thus neither new nor controversial (indeed, it is how the internet began). Two recent examples from China underscore the commonplace but complex nature of government/governance interactions.

In a surge of standard-setting activity since the 2010s, Chinese actors have sought to standardize a new internet protocol and have introduced a wave of new 5G technologies. The protocol, dubbed "NewIP" and later renamed "Future Vertical Communications Networks," failed to be standardized, amid criticism that a government-issued standard could help shift power toward states and undermine the rights of users. In the telecom sector, on the other hand, Huawei has become the dominant developer of 5G equipment and as of 2020 China leads the world with nearly 33 percent of 5G-related patents.

Given the comparative alarm with which observers met China's proposed internet protocol, one could ask if that alarm was based more on the technology itself or more on US and European fear over China's advances as a world hegemon through innovation, subsidized labor, and government intervention in industry. The question seems reasonable in light of earlier similar government efforts in Europe to standardize the Global System for Mobiles, and in the United States during the production of the internet itself.

The example is instructive for the dynamicity it reveals between the governance of infrastructure and the intervention of governments. As we investigate the resistance of internet governance regimes to new norms, we must also bear in mind that infrastructure and its governance are proxies for the interests of countries and corporations—these balances are always contested and always in flux. With global tensions escalating between technology companies and governments, an examination of the internet's governance regime appears even more timely.

III. CONSENSUS AND RESISTANCE

The internet infrastructure is governed through a process that is open, deliberate, and notoriously resistant to change.

Like water and electricity, the internet has become an indispensable utility. It is crucial for the right to health, safety, information, expression, and association, among many other human rights. As the lives of individuals and societies become more deeply entangled with the internet, it becomes increasingly necessary to weave principles of public interest and accountability into the processes and practices that maintain the internet itself.

Transnational internet governance has supported the internet's countless positive contributions to society and communities, but the internet infrastructure is also being leveraged on a daily basis for censorship, surveillance, and discrimination. There are vulnerabilities and biases deeply embedded in the internet infrastructure. The best way to change this is to challenge and then change internet governance practices.

Internet governance organizations and practitioners are well aware of the importance of the internet infrastructure and its complexities, which makes it daunting to add societal considerations to the mix. But to avoid these increasingly urgent questions would be to undermine the public interest and, ultimately, the legitimacy of the internet governance regime itself.

Transnational internet governance has supported the internet's countless positive contributions to society and communities, but the internet infrastructure is also being leveraged on a daily basis for censorship, surveillance, and discrimination.

It is because so much relies on the internet, and its current form, that many are hesitant to make significant changes. Many of its component networks developed organically, and engineers around the world all have their own assumptions, expectations and—among some—fervently held opinions about how the system will and should behave.

In fact, it is not easy to determine what dependencies exist, what will break if changes are made. A good example of this are routers that filter traffic based on the protocols they know. This means that they do not recognize new protocols, which harms the very nature of permissionless innovation. This is why the Secure Transmission Control Protocol, which took 15 years to develop, and worked perfectly "in the lab," has never been deployed on the internet.[22] This is an example of how the lack of a centralized authority affords freedom but does not allow for accountability. "Why was the world created in six days?" an engineer asked me once, then answered, "because there was no pre-installed user base," i.e., no standards, habits, or obstacles to take into consideration.

The many practical and technical challenges to upgrading the internet sit alongside an equally complex cluster of cooperative, economic, and cultural challenges. Thousands of companies and engineers have a vested interest in the current incarnation of the internet. Exactly what makes internet governance so effective, namely the minimal mandate of the limited scope of increasing interconnection and interoperation between devices, things like collective action in the public interest are challenging and are not the norm.

Especially when a proposal to take the societal consequences of a particular technology or policy into account could lead to a decrease in the interconnection or interoperation, it is almost certain that such a proposal would be rejected. Also, existing norms that hamper the increase of interconnection and interoperation are subverted.[23] The result of these layers of resistance is a norm of extremely incremental development and—bluntly—a culture of resistance to new cooks in the kitchen. Compounding these dynamics of resistance is the homogeneity of gender, age, and race in the internet governance organizations, which are dominated by white American and European engineers, while the more technical groups are overwhelmingly male. The historical lack of diverse or dissenting voices has bred habits of thought and debate that are long-standing and deeply ingrained, though some shifts are observable over the last couple of years.

