The Public Internet Option
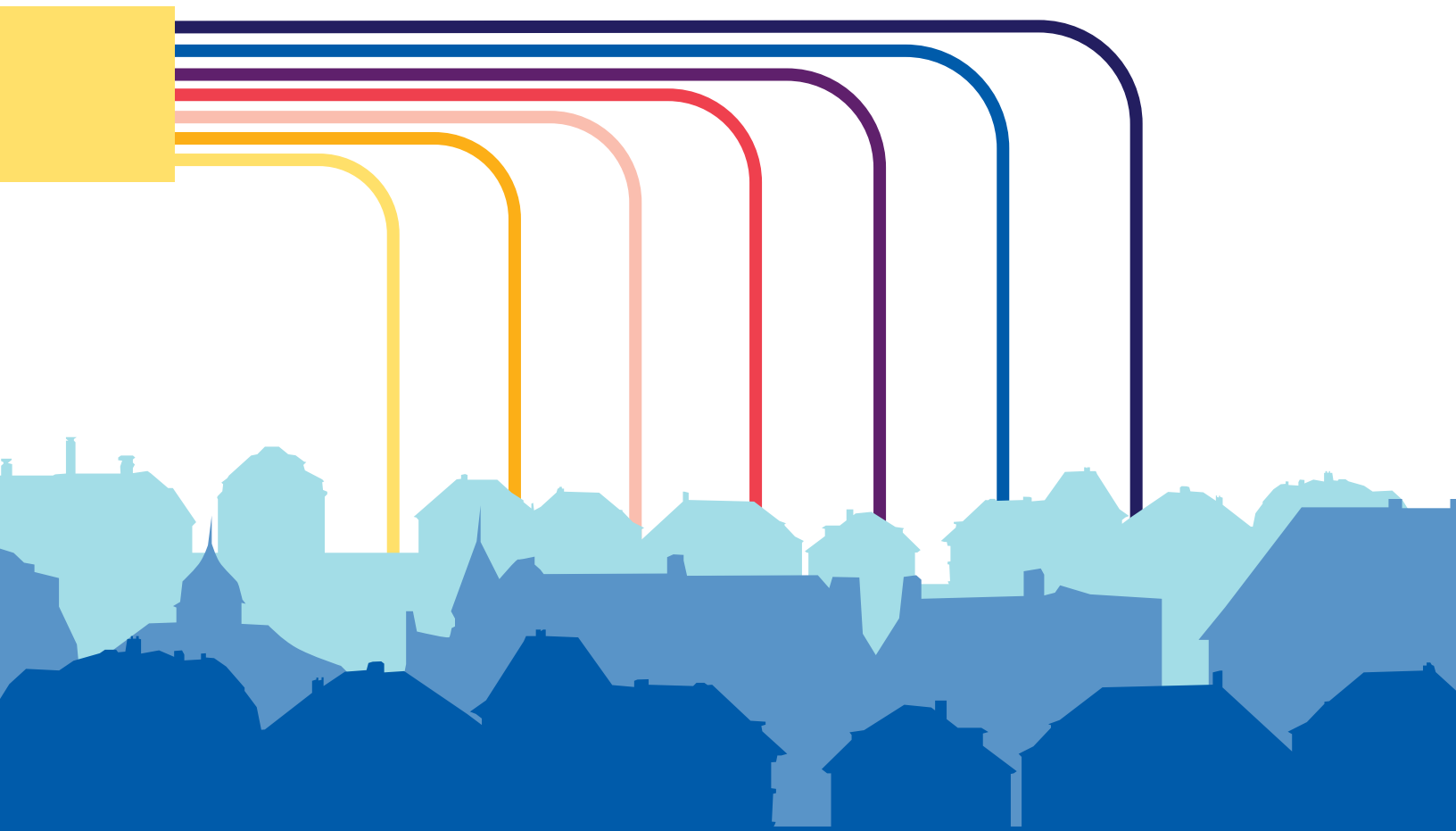
How Local Governments Can Provide Network Neutrality, Privacy, and Access for All

ACLU

The Public Internet Option

ACLU

Contents

Introduction

The internet has become a necessity, like traditional utilities such as water and power. Internet service is necessary for engaging meaningfully with society: to become educated, to participate in political and professional communities, and to seek help and companionship from those with similar interests or problems. Most importantly, perhaps, it is the primary medium for exercising our constitutionally protected rights to seek and share information.

Yet unlike water and electricity, access to home broadband internet remains highly inadequate in the United States 20 years after public internet usage first began to take off. A surprisingly high percentage of the U.S. population lacks any local access to broadband internet at usable speeds. And for those who do have some access to broadband, there is a troubling lack of market choice; when a choice between carriers exists at all, it is usually only between two — and that kind of duopoly is hardly sufficient to ensure robust competition over price and service.

In addition, corporate broadband providers have successfully pressured Washington policymakers into abandoning crucial internet protections, including network neutrality and fundamental communications privacy rules. This marks a stark departure from longstanding practice. The United States has long protected the privacy of our primary communications media, including the mail, telegraph, cable, and telephone systems. And the United States has long insisted on neutral "common carrier" protections to establish a level playing field for facilities that are crucial to the functioning of society and the economy, such as bridges, roads, trains, airlines, and the telephone system.

Hundreds of communities have built municipal high-speed fiber networks.

