Perspectives from FSF Scholars
January 3, 2018
Vol. 13, No. 1

A Case of Hypocrisy: Government Network Censors Support Net Neutrality for Private ISPs

by

Enrique Armijo *

Much of the current debate around the Federal Communications Commission's *Restoring Internet Freedom Order* (*RIF Order*) induces what Yogi Berra once famously called "deja vu all over again." To the casual observer, all that seems to have changed is which side won out. There is, however, one interesting new wrinkle this time: the joining of the fight by state and local governments, most of whom claim that the order is unlawful.

Some of these governments have responded to the *RIF Order* by participating in an effort led by New York Attorney General Eric Schneiderman to challenge the rules in court. (So far, the suit – which is built on an investigation led by Schneiderman's office that uncovered millions of bot-filed comments in the proceeding docket, some of which used the names and addresses of actual people – seems to be a *Wired* exposé in search of a legal theory, at least with respect to the legality of the *RIF Order* itself.) Along with California and Washington, New York has also declared its intent to pass its own state-level laws preserving net neutrality for ISPs doing business in those states, setting up another potential federal preemption battle that the FCC is likely to win.

And most relevant for present purposes, the mayors of more than 50 cities, many of which own or operate their own municipal broadband networks or are exploring ways to do so, want the FCC to preserve the restrictions on private ISPs set out in the FCC's previously governing 2015 *Open Internet Order*. Among other arguments, the mayors claim that "critical to our communities' reliance on the Internet is the confidence that our use of the Internet is not subject to the whims, discretion, or economic incentives of gatekeeper service providers to control or manipulate the experience of Internet users." Abandoning the 2015 Order, the mayors argue, would "permit[] blocking, throttling, and other interference with access to the Internet."

These mayors are undoubtedly correct that when the traffic being carried over the Internet is speech, freedom of expression is directly implicated. But it appears the sauce of net neutrality – at least so far as "net neutrality" means barring the service provider's ability to block or throttle user content in order to censor it – is not good enough for some of these geese. As I discussed in a prior *Perspectives from FSF Scholars* paper, the record of local governments so far, at least with respect to the conditions they place on the speech traffic that is carried over their *own* municipal broadband networks, is decidedly mixed.[1] Thus, there is considerable irony, even hypocrisy, in their plea that private Internet service providers be prohibited from engaging in blocking or otherwise restricting content while they proclaim that they may engage in the very same practices.

***

Comparing examples from two different points in time might illustrate the danger that these government-owned networks can present to free speech. In the 1965 U.S. Supreme Court case of Lamont v. Postmaster General, a federal statute empowered the Postmaster General to confiscate foreign-originated mail that he deemed to be "Communist propaganda."[2] The Lamont petitioner, a pamphleteer who received notice of the Post Office's confiscation of his copy of the Peking Review, sought to enjoin the statute's enforcement, arguing that it violated his First Amendment right to receive information. Even though the statute provided that an addressee could request mail that the General had confiscated by returning an official reply card, the Supreme Court unanimously agreed with Lamont that the statute violated his First Amendment rights. The Court noted that "the United States may give up the post-office when it sees fit, but while it carries it on the use of the mails is almost as much a part of free speech as the right to use our tongues."[3]

The principle affirmed in Lamont – that the government must carry the speech of its users without prejudice against the content of that speech – extends back to the founding of the postal service. Though the U.S. Supreme Court strayed from this foundational understanding for a time, finding that the government did have authority to make content-related decisions as to the

[1] Perspectives from FSF Scholars, Enrique Armijo, *Municipal Broadband Networks Present Serious First Amendment Problems* (Feb. 23, 2015).
[2] 381 U.S. 301 (1965).
[3] *Id.* at 305 (quoting United States *ex rel.* Milwaukee Soc. Democratic Pub. Co. v. Burleson, 255 U.S. 407, 437 (1921) (Holmes, J., dissenting)).

mail it carried,[4] the provenance of the principle is not in dispute. As Ithiel de Sola Pool recounts in his seminal *Technologies of Freedom*:

> In 1836, President Andrew Jackson, concerned at the upsetting effect that the distribution of antislavery propaganda might have in the South, urged Congress to ban such matter from the mails. An ad hoc committee of the Senate chaired by [John] Calhoun, America's classic defender of slavery, rejected the President's request because, in his view, Congress had no such power: "If it be admitted that Congress has the right to discriminate … what papers shall or what shall not be transmitted by the mail, it would subject the freedom of the press, on all subjects, political, moral, and religious, completely to its will and pleasure."[5]

