Alternative internet(s): Governance by internet infrastructure

Francesca Musiani is a researcher with the French National Centre for Scientific Research (CNRS), affiliated with the Institute for Communication Sciences (ISCC). In this latest post in our series on alternative internet(s), she looks at the implications of governance by control of internet infrastructure.

Perhaps due to the snowball effect of the Snowden revelations, never in history have conflicts over Internet governance attracted such widespread attention of policymakers and the general public. 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 incongruous with national borders.

The 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. Laura DeNardis and I have recently called this the "turn to infrastructure in Internet governance."

Drawing from the field of Science and Technology Studies (STS) and previous research on global Internet governance, we argue that the understanding of Internet governance today requires a conceptual framework linking infrastructure and social control to an examination of the co-opting of Internet infrastructure by political and private entities alike for broader political and economic purposes. "Co-opting" simply refers to the use of Internet infrastructure and systems of governance – such as the Internet's Domain Name System – for purposes other than those for which they were initially designed. Several recent cases centered on geopolitical conflicts, intellectual property rights and individual civil liberties provide myriad specific examples of economic and political interests turning to Internet infrastructure and systems of Internet governance as proxies for resolving broader global tensions arising both offline and online. In other words, systems of Internet governance and architecture are no longer relegated to concerns about keeping the Internet operational, secure, and expanding. These systems are now squarely recognized by policymakers, economic interests, and even citizens, as sites of intervention for achieving auxiliary purposes, whether protecting economic interests, influencing political conditions, or gaining real or even merely symbolic nation-state power over cyberspace.

To be clear, values have always entered into the design of technological infrastructure. For example, Internet engineers have designed protocols that affect individual privacy, accessibility for the disabled, and other public interest concerns. But these values have entered into technological infrastructure, for the most part, as designed to carry out its core functions. The politicization of infrastructures of Internet governance to carry out functions completely extraneous to the core technological objective of the system – such as resolving names into numbers, algorithmically returning relevant links – is well at hand, raising questions about the unintended consequences of these developments for the stability and security of the Internet as well as human rights online.

This recognition of infrastructure as a means to advance various externalities has also raised the stakes over the question of who should control Internet governance and architecture. These power struggles, such as control over the Internet's root zone file, have existed for years but have escalated in consort with the rising recognition of the role of infrastructure in mediating political and economic conflict. The nature of these questions will be much more profound as the Internet continues to move from a communication system to an "Internet of things" used not only as a public sphere for communicating and exchanging content, but also as a control system that ubiquitously connects everything from industrial systems to home appliances.

Much of the Internet governance ecosystem – both technical architecture and coordinating institutions and companies – is behind the scenes but increasingly carries significant public interest implications. This transformation into an era of global governance *by* Internet infrastructure presents a moment of opportunity for scholars to bring these politicized infrastructures to the foreground.

This contribution draws heavily from joint work with American University professor Laura DeNardis, most notably from our paper « The Turn to Infrastructure in Internet Governance » presented at the American Political Science Association conference in Washington, DC on August 29, 2014.

This article gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics.

November 28th, 2014 | Alternative Internet(s), Featured, Internet Governance, Privacy | 2 Comments