These principles are particularly critical for the internet — overwhelmingly our dominant form of communication today, and certainly an essential facility for individuals and markets alike. But in March 2017, privacy rules clarifying the application of longstanding law to the internet that were created by the Federal Communications Commission (FCC) were reversed by Congress, allowing broadband providers to sell their customers' browsing histories and any other data. And in December 2017, the new Trump-era FCC voted to reverse the commission's network neutrality protections and, for the first time in the history of the broadband internet, remove the agency from any role in enforcing network neutrality principles.

In light of these actions, many citizens and local leaders have wondered, "what can we do?" Communities can and should take action on a number of fronts, including pushing their representatives in Washington to veto the FCC's action through the Congressional Review Act (before that option expires), and supporting presidential candidates who pledge to appoint FCC commissioners who will reverse it. They should also do everything they can to push for state and local privacy and network

neutrality protections to fill the vacuum created by the removal of the FCC from its protective role in this area. At the time of this report, many state and local governments were showing a lot of interest in doing this. Unfortunately, in repealing network neutrality protections, the FCC also purported to preempt state and local governments from creating their own protections. That means any such legislation will inevitably be subject to legal challenge by internet service providers (ISPs), and we don't know how the courts will resolve that dispute.

Another option for local action

The good news is that there is another, longer-term avenue open to communities that are serious about protecting privacy and network neutrality: investing in internet infrastructure that is owned by municipal and county governments rather than by private companies. Nothing the FCC has done prevents a city, county, or town from directing its own, municipally run service to honor strong network neutrality and privacy policies. If the commercial providers are determined to make money by violating the privacy and speech rights of their users, and if some policymakers in Washington are determined to clear the way for them to do that—then states, cities, towns, and counties should take matters into their own hands by creating publicly owned services that do honor those values and can help ensure an open internet.

Communities can go all the way and provide high-speed fiber connections directly to their residents' homes, along with internet services to go along with them. Or they can leverage their ownership of crucial assets such as conduits (tubes, pipes, tiles, and other casings for cables) to require private-sector providers using those assets to respect free-internet principles. Or any strategy in between.

A growing number of cities, towns, and counties across the United States have already moved in these directions. Hundreds of communities have built municipal high-speed fiber networks of various kinds, and some cities have already begun to act in

response to the FCC vote on net neutrality.[1] Fort Collins, Colorado, for example, gave final approval to a gigabit-speed municipal fiber network that, the city said, would honor network neutrality and privacy principles. San Francisco, meanwhile, issued a call for bids from private-sector companies to build a citywide internet network that would do the same.[2]

Such networks can offer other advantages besides protecting privacy, accessibility, and network neutrality. They can often bring service to areas where commercial providers have not, and bring faster service at cheaper rates. They can also create competition where only monopoly service is currently available. Such advantages have been perceived by practical people across the political spectrum: many municipal broadband systems have been built by— and widely supported within—small, conservative towns.[3]

The problem with the monopoly telecoms

The problem for the monopoly telecoms is that what people want is simple and boring. They want clean, simple, fast, cheap internet service. They want the cable and phone companies to deliver data without messing with it and violating network neutrality, or spying on it and violating privacy. But these Wall Street-financed public corporations are under enormous pressure to produce dynamic new products that will allow for soaring profits. As a result, the fast, cheap, reliable, boring commodity connections that everyone wants are under constant threat from "innovations" by hungry carriers eager to extract additional revenue from customers.

Of course, we all want excitement and innovation in internet *services*—social networks, information, gaming, entertainment, and other services that send data *across* the internet. But what innovations are the carriers going to produce by being allowed to monitor and distort their customers' traffic? Most likely: becoming better at spying on and manipulating data to extract profits.

By putting public utilities in charge of internet service, communities can obtain the straightforward service their members actually want.

Big telecoms that control the one or two viable internet options in a community can add to their profits by gathering and selling data on their customers' web surfing, application usage, daily activity patterns, and no doubt many other "innovative" sources of information about them. These corporations can also increase profits by finding "innovative" new ways to prioritize their own content and slow down everyone else's. Remember, Comcast owns its own video streaming service — and also NBC, Universal Pictures, DreamWorks, Telemundo, the Weather Channel, Bravo, USA Network, Lifetime, A&E, Syfy, E!, Oxygen, and many other media properties. Comcast's competitors, like AT&T and Verizon, also own and are working to expand their own media properties.

By putting public utilities in charge of internet service, communities can obtain the straightforward service their members actually want from an internet provider.

Unfortunately, telecom lobbyists have convinced at least 21 state legislatures to enact restrictions or outright bans on the ability of municipalities in those states to create their own broadband service — thereby leaving people no choice but to utilize the commercial services that are often slow, unjustifiably expensive, and now poisoned by their lack of protections for privacy and network neutrality. The Obama-era FCC issued an order preempting state laws and clearing the path for municipal broadband,

but that preemption has been successfully challenged in court, so municipalities in many states face varying degrees of obstacles in creating broadband services for their residents. Residents of those states should start by demanding that their state legislators reverse those laws.[4]

Community internet needs to be done right

There are many good reasons for communities to provide internet service—but it needs to be done right. Indeed, local governments should see community internet systems as a unique opportunity to show their commitment to their residents' constitutional rights. Cities can be sanctuaries for the privacy and diversity of telecommunications. They can resist bad policies emanating from Washington and give people a way to take control of their online destiny through local political activism.

This paper seeks to encourage the adoption of municipal broadband as a means of protecting privacy and free speech (including network neutrality), and also to offer a set of "best practices" for those cities and towns that adopt municipal broadband.[5] Our recommendations are focused on the following three principles:

1. High-speed broadband must be accessible and affordable for all.

2. Community broadband services must protect free speech.

3. Community broadband services must protect privacy.

While this paper is focused on municipal broadband, citizens and consumers should also demand that commercial ISPs comply with the principles we outline here. Indeed, a number of smaller ISPs have said they will abide by such protections.