Compare the statute found unconstitutional in Lamont, as well as the historical basis underlying its invalidation, to the following proscriptions, all of which come directly from municipalities' terms of service for use of their publicly accessible broadband networks, some of which I referred to in my earlier February 2015 *FSF Perspectives*:

- The "Acceptable Use Policy" for the municipal utility-owned and operated Chattanooga, Tennessee, fiber optic network bars users from using the network to "transmit, distribute, or store material . . . that is," in addition to illegal or obscene, "threatening, abusive or hateful," or that offends "the privacy, publicity or other personal rights of others."[6] Nor may users of the network "post messages" on third-party blogs "that are excessive and/or intended to annoy or harass others"—"regardless of [the] policies" of the blogs on which the users post.[7]

- The Terms and Conditions for GOWEX, the private partner offering Internet access for New York City as part of the city's Wireless Corridor Challenge, "bars the transmission of data . . . via Hotspots managed by GOWEX . . . whose content is threatening, derogatory, obscene, pornographic, or the transmission of any other type of material which constitutes or incites a conduct which may be considered a criminal offense, is prohibited."[8] GOWEX also "reserves the right to prevent or block access to any user" who violates the content policy.[9]

- The City of Wilson, North Carolina's Terms of Service for its Greenlight network states that users may not "send[], post[], or host[] harassing [or] abusive" materials, or may not "engag[e] in any activities or actions intended to withhold or cloak any user's identity or contact information." Greenlight also may, in its "sole discretion," "temporarily or permanently remove content" that it believes violates its Terms of

[4] *See, e.g.*, Milwaukee Social Dem. Pub. Co. v. Burleson, 255 U.S. 407 (1921).
[5] ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 82 (1984).
[6] *See* Electric Power Board of Chattanooga Fiber Optic Acceptable Use Policy, *at* https://epbfi.com/support/legal/acceptable-use-policy/.
[7] *Id.*
[8] GOWEX Terms and Conditions for the New York City Wireless Corridor Challenge (on file with author); *see also* www.nyfreewifi.com/nycedc.
[9] GOWEX Terms and Conditions, *id.* (on file with author).

> Use. Furthermore, Greenlight may, pending its investigation of a violation, "suspend the account or accounts involved and/or remove or block material that potentially violates this policy."[10]

These terms of service decidedly are not examples of network neutrality. These government-owned networks severely restrict users' speech on the network in exchange for access – and in doing so, facially violate the First Amendment in any other context. First Amendment doctrine in the United States makes clear that outright bans on protected speech – even indecent speech, let alone "excessive," "derogatory," "abusive," or "hateful" speech – are never sufficiently narrowly tailored to survive constitutional scrutiny.[11] It is also black-letter free speech law that prior restraints – and there is no question that a network operator's "rejecting or removing" material because of its content before that material reaches its intended recipient is a prior restraint, as is the case here – are presumed unconstitutional.[12] And the right to speak anonymously is well enshrined in the Speech Clause's protections as well.[13] Terms of service such as those used in Chattanooga, Wilson, and potentially scores of other cities thus violate basic tenets of First Amendment law, let alone the principle that network providers should not block or throttle speech because of what it says.

***

To the extent online expression is both a mediated and monitored experience, it is certainly so that private companies are doing much, if not most, of the mediating and the monitoring. Hence all the First Amendment-related discussion permeating the net neutrality debate. But importantly, net neutrality is not, as many have argued, "the First Amendment issue of our time." That level of bombast – often asserted, ironically enough, by government officials – is a diversion. It is intended to trick us into losing sight of free expression first principles: it is governments, not private parties, which have historically represented the first-order threat to free speech and access to information. And it's worth remembering that the First Amendment prohibits government from restricting speech, not private parties.

An example, borrowed from prominent Internet critic Evgeny Morozov, might help to illustrate the point. As noted in Morozov's *The Net Delusion*, expression's move from physical space to online has been a boon for speakers, but it has also made it much easier to be a spy. In the 1970s, it literally took teams of KGB officers to drill holes for bugs, monitor workplaces, establish observation points below and above a single dissident's apartment, and listen to every conversation in order to collect speech and associations that the government believed to be incriminating. That is a lot of work to surveil one person. Now, however, a single officer of the modern-day secret police can run keyword searches of millions of intercepted emails by

---

[10] *See* Greenlight Community Broadband Terms of Service, *at* http://www.greenlightnc.com/termsofservice/ (last visited August 11, 2014).
[11] Sable Commc'ns. of Calif. v. FCC, 492 U.S. 115, 126-28 (1989) (upholding ban on obscene telephone messages, but finding ban on indecent messages not narrowly tailored).
[12] *See* Promotions, Ltd. v. Conrad, 420 U.S. 546, 553 (1975) (holding a city's denial of use of its theater for a production of Hair on the grounds the play was "not in the best interests of the community" was an invalid prior restraint).
[13] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

thousands of users without leaving his desk.[14] The overwhelming majority of those email accounts are provided by private companies and the emails themselves mostly travel over private networks. But private actors do not replace government interferences with privacy and association; in some cases, they can be forced to facilitate it. So too with interferences with speech.