Rollouts for new security protocols that could make the internet safer are equally subject to the painstaking pace of change. Even the update to the

22 ten Oever, 2021.

23 ten Oever, 2020.

internet's most basic routing protocol, IP (for "Internet Protocol") is taking more than 25 years to roll out across the entire network. Everyone knows the internet would be better if IPv6 was deployed everywhere. Everyone knows it has to be done. But no one wants to carry the burden of ironing out every bug and performance issues. Meanwhile, the shortage of IPv4 addresses has spawned a trade market of its own. The gap between decisions and consistent, assured implementation has human and financial costs.

To help create a path toward internet governance that is better wired to account for societal impacts and the public interest, it is important to understand the format and culture of its current operations. The defining characteristics of the governance bodies—consensus building, voluntary standards, multistakeholder governance, and an often insular expert culture—provide opportunities for insight, and several potential avenues for adaptation.

1. The open and consensus-driven governance of internet infrastructure drives connectivity for networks but limits the scope and capacity of governance.

The many practical and technical challenges to upgrading the internet sit alongside an equally complex cluster of cooperative, economic, and cultural challenges. Thousands of companies and engineers have a vested interest in the current incarnation of the internet.

The Internet Engineering Task Force has always had an unofficial battle cry: "We reject kings and presidents, we believe in rough consensus and running code." It seems an unlikely motto for an institution that sets the norms for a market worth roughly $50 billion, but the tension between command and consensus—and between compliance and cooperation—defines the power of the internet governance model, and also its weaknesses.

Through deliberation, members of internet governance organizations can cooperate to reach practical solutions, even when there are competitors or parties with their own agendas at the table. Consensus-building has worked particularly well in internet governance because the primary shared objective among participants has been so strong: to increase the size of the internet through interconnection of more networks and services. This is the value they seek to create and the narrow focus they have sought to preserve.

The governance bodies are an important mechanism for industry self-regulation, but they remain open to anyone. This reflects the spirit—and the idealism—of the early internet engineers, who believed that connectedness, openness, and growth were all positive values and all supported each other and the public interest. Indeed, many have argued that the internet was a tool for democratization, and said its decision-making practices were promising models of multistakeholder governance.

The discussions in internet governance organizations are often highly specialized, littered with acronyms and references to past events, protocols, policies, and anecdotes.

It takes a lot of time to build up the knowledge, experience, and relationships to be—and feel—welcome as a full contributor.

People believed that the internet could have "no permanent favorites," and that its distributed design would be a natural deterrent to centralization.[24] The commercialization and privatization of the internet at the beginning of the 1990s was expected to bring about innovation and competition, but, in practice, it has led to the emergence of oligopolies.[25] In all significant submarkets, such as networking equipment vendors, "Top-Level Domain" registries, and network operators, a few large corporations are dominant. Today, these companies have a disproportionate influence on internet infrastructure, and vast resources to produce technologies and policies, and also to send people to participate in the governance process.

Anything that is not in the interest of a significantly represented stakeholder group will not move forward. With the private sector the best-represented stakeholder in all internet governance bodies, the prospects are slim for any proposal that does not advance the dominant players' business models.

The concentration of power inevitably affects the consensus-based governance discussions. Anything that is not in the interest of a significantly represented stakeholder group will not move forward. With the private sector the best-represented stakeholder in all internet governance bodies, the prospects are slim for any proposal that does not advance the dominant players' business models.

There are also many online technologies that do not get standardized, resulting in "walled garden" platforms like Facebook or the Facebook-owned WhatsApp. And while email itself is still a federated model in which people can communicate across multiple services, Google's Gmail has such a huge share of the market that Google can set de facto standards. Other email providers will always want to ensure that Gmail users receive their emails, so they will adapt to accommodate Google's choices.

Walled gardens are the reason you may have only one email app on your phone, but multiple messaging apps. And because WhatsApp, Telegram, Signal, Wire, and Twitter DMs do not interoperate, users cannot easily manage all their private message data and much of that data resides privately held data silos: the opposite of individual control over one's information.