The Need for Fast and Equitable Broadband Service

One reason that community broadband is proving so attractive is that good commercial broadband services remain inaccessible for many Americans. Sometimes that is because people cannot afford our country's relatively expensive broadband services; it is also because in many locations broadband is simply not available at any price.

The Federal Communication Commission's most recent data shows that 24 million Americans — over 7 percent of the population — still lacked access to broadband speeds that met the FCC's benchmark of 25 megabits per second (Mbps)[6]. (Even that benchmark is increasingly too low for average household data usage; 25 Mbps is about how much a single 4K video download would require, leaving no room for other connected devices in a household.[7] See Figure 1.) This problem is particularly significant in rural areas. According to the FCC, more than 30 percent of the population of rural America lacks access to 25Mbps service.[8] Such remarkable disparities in access, along with racial and economic "digital divides,"[9] have an increasingly detrimental effect as more and more of our lives — from political activity to education, job applications, and bill payment — move online.

And the FCC is widely seen as having overestimated the quality and deployment of internet service in the United States, particularly since President Trump appointed Ajit Pai as the agency's chair.[10] At one point Pai floated the idea of lowering the bar for "adequate" broadband even more, from 25 to 10Mbps, which would have just *defined away* the problem that the United States is being very poorly served by its monopolist telecoms.[11]

Apart from access problems, many people who do have a provider serving their area nonetheless do not subscribe to broadband (see Figure 2). The number of residents who actually get wire broadband appears to have stalled in recent years at around 70 percent of the population.[12]

A report issued by the FCC in May 2015 looked at barriers to broadband adoption and found that cost, relevance, and digital literacy were the key factors preventing broadband adoption for low-income consumers. Of course, these three barriers
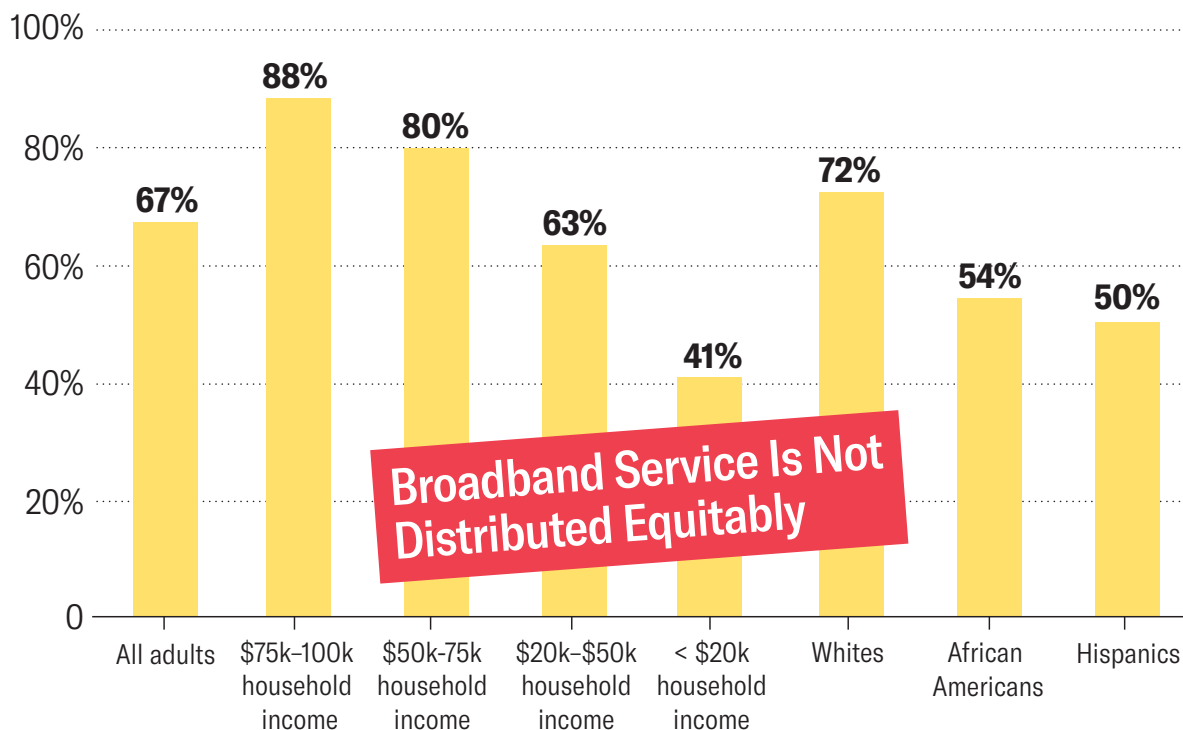
FIGURE 1

BROADBAND SPEED SCALE

Source: Pew report, "Home Broadband 2015"

FIGURE 2

PERCENT OF HOUSEHOLDS WITH BROADBAND AT HOME

Source: Pew report, "Home Broadband 2015"

are inextricably intertwined; an individual's willingness to pay for broadband is "directly related to the perceived relevance of the broadband and how 'digitally literate' the individual is in using the service."[13] There is also a racial element to the digital divide. Far fewer Blacks and Latinos than whites have high-quality broadband at home, and people of color are more likely to rely on their cell phones for internet access.[14]

