Governance Challenges in the Global Digital Ecosystem

Eileen Donahoe

The internet has become the infrastructure of the global digitized society and is affecting governance in all realms. While digital technology has facilitated dramatic expansion of the freedoms of expression, association, and assembly globally, it has also created dramatic security vulnerabilities and threats to liberty. Before addressing governance innovations and challenges in the distinct but interrelated fields of internet governance and cybersecurity, several features of digitized society that make governance difficult need to be recognized:

- *Transborder Mode of Internet Operation:* An essential characteristic of the internet is its global, transborder mode of operation. This feature is testing the post–World War II international governance framework, which rests upon the construct of sovereign nation-states defined by physical borders. International humanitarian law (which defines the limits of legitimate state use of force in relation to other states) and international human rights law (which defines the obligations of governments to citizens and people within their jurisdiction) rest on the presumption that governments have sovereignty over people and activities within their jurisdictions defined by geography. The internet provides instantaneous transborder connectivity and extraterritorial reach—to governments and nonstate actors alike—without reference to geography. This feature presents new security threats and governance challenges. The constant transborder flow of information and data is creating confusion over who has jurisdiction over this data flow and on what basis. Prime examples of these jurisdictional conundrums can be seen in cases such as Google Inc. v. CNIL, the French data protection authority (regarding the "right to be forgotten"), and Microsoft Corp. v. United States (regarding extraterritorial access to data).

- *Digitization of Everything:* The rapid adoption of digital technology means that everything individuals say and do (in the connected part of the world) can now be tracked and monitored by government and private sector actors. This presents a variety of challenges to democratic governance and to the enjoyment of human rights. First, and most obviously, it undermines the right to privacy, which is more important to the exercise of fundamental freedoms than is often recognized. If everything an individual says or does can be tracked and monitored, it will have a chilling effect on what individuals feel free to say, with whom they feel free to meet, and what information they feel free to access online. Digitization of everything also risks inverting the basic democratic order in which sovereign citizens watch the government by instead ensuring that governments and the private sector can watch and monitor literally everything said or done by citizens and consumers.

- *Privatization of Governance:* As digital technology has infiltrated all dimensions of society, there has been a corresponding trend toward the privatization of governance, whereby private sector actors are taking on traditional governance responsibilities for security and liberty. Democratic

government is built on the notion of a social contract: sovereign citizens agree to be governed in exchange for protection of security and liberty, and government is accountable to the people. This notion of a democratic social contract is being disrupted. Digital platforms have essentially become the public square for citizen discourse, and private sector platforms effectively govern the limits of free expression through terms of service, community guidelines, and algorithms. Similarly, private sector actors currently own, operate, and secure most of the critical civilian infrastructure and house the data of citizens and consumers. (Facebook's recent commitment to take on information operations and inauthentic amplifiers reflects a private sector move into a traditional government area of responsibility for security.) But the private sector does not have formal accountability to the public.

Furthermore, under international human rights law, the primary obligation to protect and not violate the human rights of citizens and people within their jurisdiction rests with government. In 2011, the Guiding Principles on Business and Human Rights were adopted by the member states at the UN Human Rights Council. These guiding principles established norms for private sector entities to respect and protect human rights where their business operations affect the enjoyment of rights. Many private sector entities voluntarily embrace the responsibility to protect human rights where they can. But formal governance obligations to protect human rights rest with government under international law.

These three features of the globally digitized environment are challenging all governance actors and will need more attention, especially if existing international humanitarian law and human rights law norms are to survive into the twenty-first century.

INTERNET GOVERNANCE: LANDSCAPE AND INNOVATIONS

The starting place for a discussion on governance challenges and innovations in the realm of internet governance can be found in the critical distinction between governance of the internet and governance on the internet.

Governance of the Internet

Governance of the internet refers to policies, standards, norms, and practices that govern the technical layers of the internet itself—at the architectural/hardware layer or at the naming-numbering protocol/software layer. The animating energy within the internet's founding governance community was open, multistakeholder, and merit-based. The shared goal was to create a reliable, globally interoperable mode of instantaneous communication available to anyone who could connect. The early modus operandi of this internet governance community was to test the efficacy of technology protocols in open dialogue, based on whether they would serve the purpose of creating a stable, globally interoperable internet. The community would converge upon the technical solutions that garnered the most support.