It is in the public interest for technologies to be standardized in an open setting with input from a variety of stakeholders, instead of standards set de facto by transnational corporations or local lawmakers. A proliferation of standards, processes and data streams also makes it harder to analyze the impact of any new policy, and even harder to understand how it interoperates with other parts of the infrastructure. Therefore, it is all the more important to cement the expectation of impact assessment when new policies and technologies get considered for standardization.

24 Internet Society, 2012.

25 Cowhey, Aronson, and Richards, 2009; Van Schewick, 2012.

2. The voluntary standards set for internet infrastructure enable cooperation but reduce enforcement and authority.

The rules guiding the internet's infrastructure are effective largely because they prioritize connectivity over uniformity or enforcement. The voluntary nature of internet governance lets competitors collaborate on interoperability, which enables the overall network to grow. The internet's governance organizations and the people who drive them have been rigorous—even zealous—in this narrow focus.

Voluntary standards reduce friction and promote the expansion of the internet, but they can also lead to policy challenges. When new security protocols are rolled out, for instance, or new measures arise to fight bots or spam, internet governance does not provide a mechanism for coordinated enforcement. As with the example of Status Code 451, a confirmed standard to support human rights or access is not an affirmative position to preserve those values, much less a mechanism to do so.

Another challenge of the voluntary regime is that even when governance decisions are made, this is no guarantee new standards will be implemented. The same efficacy that enables sufficient market coordination is insufficient to ensure coordinated adoption.

Because of this gap in capacity, the internet governance regime may be losing its force—even legitimacy—with other stakeholders. Increasingly, new technologies and policies are being developed by corporations or governments outside of the governance regime. The General Data Protection Regulation (GDPR), for instance, was created and promulgated within the European Commission and has required significant changes in the WHOIS registry of domain owners managed by the Internet Corporation for Assigned Names and Numbers, and while the QUIC protocol was standardized by the Internet Engineering Task Force, it was initially created by Google.

In this sense, internet governance can become a forum for reactive coordination among heterogeneous actors, rather than a governance regime. The proactive mandate of internet governance has—conventionally—been only to increase interconnection and interoperation. This is another reason why strengthening the review of societal impacts has proven very difficult thus far. The self-limiting scope of the governance institutions, and the lack of enforcement mechanisms, have also fueled governments' doubts about the effectiveness of internet governance.

3. As national governments scramble to regulate the internet, the multistakeholder governance of the internet faces new—but necessary—pressure.

From Roman roads to railroads, global communication networks have often been proxies for power but, historically, government has played the central role shaping or regulating these systems.

The case of the internet is different. In the globalizing world, changes "are being written, not in the language of law and diplomacy, but rather in the language of infrastructure," to quote Keller Easterling.[26] Whoever manages the internet's infrastructure sets the terms of governance, deliberately or by default—at least until lawmakers catch up. Technology companies have created most of the internet's physical and digital infrastructure. While the internet is often described as a public space or a public square, it is actually a mosaic of overwhelmingly privately owned infrastructure. The internet is more like a cluster of interconnected malls and garages than a public space.

The internet governance regime may be losing its force—even legitimacy—with other stakeholders. Increasingly, new technologies and policies are being developed by corporations or governments outside of the governance regime.

These corporations also have dominant representation in the infrastructure governance organizations. Staff members and colleagues of the hardware and software makers comprise a large proportion of the active governance bodies (though it is customary for members to participate as "civilians" not as company representatives).

Thus, the same shift in technical maintenance of the internet infrastructure that took place from the late 1970s through the late 1990s—from governments and universities to private companies—also took place in the governance of that infrastructure, as company representation grew in the governance bodies.

Some observers have said the multistakeholderism of internet governance is a significant step in democratic participation, but internet governance researcher Jeanette Hoffman wrote in 2020 that neither formal nor informal authorities "like to be held accountable, and bottom-up consensus proves to be as contested as other modes of decision-making. Multistakeholderism," she writes, "it turns out, is less a regulatory approach than an end in itself; an end that shifts attention to process and requests a high degree of belief and loyalty from its followers."

The consequences of governance through an open, multistakeholder, industry-centric process instead of a government-driven multilateral process are not simply good or bad. It's complicated. Multistakeholder governance has allowed not only for faster innovation, but also for more democratic

26 Easterling, 2014.

deliberation, enabling actors with different interests and backgrounds to collaborate to build a global network without a central point of failure.