Ownership of a cellphone is not a sufficient replacement for home broadband. A Pew study found that 69 percent of Americans say not having home broadband "would be a *major disadvantage* to finding a job, getting health information or accessing other key information."[15] Job applicants, for example, often have trouble getting information to display properly on their phone, or submitting resumes and other important documents as part of a job application.[16] Pew also reports that those who are "smartphone-dependent" are more likely to have to

cancel or suspend their phone service due to financial constraints.[17] As the FCC concluded after examining the issue:

> fixed and mobile broadband services are not functional substitutes for one another … Fixed and mobile broadband are both critically important services that provide different and complementary capabilities, and are tailored to serve different consumer needs.[18]

Most Americans face a lack of choices and competition when choosing a broadband provider. The FCC found in its 2016 report that only 38 percent of Americans have more than one broadband provider to choose from (see Figure 3), and most of that group only has two choices.[19] This dearth of options has meant that commercial broadband providers have little incentive to make their services affordable, hindering equal access to this vital utility.

Levers of control

Such problems are a major reason why hundreds of American communities are offering their own internet access services. In a democracy, it is vital that citizens have actual and felt control over the institutions that govern their lives — including their increasingly crucial broadband providers. In the absence of competition, or as a supplement to it, community broadband offers citizens such control through the democratic political process. Where customers faced with inadequate service can't easily switch to an equivalent provider, they can at least complain to their city council member or other elected officials. When local government is in charge of providing internet access, those complaints are much more likely to be effective than when a town's mayor tries to exert influence over a major national telecommunications company like Verizon, Comcast, or AT&T, or over the FCC in Washington.

Municipalities are offering several varieties of internet service, including residential wireline broadband, broadband to businesses, and public Wi-Fi (which can be deployed easily at a very low cost to provide broadband connectivity in municipal spaces).

There is a long American tradition of cities and towns providing vital services through municipally run utilities or cooperatives in which each customer is a member and owner of the enterprise. Today, 27 percent of electric customers and 77 percent of water customers are served by municipally owned utilities or co-ops.[20] Of the 1,300 natural gas utilities in the nation, 1,000 are municipally or cooperatively owned.[21]

Lower prices and better performance

Many cities have had good experiences with municipal broadband. Hundreds of cities have built their own networks, many of which offer high-speed services to their customers at rates below what for-profit telecoms typically charge.[22] A 2018 Harvard

ESTIMATED % OF AMERICANS WITH MULTIPLE OPTIONS FOR FIXED ADVANCED TELECOMMUNICATIONS CAPABILITY
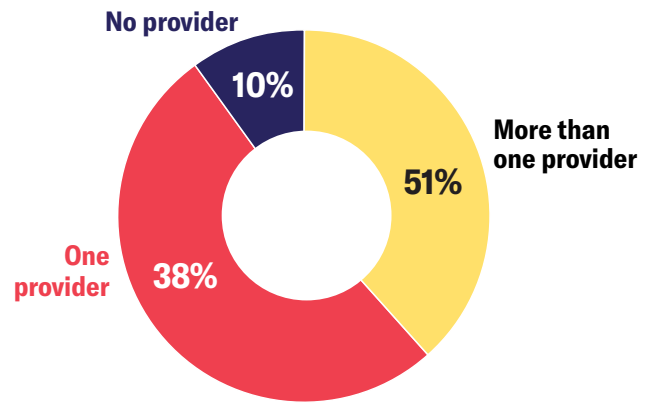
Source: FCC 2016 Broadband Progress Report

study found that community-owned fiber-to-the-home networks generally charge less than private providers. The study also found that private companies tended to make their pricing complex and obscure.[23]

Overall, consumers in the U.S. tend to pay more money for slower speeds than those in Europe and Asia, even in big cities.[24] In Seoul, Tokyo, and Paris, one study found, service at 200-300 Mbps could be had for the same price residents of Los Angeles and New York were paying for less than 50 Mbps. But, as The New York Times put it:

> Some surprising smaller American cities — Chattanooga, Tenn.; Kansas City (in both Kansas and Missouri); Lafayette, La.; and Bristol, Va. — tied for speed with the biggest cities abroad. In each, the high-speed internet provider is not one of the big cable or phone companies that provide internet to most of the United States, but a city-run network or start-up service.[25]

Municipalities that lack good broadband access find that shortfall to be not just an inconvenience to residents, but also to pose significant economic disadvantages. Good internet access is now in

the same category as good schools, convenient transportation, and a well-run government: important in generating, attracting, and retaining businesses. Good residential broadband and public Wi-Fi are increasingly being seen not as costs, but "as an economic development engine, innovation stimulus and revenue generator."[26] Cities desperate for economic development cannot afford to rest their fates on the whims of a handful of large broadband providers, and practical, non-ideological people around the country are moving to do what they need to do. As the Roanoke (Virginia) Times put it in an editorial about whether the city should invest in municipal broadband:

> The idea is not exactly one being pushed by beret-capped socialists quoting "Das Kapital." On the contrary, it's cold-eyed disciples of Adam Smith — specifically business leaders, the captains of the private sector — who are usually the most enthusiastic champions.[27]

Companies selling internet access, however, have an economic interest in keeping broadband access scarce. Many commercial services, for example, contractually prohibit their residential customers from offering open Wi-Fi to the public. Offering free high-speed Wi-Fi across an entire city may help expand internet access, but it doesn't help for-profit companies increase their subscriber base. And without network neutrality, providers have an incentive not only to make service scarce, but also to make it slow, so they can charge extra for internet "fast lanes."