And, of course, the current President of the United States has made his views on the issue of blocking content online known. While a candidate, he argued that in response to the spread of radical extremism online, "we have to talk [to the executives of private technology companies like Microsoft and Google] about, maybe in certain areas, closing that Internet up in some way."[15] Though one might laugh this off as campaign blather, it is very likely that the President has the power in the event of a national security emergency to shut down wire communications throughout the United States. The U.S. Communications Act's 47 U.S.C. § 606 states that the "war powers of President" include the ability to, "if he deems it necessary in the interest of the national security and defense, … cause the closing of any facility or station for wire communication."[16] So if President Trump, or any other president, decides he needs to turn off the Internet in the United States, he doesn't need Bill Gates's help – or, perhaps, even Congress's consent. This is yet another reminder that it is the government, not private companies, which represents the first-order threat to free expression.

***

Here is a thought experiment. Imagine a proposal for a nationwide high-speed wireless network in the United States, built by the federal government, with Internet access service provided over the network by local utilities, pursuant to terms of use adopted by those utilities and subject to whatever strings the feds would impose in exchange for network access. Imagine that this network was proposed in 2014, around the time the U.S. Court of Appeals for the D.C. Circuit struck down the FCC's first attempt at adopting net neutrality rules for private ISPs. Would you have been in favor? Would you have found the government's involvement in developing such a network consistent with, and promotive of, principles of free expression, innovation, and democratic discourse?

---

[14] EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 150-51 (2011).

[15] Nick Statat, *Donald Trump thinks he can call Bill Gates to 'close up' the Internet*, Verge.com (Dec. 7, 2015) (quoting Trump statement at rally in Mt. Pleasant, SC), *at* http://www.theverge.com/2015/12/7/9869308/donald-trump-close-up-the-internet-bill-gates. To be fair, government's attempts to enlist technology companies in the fight against extremist speech online have been bipartisan. *See* Danny Yadron, *Revealed: White House seeks to enlist Silicon Valley to 'disrupt radicalization,'* The Guardian (Jan. 7, 2016), *available at* https://www.theguardian.com/technology/2016/jan/07/white-house-social-media-terrorism-meeting-facebook-apple-youtube- (detailing Obama administration intelligence officials meeting with executives from Facebook, Google, Twitter, and other companies).

[16] *See also* S. Rept. 111-368, Senate Committee on Homeland Security and Government Affairs, Protecting Cyberspace as a National Asset Act of 2010, at 10 ("The Committee understands that Section 706 gives the President the authority to take over wire communications in the United States and, if the President so chooses, shut a network down.")

Now imagine the same project being proposed today. If you were in favor in 2014, would you be in support now? Do you still trust the government to provide nondiscriminatory access to the Internet, the way we have always presumed it offers access to other public goods like roads, water, sewers, and sidewalks? Or is Internet infrastructure, where information is the public good on offer, somehow different?

It is certainly so that creating an infrastructure of free expression involves positive policymaking – affirmative acts by governments intended to fuel the production of knowledge and innovation, and the interaction between diverse, and at times conflicting, ideas, cultures, and beliefs. "Net neutrality," whether one is for or against it, is an example of such a policy debate. Those debates, however, must also take into primary account the negative liberty principles that protect speakers and listeners from government interferences with speech. This constitutional norm may have been born with the First Amendment, and intended for pamphleteers instead of bloggers. But as speech moves from physical to virtual space, we need to remember it now more than ever.

We should thus be wary of mayors arguing that what is good for Comcast or Verizon is no good for them. The fact that they proclaim, however loudly, that they favor net neutrality, including the restrictions on blocking and other practices contained in the FCC's 2015 Order, while employing terms of service for their own government networks that are wholly inconsistent with those restrictions, ought to give one pause.

* Enrique Armijo is a member Free State Foundation Board of Academic Advisors and Associate Dean for Academic Affairs and Associate Professor of Law, Elon University School of Law, and Affiliated Fellow, Yale Law School Information Society Project.