CHAPTER 1

Governance by Infrastructure

Laura DeNardis and Francesca Musiani

From Governance of Infrastructure to Governance by Infrastructure

Injured victims of a Hamas-planned suicide bombing in Jerusalem were awarded hundreds of millions of dollars in compensation from Iran in a 2014 US court action because of the Iranian government’s support of Hamas. As part of a decade-long effort to collect damages, the plaintiffs asked the Internet Corporation for Assigned Names and Numbers (ICANN) to seize the country-code top-level domains (ccTLDs) of Iran, as well as North Korea and Syria, and turn them over to the plaintiffs. For a variety of technical, political, and legal reasons, ICANN pushed back against “seizing” ccTLDs and handing them over as compensation in a civil lawsuit (ICANN, 2014).

One example among many in recent history, this conflict over control of ccTLDs raises a number of Internet governance questions: Are country codes property? Should the issue of international control of ccTLDs be addressed in such a civil lawsuit or should this be the purview of international government relations? Who has jurisdiction over ccTLDs? What this case also points to is that infrastructures of Internet governance are now recognized as sites of economic and political power and, as such, they are being co-opted for purposes far beyond their originally constructed technical and policy functions.

Never in history have conflicts over Internet governance attracted such widespread attention from policymakers and the general public. High-profile controversies include the disclosures about NSA surveillance by intelligence analyst Edward Snowden, controversy over a decision by the US government to relinquish its historic oversight of Internet names and numbers, and countless cybersecurity breaches involving unauthorized...
access to Internet users’ personal data. The increasing recognition of the Internet as a basic infrastructure supporting economic and social life has also drawn attention to the underlying institutional and technical systems necessary to keep the Internet operational and secure. An area once concealed in institutional and technological complexity is now rightly bracketed among other shared global issues—such as environmental protection and human rights—that have considerable global implications but are simply incongruous with national borders.

Internet governance is, of course, not new. Since the Internet’s inception, someone has had to manage the distribution of unique domain names and Internet Protocol addresses, respond to cybersecurity threats, and agree to interconnect autonomous networks to collectively form the global Internet. Companies providing content mediation platforms such as search engines or social media have long established policies about how to address cyberbullying problems, or determine the extent of personal data gathered from subscribers. Volumes have been written about how the Internet is governed and the open global debates that exist at various layers of this ecosystem (Goldsmith and Wu, 2006; Mathiason, 2008; Bygrave and Bing, 2009; Weber, 2009; Mueller, 2010; Raboy, Landry and Shtern, 2010; Brousseau and Marzouki, 2012; Kulesza, 2012; DeNardis, 2014). What is interesting about Internet governance is that it transcends traditional government-centric mechanisms like national statutes or intergovernmental treaties. Governance is collectively enacted by the design of technology, the policies of private companies, and the administrative functions of new global institutions like ICANN and the Internet Engineering Task Force (IETF), as well as national laws and international agreements.

This broad ecosystem of institutions, laws, and private ordering that keeps the Internet’s infrastructure operational, as well as the enactment of public policy around this infrastructure, is generally called Internet governance. These administrative and coordinating functions have always been instruments of power because of the ever-growing importance of the Internet to global systems of economic trade, social life, and the political sphere.

But in an era in which nation-bound laws regarding content no longer neatly comport with the globally dispersed and decentralized architecture of the global Internet, there is increasing recognition that points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the flow of money, information, and the marketplace of ideas in the digital sphere. We call this the “turn to infrastructure in Internet governance.” As such, the contributions in this volume—starting with this introduction—depart from previous Internet governance scholarship, by choosing to examine governance by Internet infrastructure, rather than governance of Internet infrastructure.