Some may worry that government-run broadband service will be bureaucratic and inefficient. But large corporate bureaucracies are often just as bad or worse — especially when competition is not tight. That's probably why cable television and internet service providers are among the industries most hated by consumers (ranking far below both municipal and co-op utilities).[28] Many local utilities, on the other hand, get strong reviews from their customers. The public utility-run internet service in Chattanooga, Tennessee, for example, was rated in 2017 as the nation's top ISP in terms of consumer satisfaction by Consumer Reports.[29]

Different models

Localities are taking a variety of approaches to creating community broadband services, both in terms of the services provided and in the degree of involvement of private for-profit or non-profit companies.[30]

Some municipalities offer complete wired internet services into residents' homes — providing all the services that for-profit cable and telephone companies offer in other places, and operating much like municipal water or electricity companies. Chattanooga, Tennessee, has deployed this approach. After the FCC's December 2017 order eviscerating network neutrality protections, the city's utility issued a public statement promising to honor network neutrality principles, saying "We're committed to having an open Internet."[31]

Other cities are relying on public-private partnerships. Some build networks of fiber-optic cable (with its enormous bandwidth capabilities) that reach directly into homes and businesses, and then lease those networks on a nonexclusive basis to any ISP that wishes to provide services (such as internet, television, and telephone) over those wires. The wire infrastructure itself is thus operated like a utility, while competition can flourish among companies providing services over those wires. This model has proved successful in cities like Huntsville, Alabama, and Westminster, Maryland.[32]

Another approach that allows an even larger private-sector role is to offer "middle mile" broadband—a backbone network that does not include the "last mile" connections to customers' homes or businesses. An example of this approach is a statewide broadband program under construction in Kentucky called "KentuckyWired." KentuckyWired involves the construction and operation of a 3,200 mile network connecting all 120 counties in Kentucky to the global internet. It then will provide non-exclusive access to any competing internet provider that wants to lease bandwidth and build the "last mile" connections to customers' homes.[33] Kentucky's network does not currently include provisions for network neutrality or privacy protections, however, and experience elsewhere suggests that middle mile networks do not always attract partners to build expensive last-mile networks, especially in low-density areas.[34]

Instead of providing actual fiber or other internet services directly, some cities are turning to a strategy of investing in city-owned networks of conduits, which they then allow competing private ISPs to run wires through using non-exclusive contracts. Lincoln, Nebraska, has done this—and its Broadband Franchise agreement requires that ISPs using the publicly owned conduit adhere to network neutrality rules.[35]

Public-private partnerships and preemption

One factor that municipalities should consider in entering public-private partnership is the possibility of restrictions on their authority to protect network neutrality in service delivered by private companies. We don't know whether courts will find network neutrality rules imposed on private partners to be preempted by the FCC's December 2017 order eviscerating network neutrality. That order purports to preempt "any state or local measures that would effectively impose rules or requirements that we have repealed or decided to refrain from imposing in this order."[36] In other words, the FCC has explicitly decided to create a regulatory gap and is trying to forbid state and local governments from filling it.

It's unclear what the boundaries of any such preemption might be. Generally, the greater the private-sector involvement in community broadband, the more cautious localities should be about this issue. Overall, a state or local governmental entity making a straightforward purchasing decision in contracting for services will be on stronger ground in the preemption context than government entities that try to use their purchasing power as a backdoor means of regulating private parties. And cities, towns, and counties can certainly direct their own municipally owned services to honor strong network neutrality and privacy policies without raising preemption problems.

Government-Provided Broadband Service Must Honor Constitutional Values

Internet access has become integral to full participation in our society, economy, and democracy. Municipal internet providers thus have special responsibilities to offer broadband access in a responsible and constitutional manner. Government entities are constrained by the Constitution in ways that private entities are not, and local governments have a duty to serve their entire communities, not just paying customers.

This is true regardless of the model a city or town follows for the provision of access. Even if its role is simply to lease pipes or provide funding for broadband programs, the government must do everything possible to bake good policies and constitutional values into contracts and requests for proposals. In particular, municipalities must ensure they achieve three crucial goals: to make high-speed broadband accessible and affordable for all, protect free speech, and protect privacy.

1. High-Speed Broadband Must Be Accessible and Affordable For All

When the internet was first popularized in the 1990s, it was often called the "Information Superhighway" — an apt metaphor. Just as the roads and sidewalks are open to all, so too must the internet be available to all. Community broadband should not be deployed principally to serve businesses and the affluent. It must be equally accessible to residents of rural and low-income areas and communities of color. Municipal systems should be built to serve all residents equally, even though the demands of affluent neighborhoods might be louder than others.

> Municipal systems should be built to serve all residents equally, even though the demands of affluent neighborhoods might be louder than others.

For instance, communities could require their municipal utilities and any private sector partners to build in areas that are historically unserved or underserved.[37]

Fair access to high-quality internet is a constitutional issue because such access is essential to our ability to access and share information, which in turn enables us to shape our political, civic, and social systems. As the internet becomes ever more central to our lives, individuals' ability to exercise their First Amendment rights depends increasingly on access to online platforms. Unequal online access therefore means unequal power to exercise First Amendment rights.

Public Wi-Fi accessibility

Public Wi-Fi can be an important supplement to wired residential broadband, providing an alternative means of getting online for those who do not have a residential broadband subscription. It can also be a valuable economic asset for a community and a simple

convenience for everyone. For those who do not have residential service and rely exclusively on their phones to get online, it can also help keep data costs low.

For these reasons, it is important that communities keep their Wi-Fi services as open and accessible as possible. There are several accessibility considerations that municipalities should take into account when deploying public Wi-Fi.