A significant innovation in governance of the internet took place in 1998, with the creation of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN, sometimes referred to as the phone book or phone numbering system of the internet, was formed as a private sector, public purpose corporation in California. Policymaking at ICANN concerns issues such as generic names for top level domains (.com, .org, .edu) or country code names (.uk, .ca, .cn). The core function of ICANN

was and is to make sure that people anywhere can communicate via the internet through a stable unified global system of unique identifiers. To communicate on the internet, a unique identifier or destination—entered as a name and translated into a number—is needed so that intended recipients can be correctly located. As a governing entity, ICANN coordinates the activities of a variety of stakeholders, including domain name registrars and registries, that play different roles in this global system.

The multistakeholder model of ICANN is a prime example of governance innovation that does not rest exclusively on governmental decision-making. ICANN address management is done through a community of supporting organizations, advisory committees, and the board. It includes a governmental advisory committee, but government actors do not have the same presumed status as primary governance authorities, unlike in traditional multilateral forums.

In October 2016, the U.S. government transitioned away from its stewardship role for Internet Assigned Numbers Authority–assigned numbering functions at ICANN and handed off full responsibility for ICANN governance to the nongovernmental community. This move was based on an assessment that the community had demonstrated its ability to reliably manage global naming and numbering responsibilities since ICANN's founding in 1998.

Governance on the Internet

Governance on the internet refers to the broad range of policies, regulations, and laws that govern activity on the internet at the content, social, and political layers, such as government policies for taking down illegal content, rules on accessing user data or communications for law enforcement or foreign surveillance, or norms on cyber offense.

Traditional governance activities of government as they relate to protecting security and liberty come into play with governance on the internet, as do international humanitarian law and international human rights law. In June 2012, the first UN resolution on internet freedom was passed by consensus at the UN Human Rights Council. This resolution laid down the foundational concept that human rights need to be protected online as they are offline. Similarly, in 2013 (and again in 2015), the group of governmental experts at the UN General Assembly First Committee agreed on that international humanitarian law is applicable in the cyber realm. But governments have been struggling to articulate how to apply international human rights and humanitarian law in the cyber realm.

Furthermore, as noted earlier, international human rights and humanitarian law rest on the traditional presumption that governments are the primary actors. But private sector actors have taken on much of the responsibility for digital security and are effectively governing the public square. Therefore, the present moment is one of conceptual confusion about governing roles and responsibility on the internet.

During the Brazilian-led Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) in April 2014, the global internet governance community converged upon the idea that multistakeholder governance on the internet is feasible and preferable to traditional multilateral governance models. The NETmundial outcome document highlighted human rights principles and open, accountable governance processes as the shared basis for moving toward broader global multistakeholder governance. This moment coincided with German and Brazilian initiatives at the United Nations, taken after disclosures made by Edward Snowden, to bring human rights, democratic values, and the rule of law to governance on the internet (see, for example, joint Brazilian and German efforts at the UN General Assembly and the UN Human Rights Council on the right to privacy in the digital age).

However, this moment of enthusiasm for global multistakeholder governance on the internet seems to have passed. With the growing awareness of systemic cyber vulnerability, conceptual confusion has combined with fear of digital insecurity to bring a retrenchment of sovereign government control over activity on the internet. Furthermore, at the geopolitical level, leadership on multistakeholder governance has evaporated: the Donald J. Trump administration has not embraced the general concept of multistakeholder internet governance after the October 2016 transition. Brazil has stepped back from its global role as champion of such internet governance due to domestic political challenges. The German government has shifted emphasis to the disruptive effects of digital technology on democratic discourse and processes, as reflected in its draft law imposing steep fines on digital platforms for failure to take down illegal content within twenty-four hours. The German draft law has been criticized by civil society for its illiberal approach to the international human right to freedom of expression as well as for the threat the draft law presents to the core concept of platform immunity from liability that has facilitated the free flow of information globally.

The bottom line is that civil society is increasingly concerned that even democratically oriented governments are backtracking on exploration of innovative multistakeholder internet governance arrangements, and progress on commitments to apply universal human rights and humanitarian law principles in the digital realm has slowed.