At the same time, each governance organization has its own narrow remit, and the private companies represented do not have the public interest as their main objective. So private actors have been able to say that discussions about the societal and political implications of technology have no place in internet governance. And while most of the governance organizations have social good and the public interest written into their mission statements, there continues to be no standardized practice of social impact assessment for new tools and policies under review. The governance infrastructure of infrastructure governance does not yet have human rights considerations built in.

Between the narrow focus of governance bodies on preserving interoperation and interconnection, and the limits of self-regulation by private companies, it has proven nearly impossible to strengthen societal impact considerations without external pressure. Meanwhile, the world has faced the growing urgency of the internet's potential harms, and the network's vulnerabilities to misuse, misinformation, and attacks on basic freedoms like privacy and free expression.

It's no surprise, then, to see an uptick in new internet laws and regulations from the United States to Germany, from Russia to Brazil. After years of deregulation, there seems to be a gusto for oversight. Indeed, one of the main criticisms of internet governance from world capitals is that the responsible organizations have not taken societal norms or consequences into account, even as new crises of public safety and human rights reveal the dangers of an internet without accountability.

For years, the International Telecommunications Union (ITU), the UN's special agency for Information communication technologies (ICTs), has also sought to increase its influence on the governance of the internet. However, in the ITU only nation-states have a vote, not all documents are publicly available, and the process is not open to everyone. Furthermore, some of the internet proposals fielded by the ITU in the past contained clear threats to privacy and free expression.

All of this suggests that the influence of internet governance regimes as we know them could be giving way to the international multilateralism that traditionally governs areas such as trade or, increasingly, climate. External pressure from lawmakers around the globe could combine with the growing public alarm about misinformation and hate speech online to galvanize governance bodies into tackling the hard issues that remain insufficiently addressed.

However, the pressure on multistakeholder governance should not limit a thoughtful analysis of its effectiveness or its successes. If the world's capitals rush into new rules for oversight, without coordination or sufficient information, such a trend could harm the fabric of the internet in even worse ways.

4. The internet's governing bodies are more accessible to some groups than others—logistically—creating participation barriers for many who could speak for economically or politically disenfranchised groups.

When compared to other global governance processes, participation in internet governance discussions is remarkably easy. Internet governance organizations are organized in the same democratic spirit that drove the early internet itself. Most require only an email address to participate. Remote participation is often the norm (even in non-COVID times). Discussions are well documented and archived.

The same culture that resists—or rejects outright—the consideration of human rights as part of standards development also resists the kinds of change that would open doors and widen the governance discourse.

But though this openness reflects the aspirations of "the Net's" early days, in practice it has also reflected the mistaken assumptions—and the naiveté—of the internet's utopian era. To be a full participant in the governance process requires resources and even privileges that not all stakeholders possess. There are barriers of geography, expense, and language, as well as social barriers involving expertise and in-groups.

In normal times, most participants attend in-person meetings, and while many meetings are free, there still are significant airfare and accommodation costs. Furthermore, five days meetings, often preceded by side events and preliminary gatherings, can be prohibitive for participants with a traditional work week. And though one can fully attend online, the meetings are an important place to build relations of trust and familiarity that can be crucial in the actual governance negotiations.

The discussions in internet governance organizations are often highly specialized, littered with acronyms and references to past events, protocols, policies, and anecdotes. Sometimes there are so many abbreviations in a sentence that one can almost lose track of what language is being spoken. This habit of jargon comes partly from the specificity of the topics, but it also reflects the members' varied backgrounds, internet governance spans many different disciplines and communities and the polyglot of acronyms, though it can raise the barriers to entry, serves as a bridge between the actors. Whatever its practicalities, internet governance lingo can be quite exclusionary, which contrasts with the acclaimed open design of these processes. It takes a lot of

time to build up the knowledge, experience, and relationships to be—and feel—welcome as a full contributor.

It is perhaps unsurprising that the people with the greatest capacity to participate in internet governance processes tend to be from the United States and Northern Europe.[27] Participants are primarily English-speaking and live in places that tend to have reliable electricity and high-speed internet access. Travel and travel visas are easier for them to manage than for many of their African and Asian colleagues, for example. And many of them have their travel and accommodation supported by a corporate employer or university, an advantage that is often unavailable to an NGO staffer, advocate, or unfunded researcher.