Municipal broadband providers should never prohibit customers from running open access points.

Many online users allow others to use their broadband connections by offering their routers without passwords and free of charge. In some places, the provision of these unrestricted routers (or "open access points") has become something of a social movement, as individuals work to share their plentiful bandwidth with the public. The movement has even produced wireless firmware that customers can install in their routers that allows residential customers to split their bandwidth into two streams: an open Wi-Fi access point that anyone can access, and a locked, password-protected connection for the customer's exclusive use. The customer's private traffic can be configured to have priority, so that personal access is not slowed, while spare capacity is "donated" to the public.[38] But many commercial providers enforce limits on such provision of open access.[39]

Cities and towns should consider building such dual configurations into their residential services to enable open access points. Residential broadband might be configured so that each home receiving high-speed internet access doubles as a municipal wireless access point. By serving this double function, home routers can not only spread Wi-Fi access around neighborhoods, but can also co-mingle residential and Wi-Fi traffic to help protect the privacy and anonymity of internet use. Mixing together a wireline subscriber's internet traffic with that of random members of the public using Wi-Fi makes it difficult for anyone seeking to track internet usage to tell exactly who is doing what online.

Some municipalities have suggested they believe that federal communications laws (specifically, CALEA) require them to be able to identify internet users and preclude them from offering open access points. This is not the case.[40]

Municipal Wi-Fi should not require accounts, logins, or complex signup procedures.

Those who want to get online should not have to go through complex signup procedures — which are most likely to filter out those with the fewest options for access — in order to get online. Nor should public Wi-Fi service (or any other kind of internet access) require accounts or logins, which threaten privacy by providing a way for users to be tracked within and across their online sessions. Accounts and logins also pose significant usability barriers: the time and effort required for initial signup, the user's need to manage their username and password or other credential, and the occasional requirement for specific hardware or software that not everyone has.

Municipal Wi-Fi should offer unencrypted access.

The simplest and most universally accessible type of Wi-Fi link is an "open" or unencrypted one, which allows anyone with a Wi-Fi device to get online. Encrypted access points help protect privacy and security to a degree, but the marginal increase in security that this kind of encryption provides is not worth the downsides: a loss in anonymity and in ease-of-access.

Wi-Fi encryption systems try to prevent anyone with a nearby listening radio from snooping on the network traffic or spoofing or modifying it in transit. But such systems cover only one "hop" (between a user's device and the access point) in a complex chain of communications, any of which may be insecure. Once a user's data travels beyond the Wi-Fi access point and enters the rest of the internet, all the same risks of snooping, spoofing, and modification apply. The only way to get protection along that entire path is for the user to use strong encryption on their own devices (such as HTTPS or other protocols that

establish a secure channel all the way to the remote endpoint).

Most Wi-Fi encryption schemes require users to use a password, which complicates deployment and makes connecting harder to do. And these schemes don't prevent anyone from deploying a fake or "rogue" access point with the same configuration information, which can dupe a user into connecting to and inadvertently sharing information with its operator. Other schemes are capable of protecting against rogue access points, but require device registration with a long-term credential that facilitates privacy-invasive tracking of the user by the network operator.

Overall, the problems with existing Wi-Fi encryption schemes (difficulty in deployment and use; lack of universal access; and heightened user-tracking) outweigh their limited benefits. For now, municipalities should offer universally acceptable unencrypted Wi-Fi links. Meanwhile, they should encourage and support the creation of user-focused, privacy-friendly Wi-Fi link encryption.

2. Municipal Broadband Services Must Honor Free Speech and Enable Open Access To Digital Content

The ACLU has long fought for an "open" internet, where users can explore the web, find and respond to information, and share their opinions online without

> Unfortunately there are numerous examples of internet service providers secretly hiding and blocking access to certain online content.

discrimination or censorship by the ISPs. Indeed, the ACLU supported and fought for the principles of network neutrality precisely because we believe that the internet is a public utility, which should never be subject to secret censorship or manipulation. When users go online to search for particular speech, they should have confidence that the results they see aren't secretly filtered, altered, or slowed by those operating their broadband connections because ISPs don't want them to see or speak about certain things.

 Unfortunately there are numerous examples of internet service providers secretly hiding and blocking access to certain online content. In Canada, workers investigating which labor union they might want to join were thwarted for a brief time in 2005. Their ISP hid access to the website of a key telecommunications workers union with which it was locked in a political fight.[41] In 2014, Comcast intentionally slowed, or "throttled" all traffic passing through the Netflix service, holding the company and its users hostage until Netflix paid Comcast higher fees for access.[42] Similarly, AT&T in 2012 blocked its users' access to the online application FaceTime, which it considered a competitor.[43]

Of course, no ISP is likely to advertise that a customer will get compromised service. But it happens — the above is just a sampling of incidents — and it's often invisible to the consumer. In the wake of the FCC's decision to roll back network neutrality protections, it's also likely to happen increasingly often.[44]

This kind of secret corporate censorship is creepy enough. But it's far worse if the censor is the government. Those logging into municipal wireless systems should not have to wonder whether their government is using online access as a weapon of censorship. And indeed, First Amendment principles prevent the government from targeting certain ideas or viewpoints for censorship or reduced access. Governments risk violating the Constitution if they create blacklists of disfavored websites, only permit access to "approved" websites, engage in content filtering, or ban anonymous online browsing or writing. Municipalities offering broadband access must ensure that their systems offer equal,

uncensored access to the full range of lawful digital content.