CYBERSECURITY: LANDSCAPE AND INNOVATIONS

With digitization of everything and the collapse of the online-offline distinction, digital security runs through every dimension of security—national security, international peace and security, consumer protection, economic security, security of critical infrastructure, and protection for dissidents and human rights activists. The combination of digitization and the inherently transborder mode of internet operations presents extreme challenges for governance actors responsible for security, as criminals, terrorists, hackers, and governments anywhere now have instantaneous extraterritorial digital reach to affect the security of people anywhere else.

A daunting range of new security threats use cyber vectors of attack—from cyber to kinetic attacks on critical infrastructure or weapons systems to hacking of democratic discourse and election processes, global ransomware attacks on businesses or hospitals, and undermining the integrity of widely reliable data. Notwithstanding the benefits of technology, there is a growing awareness of systemic cyber vulnerability and society-wide digital insecurity and a general sense of the powerlessness of governments to protect against these threats.

Added to this sense of insecurity is confusion over the optimal relationship between public and private sector actors, given that the private sector is often better positioned to ensure the stability and security of digital infrastructure and to protect data or access data for security purposes.

The starting place for grappling with governance challenges in the realm of cybersecurity is recognizing that responsibility for cybersecurity needs to run throughout society and multistakeholder participation in cybersecurity-related governance is essential. Traditional governance actors tend to work in isolated frameworks and often do not understand the inherent interconnectivity among all dimensions of digital security. For example, only recently have national security experts come to appreciate the threat of doxing to national security or the threat of ransomware to economic security. Furthermore, security experts are increasingly recognizing that cyberattacks on small targets—such as on Google accounts that have not enabled two-factor authentication—can have dramatic consequences

for national and international security. The bottom line is that cybersecurity governance needs to incorporate all dimensions of society.

Several existing strands of work related to cybersecurity governance need to be reinforced, including development of state norms restraining offensive use of cyber weapons and public education on digital security. Interestingly, several private sector actors have pushed for leadership on this front. For example, Microsoft President Brad Smith has called for a digital Geneva convention to restrain state-sponsored hacking of civilians. While the likelihood of a treaty on any subject is low, this rallying cry could represent an important shift in recognition that cybersecurity is ultimately about protection of citizens, consumers, and civilians. Apple's CEO Tim Cook also has called for a massive public education campaign on fake news and has urged governments, private sector actors, and citizens to be more forceful in preventing disinformation from disrupting democratic discourse.

One state-led innovation in cybersecurity governance that took off with great potential but has since waned is the Freedom Online Coalition (FOC). The coalition, which includes thirty governments, was created in 2011 with the goal of ensuring that human rights are protected online as they are offline. FOC has shown some degree of multistakeholder leadership through working groups that included civil society, technologists, academics, and the private sector, but it has struggled to assert its influence globally as member governments struggle with bringing their own cyber practices into line with human rights principles. The FOC working group on "An Internet Free and Secure" sought to bring about a paradigm shift in the members' understanding of the relationship between freedom and security online. The working group developed a set of practical recommendations for a human rights–based approach to cybersecurity, identifying digital security as a critical dimension of the fight to protect freedom online. A core idea behind the recommendations was the need for states to recognize that digital security of citizens, consumers, and civilians is essential to national security and that protections of digital freedom and digital security are mutually reinforcing in the global digital ecosystem. Much more work needs to be done within the national security community, as well as in the general public, to bring about this paradigm shift in awareness about the symbiotic relationship between freedom and cybersecurity.

THE CHALLENGE: CLARIFYING OPTIMAL GOVERNANCE AND SECURITY ROLES IN THE DIGITAL REALM

Perhaps the most ominous threat in the global digital ecosystem, one that constitutes both an internet governance and cybersecurity challenge, is the threat to democratic governance from digital disinformation. Transborder information operations by nondemocratic forces, especially when combined with digital mechanisms that amplify the effects of disinformation on democratic discourse, are peculiarly daunting. This perplexing combination of instantaneous extraterritorial reach, connectivity of everything that is digitized, and confusion about governance roles when private sector social media platforms become the vector of attack, has wreaked havoc on traditional governing concepts in democracies. Figuring out the optimal roles and responsibilities of private sector technology companies and government in addressing digital disinformation will be essential to moving toward greater security. The challenge of the twenty-first century is to find a means of defending against digital disinformation without eroding democratic values and freedom.