These disparities in accessibility hamper the effective inclusion of voices and viewpoints that would help to move consideration of technology's societal impacts further into the mainstream of internet governance.

5. Internet governance still lacks diversity in who is represented—and who is made welcome—with significant impacts for policies and technologies.

The IETF's guidance document for newcomers warns that members can be "surprisingly direct, sometimes verging on rude."

To newcomers and many non-engineers, internet governance meetings can feel more like a clubhouse than a policy body. One gets the impression that participants have known each other for many years, which actually is often the case. Discussions take place entirely in English, and questions, interruptions, and debates can be quite fierce in the meetings and mailing lists where policies, standards and proposals are submitted and exhaustively analyzed.

Governance participants with long tenure often function as de facto gatekeepers for new issues—and as models for group culture, which in turn continues to hamper diversification. As importantly, the members with the longest tenure and greatest influence are mostly American and European technologists in their 40s and 50s, are disproportionately male and largely white.

When a topic is "too political," members often cite the need to maintain a narrow remit in internet governance. This argument has been used to reinforce existing practices during discussions about diversity and sexism, and in the current debate over terms with historically racist connotations.

The governance organizations have acknowledged by now that they lack diversity, and they are trying through various methods to address the issue,

27 For instance, see this breakdown of IETF "Requests for Comment" by country of author: https://www.arkko.com/tools/rfcstats/d-countrydistr.html.

including the development of Codes of Conduct for live and virtual conversations.[28] In the Internet Engineering Task Force, efforts are underway to reform the more combative, exclusionary aspects of the culture, but research suggests that these dynamics persist. Many in the membership of IETF still believe that "the roughshod norms are crucial to getting the job done," according to PhD researcher Corinne Cath, who has noted the IETF's proud reputation as a forum of "loud men talking loudly."[29] The IETF's own guidance document for newcomers warns that members can be "surprisingly direct, sometimes verging on rude."[30]

For the internet governance organizations and their members, the idea of a more welcoming culture may not be an annoyance but an existential requirement.

In the public discussions where these groups deliberate, some contributors seek to blame the lack of diversity on external factors such as disparate education levels or language barriers, often adding the governance processes have always remained open to all interested participants. Such complaints—which sound archaic even on their own terms—ignore the logistical barriers mentioned already, as well as the bias toward the status quo among many internet governance participants. A number of these experts are not just defenders of the internet's original precepts and processes, they are actually the same people who built the internet and established those norms. Like many founders, they look favorably on the approaches that helped drive their historic, world-changing successes up to the present day.

As a result of these interlinked dynamics, the same culture that resists—or rejects outright—the consideration of human rights as part of standards development also resists the kinds of change that would open doors and widen the governance discourse. This cultural resistance—as deeply-rooted in some places as physical infrastructure—in turn slows the adaptations that would make discussions of human rights and the public interest more effective in the self-governed hubs of internet development.

The same group that stands squarely against becoming "the protocol police," may have grown into process police to their own detriment. As Corinne Cath concludes, "IETF's lack of diversity is a direct function of the IETF's culture."[31]

As culture wars surge internationally over race and gender biases—and the linked economic and social inequities—internet governance organizations

28 Cath, 2021.

29 Cath, 2020.

30 ten Oever and Moriarty, 2018.

31 Cath, 2020; a forthcoming Ford Foundation report by Corrine Cath explores the tension between internet infrastructure governance and the harsh realities of the current governance culture in further depth.

face pressure to adapt from both external and internal sources. Transnational corporations and governments have the power to drive internet infrastructure without the existing governance bodies, through new technologies that set de facto standards and laws that govern "at" the internet not "with" it. Meanwhile, internal disputes over inclusivity and combative culture threaten to fracture governance bodies from the inside. For the internet governance organizations and their members, the idea of a more welcoming culture may not be an annoyance but an existential requirement.

The prospects for culture change in the internet governance community are better than they have ever been, so it is important to think today about what might happen as governance processes become more open to traditionally sidelined points of view. Opening the door is not the same as taking away all thresholds or leveling the field for new players, and diversity is not the same as accountability. Both are needed, and each strengthens the other, but a diverse community can still be unaccountable. Ideally, the wider range of perspectives that a diverse community offers can also increase accountability, building a stronger circuit of feedback among governance institutions, governments, companies, users, and advocates.