In addition to net neutrality, good privacy policies and practices are also important for free speech. Surveillance chills speech, particularly on controversial topics, and those who believe their government is watching will not feel free to reveal their beliefs or seek out those of others. A number of studies have confirmed this intuitive truth, finding that surveillance suppresses people's willingness to express nonconformist views and causes them to self-censor their writings, internet searches, online discussions, and political activism.[45] A 2012 study found that fully 40 percent of American adults post political content to social media sites.[46] The government must never block such speech, and it should never systematically monitor it.

Free speech principles for community broadband

To help ensure that community-owned internet access is offered and administered in a manner consistent with free speech values, community providers should:

- Enact strict anti-censorship rules, and make plain in publically available policies and user agreements that the service will take no steps to block, slow, or monitor traffic to any particular websites (subject to carefully limited exceptions such as reasonable network management), and will otherwise honor network neutrality principles.

- Require any company contracting with the municipality for broadband internet provision to comply with network neutrality principles.

- Provide a method for any online user to request their data profile, and receive a report of any information that has been collected, stored, or shared relating to their use of broadband systems.

- Put in place a clear oversight and review process governing internet service, to ensure

that these and any other rules and guidelines are followed and enforced.

3. Municipal Broadband Services Must Protect Privacy

For centuries, countries around the world, including the United States, have provided special privacy protections for communications, including the mail, telegraph, and telephone systems. The 1792 law establishing the Post Office, for example, already prohibited its agents from opening the mail it transported. More recently, Congress updated privacy protections in the Communications Act in 1996, declaring that "every telecommunications carrier has a duty to protect the confidentiality" of the information they get in providing service to individuals.

Broadband providers are clearly "telecommunications carriers" under Congress's definition of that term, and in 2016 the FCC developed extensive rules applying the Communications Act's privacy provisions to internet access providers. Under those rules, carriers would have been required to get customers' permission before using or sharing their browsing history, location, and other sensitive data for advertising or with advertisers and other third parties; to disclose how they collect, use, and share information; and to protect any such information with good security policies. But broadband carriers lobbied fiercely against these rules, and in March 2017, Congress passed and President Trump signed a measure reversing them. That has left an enormous gap in the protection of Americans' privacy.

The reversal of those rules represented a betrayal of legally clear, culturally deep, and historically longstanding protection for privacy in our essential communications infrastructure. This betrayal is another strong reason for Americans to push their local government to provide municipal broadband that reflects the community's values and does not operate under pressure from Wall Street and shareholders for ever-rising profits.[47]

Wi-Fi privacy

Publicly run Wi-Fi services raise some issues that are different from residential service, and municipalities should design and implement systems with a strong emphasis on protecting Wi-Fi privacy. They should not require users to sign up for an account, identify themselves, or register a MAC address to gain access to such services, or impose any other requirements for gaining access that could result in a loss of anonymity. As discussed above, that means offering open Wi-Fi connections without encryption, because the privacy and accessibility advantages of such openness outweigh the security downsides.

A particular danger is that cities and towns, wanting to offer "free" public Wi-Fi service without paying for it, will partner with private companies whose business plan is to monetize data about users' online activities, forcing users to pay for that service with their privacy. Municipalities should not enter into such deals.

Residential broadband service requires some degree of user authentication by nature, such as setting up a billing system. But beyond what is strictly necessary, residential services should also not include any kind of unique identifier that facilitates tracking of online activities.

Privacy principles for municipal broadband

Regardless of whether internet is provided via home wireline services, public Wi-Fi, or some hybrid wireless service, municipalities should follow certain basic guidelines in protecting their users' privacy:

- Do not collect, use, disclose, or retain device, web browsing, location information, or any other internet usage data beyond what is necessary to provide, maintain, and secure the service.

- If some information must be monitored or retained to administer access, de-identify that data whenever possible, and retain it no longer than needed.

- Provide clear and meaningful notice to every user and to the public about when municipal broadband systems collect, retain, or share any data, and the length of retention periods. This notice should be available in translation and in forms that users with disabilities can access.

- Do not share information with third parties, except parties like contractors who are necessary to provide the service, or with the meaningful opt-in consent of users.

- Do not require users to identify themselves in order to gain access to public WiFi services.

- Take reasonable security measures to protect customers' data. Ensure that municipal services meet standards for security and encryption that are at least on a par with industry standards. Promptly notify customers in case of any breach (if not already required by a strong state breach-notification law).

- Review the privacy policies and practices of all partners, including private-sector partners, to ensure they comply with these rules.

- Put in place a clear oversight and review process governing the internet service, to ensure that these and any other rules and guidelines are followed and enforced. This should include a public ombudsman or other meaningful complaint process for users.

- Where municipalities partner or contract with private parties, contracts should impose penalties for contractors who violate privacy or other protections.

Law enforcement requests

Municipalities should not only minimize the personally identifiable data that they retain, but they should adopt clear policies governing when such data will be shared with law enforcement or other security agencies. Those policies should ensure two things:

1. Data is not turned over to law enforcement except when required by a warrant.

2. Users will be notified of any law enforcement or other agency requests for information about them. That notification will be made at the earliest possible time permitted by the order. Of course, when internet usage is anonymous, providers will not know whom to contact in order to provide notice. Municipal operators should give whatever notice is possible, to the greatest extent possible, with whatever information they do have.

It's also important that all employees be aware of these policies and empowered to take appropriate action — such as quickly reaching a city attorney — when confronted by law enforcement seeking customer data.