IV. FUTURE PATHS

The same interdependence that makes the internet transformative and durable can enable cooperation that elevates human rights for all who depend on the internet's infrastructure.

The internet is at a crossroads for its governance practices. Even as its potential to enable harm becomes more obvious, the status quo of multistakeholder consensus influenced by private companies thwarts serious consideration of human rights or public interest outcomes (beyond the presumed value of more interconnection).

At the same time, a shift to more fragmented, multilateral intervention by nation-states is not likely to improve governability or deter many common abuses.

The integration of human rights considerations into policy and standardization processes will require the experience and expertise of all stakeholders, ranging from engineers who create the hardware and software, governments whose mandate and experience includes protecting human rights, civil society, and community members whose advocacy is grounded in lived experience, and researchers who can assess outcomes and help imagine new infrastructures and solutions. Free and open access to technology and to standard-setting is also crucial to preserve the human right of everyone to enjoy the benefits of scientific progress.

We have witnessed some progress in areas such as privacy and security, net neutrality, and broadband penetration, but it is not enough, as recent crises over misinformation and free expression vividly demonstrate. The sector needs cross-stack and multistakeholder collaboration to align incentives and realize an infrastructure that supports equity alongside connectedness. A truly global infrastructure, that will be as secure for the poorest users as it is for the wealthiest, as functional for those using non-Latin scripts as it is for English speakers. An infrastructure that is human rights enabling by default and that acts as a firewall to make human rights violations harder, more expensive, and more visible.

It is important to note that such adaptations will not make the internet exceptional. These changes in culture and practice would integrate the internet sector with government and corporate accountability processes that undergird the manufacturing, garment, and natural resource sectors, among others. The UN Guiding Principles offer a valuable initial model, and the internet governance community can seek to further these practices, for example through human rights impact assessments that also prioritize stakeholder voices from every level of power and access.

No stakeholder group, no corporation, no government, no international organization or university can build a global equitable human rights-respecting infrastructure on its own. The distributed design of the internet foregrounds the importance of interdependence, and that is a feature to be supported, not undone. The work to make human rights an inherent and non-voluntary part of internet infrastructure will increase interdependence, strengthening both the network and the fabric of society.

A truly global infrastructure, that will be as secure for the poorest users as it is for the wealthiest, as functional for those using non-Latin scripts as it is for English speakers.

An infrastructure that is human rights enabling by default and that acts as a firewall to make human rights violations harder, more expensive, and more visible.

Opportunities

Internet governance bodies and all stakeholders can consider a range of approaches that strengthen governance practices to more fully safeguard human rights and uphold the public interest.

Internet Governance Organizations

- Normalize the consideration of societal and structural impacts for new policy and technology proposals, using the United Nations Guiding Principles for Business and Human Rights, and their human rights impact assessment process as a template.
- Pilot new design practices that seek and incorporate the needs of impacted communities into the development of proposed standards. The perspectives of the varied end users with varied vulnerabilities should not simply be approximated by private sector technologists.[32]

Civil Society and Researchers

- Broaden the spectrum of engagement between civil society and internet governance organizations and companies, for instance by volunteering for positions within the governance bodies, which can demystify governance processes, increase interconnectedness between traditionally siloed social networks, and equip advocates with a fuller vocabulary.
- Establish cross-stack collaborations between civil society and technologists, network operators, and other groups impacted by internet governance proposals, in order to strengthen the substance and viability of new recommendations. Standardization is about building support for your proposal with other actors. Civil society should also partner with researchers to conduct power analyses that help identify opportunities for advocacy and future collaboration.
- Invest in strategic projects with realistic time cycles. Participating in internet governance can be difficult, but it gets easier over time; do not expect outcomes in less than a year. Governance processes are often unwieldy and unpredictable, so it is important to embrace adaptive strategies that enable advocates to be responsive, not merely reactive.

Governments

- Implement the United Nations Guiding Principles for Business and Human Rights more fully in technology policy, including the use of human rights impact assessments. The UNGPs are the world's most established corporate accountability framework.

32 Nottingham, 2020.

Inventing new frameworks is more likely to turn into "ethics-washing."

- Increase direct engagement with internet governance, rather than focusing exclusively on industry-based legislation. Stronger laws and regulations will continue to impact generations of tools, but it is still easier to address technology issues before tools are adopted and deployed.
- Update procurement policies at every layer of the internet infrastructure. Governments are the largest buyer of goods and products, especially for infrastructure and large-scale technologies. Therefore, procurement policies should include, for example, public availability of contracts and tech specifications, human rights and environmental impact assessments, incentives for open software and open hardware, and other measures for transparency and accountability.[33]
- Champion cross-sector collaboration among stakeholders in internet governance, and diversification of participants in governance organizations. Through funding and facilitation for groups with shared goals—such as stronger data encryption, or protection of personal data from networks with weak privacy—governments can empower communities, partner states and civil society to engage in key governance decisions. Governments can also be thoughtful about who they advance for positions on delegations when that is the best available way to engage in internet governance processes. By advancing a diverse participant base—and pushing for enabling culture shifts within the governance institutions—governments can use their influence to change internet governance from the outside and the inside in parallel.

Technologists and Tech Companies

- Embrace the UNGPs, as sectors including finance, telecoms and the garment industry have done. By adopting these principles and ensuring full implementation, the technology sector can clarify where and how infrastructure impacts human rights and what the proper paths are for communities and individuals seeking redress.
- Conduct human rights impact assessments (HRIAs) of new and newly deployed technologies, from the development phase through the entire product life cycle. HRIAs are robust processes that include stakeholders from "end-user" communities and more vulnerable populations. Social impact assessment processes should also involve engineers and coders, not only lawyers and compliance experts; the goal is supporting the public interest, not mere compliance.
- Invest in ongoing collaborations with civil society, researchers, and governments. If your company believes civil society organizations do not understand your work or your challenges, invite them to learn. Seek opportunities for joint projects that address the full "governance stack" to develop better understanding and better solutions.
- Contribute to the diversification of internet governance. Send new employees and people from diverse backgrounds to internet governance meetings. Use company resources to lower the barriers for participants with geographic or budgetary limitations, and to nudge company culture further toward engagement with multiple perspectives.

33 "Build Better. Build Right. Our Focus on Infrastructure," Open Contracting Partnership, accessed May 18, 2021.

Donor Groups and Agencies

- Change funding cycles for human rights and technology programs to support engagements over five to ten years instead of 12 to 24 months. Without sustained investment beyond the usual budget years and performance metrics, the philanthropies, governments, and multilaterals best positioned to shift the governance of the internet may remain trapped on the sidelines.
- Facilitate and reward cross-sector collaboration. Donor groups wield a unique power to convene conversations that bridge differences and disciplines. In this role, donors can promote internet governance as a platform for aligning the interests of more vulnerable communities, civil society groups, governments, and corporations through joint projects, research, and other forms of cooperation.

ACKNOWLEDGEMENTS

I want to thank Corinne Cath-Speth and Jed Miller for their excellent support in writing this paper—however, all mistakes are mine. I also want to thank Michael Brennan and the Technology and Society program at the Ford Foundation for their support of civil society's engagement with the internet infrastructure and support in the researching and writing of this report. I am deeply indebted to and inspired by public interest technologists around the world: you are the infrastructure of equitable change.

Credits

Editor: Jed Miller, 3 Bridges
Report Design: Michael Wiemeyer, Designlounge
Illustration/Creative Direction: Greg Straight/Mel Flanagan, Nook Studios

Illustration adapted from Niels ten Oever and Giovanni Lombardi (2020), inspired by XPLANE ICANN Three Layers of Digital Governance (2015).

Supported by


FORDFOUNDATION

REFERENCES

Braman, Sandra. 2009. “Internet RFCs as Social Policy: Network Design from a Regulatory Perspective.” Proceedings of the American Society for Information Science and Technology 46 (1): 1–29. https://doi.org/10.1002/meet.2009.1450460254.

——. 2010. “The Interpenetration of Technical and Legal Decision-Making for the Internet.” Information, Communication & Society 13 (3): 309–324. https://doi.org/10.1080/13691180903473814.

——. 2012. “Privacy by Design: Networked Computing, 1969–1979.” New Media & Society 14 (5): 798–814. https://doi.org/10.1177/1461444811426741.

Carr, Madeline. 2015. “Power Plays in Global Internet Governance.” Millennium 43 (2): 640–59. https://doi.org/10.1177/0305829814562655.

Castells, Manuel. 2009. Communication Power. Oxford, UK; New York: Oxford University Press. http://public.eblib.com/choice/publicfullrecord.aspx?p=472226.

Cath, Corinne. “What’s Wrong with Loud Men Talking Loudly? The IETF’s Culture Wars.” Hack_Curio. https://hackcur.io/whats-wrong-with-loud-men-talking-loudly-the-ietfs-culture-wars/.

——. 2021. “The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force.” Telecommunications Policy 45, no. 6 (July 1, 2021): 102144. https://doi.org/10.1016/j.telpol.2021.102144.

Cowhey, Peter F., Jonathan D. Aronson, and John Richards. 2009. “Shaping the Architecture of the US Information and Communication Technology Architecture: A Political Economic Analysis.” Review of Policy Research 26 (1–2): 105–125.

Doty, Nick. 2015. “Reviewing for Privacy in Internet and Web Standard-Setting.” In Security and Privacy Workshops (SPW), 2015 IEEE, 185–192. IEEE.

Easterling, Keller. 2014. Extrastatecraft: The Power of Infrastructure Space. Verso Books.

Hofmann, Jeanette. 2020. “The Multistakeholder Concept as Narrative: A Discourse Analytical Approach.” In Researching Internet Governance: Methods, Frameworks, Futures, edited by Laura DeNardis, Derrick L. Cogburn, Nanette S. Levinson, and Francesca Musiani, 249. MIT Press.

Internet Society. 2012. “Internet Invariants: What Really Matters.” Internet Society (blog). February 3, 2012. https://www.internetsociety.org/internet-invariants-what-really-matters/.

Mathew, Ashwin J. 2014. Where in the World Is the Internet? Locating Political Power in Internet Infrastructure. Berkeley: University of California. https://www.ischool.berkeley.edu/research/publications/2014/where-world-internet-locating-political-power-internet-infrastructure.

Meier-Hahn, Uta. 2014. “Internet Interconnection: How the Economics of Convention Can Inform the Discourse on Internet Governance.” In GigaNet: Global Internet Governance Academic Network, Annual Symposium.

Nottingham, Mark. 2020. “RFC8890—The Internet Is for End Users.” RFC Editor. https://tools.ietf.org/html/rfc8890.

Nye, Joseph S. 2014. “The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance.” Canada: Global Commission on Internet Governance. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Pohlmann, Tim, Knut Blind, and Philipp Hess. 2020. "Fact Finding Study on Patents Declared to the 5G Standard."

Russell, Andrew L. 2006. "'Rough Consensus and Running Code' and the Internet-OSI Standards War." IEEE Annals of the History of Computing 28 (3): 48–61.

ten Oever, Niels. 2020. "Wired Norms: Inscription, Resistance, and Subversion in the Governance of the Internet Infrastructure." Amsterdam: University of Amsterdam. https://dare.uva.nl/search?identifier=9dff56cd-0ec6-40fa-b136-105bed8ac243.

——. 2021. "The Metagovernance of Internet Governance." In Contested Power and Authority in Internet Governance: Return of the State?, edited by Blayne Haggart, Natasha Tusikov, and Jan Aart Scholte. Abingdon-on-Thames: Routledge.

——. "'This Is Not How We Imagined It'—Technological Affordances, Economic Drivers and the Internet Architecture Imaginary." *New Media & Society*. https://doi.org/10.1177/1461444820929320.

ten Oever, Niels, and Corinne Cath. 2017. "RFC8280 - Research into Human Rights Protocol Considerations." RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc8280.

ten Oever, Niels, and Kathleen Moriarty, eds. 2018. "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force." Internet Engineering Task Force. https://www6.ietf.org/tao.

Van Schewick, Barbara. 2012. Internet Architecture and Innovation. MIT Press.

Verhulst, Stefaan G., Beth S. Noveck, Jillian Raines, and Antony Declerq. 2014. "Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem." Centre for International Governance Innovation, December. https://www.cigionline.org/publications/innovations-global-governance-toward-distributed-internet-governance-ecosystem.

Zittrain, Jonathan. 2008. The Future of the Internet—and How to Stop It. Yale University Press.