Conclusion

There are many reasons for Americans to want their municipalities to offer broadband directly or indirectly to their residents. With internet service becoming ever more central to modern social, political, economic, and political life, access to functional and affordable broadband, like access to running water and electricity, must be available to all. Given the poor choices offered to so many Americans by corporate broadband carriers, many cities are finding they need to take matters into their own hands. And as the Trump-era FCC works to terminate important protections for the integrity and privacy of communications, many Americans are also deciding they want a broadband provider that they can trust and that is locally accountable and responsive.

As cities respond to these needs by providing internet access, they must take care to respect constitutional values of free speech and privacy and to ensure that access is provided equally to all. And communities that don't offer internet services should consider doing so as a way to advance and protect those values.

Endnotes

1   Masha Zager, "A Record Increase In Municipal Fiber Broadband," *Broadband Communities*, October 2017, http://www.bbcmag.com/2017mags/Oct/BBC_Oct17_RecordIncrease.pdf.

2   Karl Bode, "Fort Collins Votes to Build Its Own Gigabit Broadband Network," *DSLReports*, Jan. 4, 2018, https://www.dslreports.com/shownews/Fort-Collins-Votes-to-Build-Its-Own-Gigabit-Broadband-Network-140988; Joshua Sabatini, "SF puts out call for private sector to build a citywide internet network," *San Francisco Examiner*, Jan. 31, 2018, http://www.sfexaminer.com/sf-puts-call-private-sector-build-citywide-internet-network/.

3   Christopher Mitchell, "Most Municipal Networks Built in Conservative Cities," *MuniNetworks.org*, Jan. 20, 2015, https://muninetworks.org/content/most-municipal-networks-built-conservative-cities.

4   Jason Koebler, "The 21 Laws States Use to Crush Broadband Competition," *Motherboard*, January 14, 2015, at https://motherboard.vice.com/en_us/article/qkvn4x/the-21-laws-states-use-to-crush-broadband-competition.

5   Jon Brodkin, "After beating cable lobby, Colorado city moves ahead with muni broadband," *ars technica*, Jan. 3, 2018, https://arstechnica.com/tech-policy/2018/01/colorado-city-to-build-fiber-broadband-network-with-net-neutrality/.

6   That is the speed that the agency has decided constitutes "advanced telecommunications capability" under the law, the provision of which to all Americans Congress has directed the agency to push for. FCC, "2018 Broadband Deployment Report," Feb. 2, 2018, GN Docket NO. 17-199, https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0202/FCC-18-10A1.pdf.

7   See Open Technology Institute, "Comments of New America's Open Technology Institute," Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act, GN Docket No. 16-245, Sept. 6, 2016, p. 4, https://ecfsapi.fcc.gov/file/1090792243446/OTIBroadbandProgressComments.pdf.

8   FCC, "2018 Broadband Deployment Report."

9   The "digital divide" is not defined solely by relative access to the internet. It is also affected by access to factors such as the quality and speed of connection, related services (including access to computers and other wireless devices), and digital literacy training programs to train people in how to use the internet and related technologies.

10   Kevin Taglang, "FCC Perpetrates Broadband Policy by Press Release," Benton Foundation Weekly Round-up, Feb. 9, 2018, https://www.benton.org/blog/fcc-perpetrates-broadband-policy-press-release; Kieren Mccarthy, "US broadband is scarce, slow and expensive. 'Great!' says the FCC," The Register, Feb. 6, 2018, https://www.theregister.co.uk/2018/02/06/us_broadband_fcc_report/.

11   Kieren Mccarthy, "FCC drops idiotic plans to downgrade entire nation's internet speeds," The Register, Jan. 20, 2018, https://www.theregister.co.uk/2018/01/20/fcc_broadband_speeds_america/.

12   FCC, "2018 Broadband Deployment Report"; John B. Horrigan and Maeve Duggan, "Home Broadband 2015," *Pew Research Center*, Dec. 21, 2015, https://www.pewinternet.org/2015/12/21/home-broadband-2015/. Aaron Smith, "Record shares of Americans now own smartphones, have home broadband," *Pew Research Center*, Jan. 12, 2017, http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

13   David A. Bray, "Modernizing the FCC's IT," *FCC Blog*, Aug. 20, 2015, https://www.fcc.gov/news-events/blog/2015/08/20/modernizing-fccs-it.

14   Horrigan and Duggan, "Home Broadband 2015"; Monica Anderson, "Racial and ethnic differences in how people use mobile technology," Pew Research Center, April 30, 2015, http://www.pewresearch.org/fact-tank/2015/04/30/racial-and-ethnic-differences-in-how-people-use-mobile-technology/."

15   Horrigan and Duggan, "Home Broadband 2015." Emphasis in original.

16   Aaron Smith, "Searching for Work in the Digital Era," *Pew Research Center*, Nov. 19, 2015, p. 20, http://www.pewinternet.org/2015/11/19/searching-for-work-in-the-digital-era/.

17   Horrigan and Duggan, "Home Broadband 2015."

18   FCC, "2016 Broadband Progress Report," Jan. 28, 2016, GN Docket No. 15-191, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

19   FCC, "2016 Broadband Progress Report."

20   American Public Power Association, "Public Power: Shining a Light on Public Service," Sept. 2015, http://www.publicpower.org/files/PDFs/PublicPowerFactSheet20152.pdf; National Association of Water Companies, "Private Water Solutions," accessed on Jan. 22, 2018, http://www.nawc.org/our-industry/private-water-solutions.aspx.

21   Email from American Public Gas Association executive to ACLU; APGA, "Benefits of a Municipally Owned Utility," https://www.apga.org/apgamainsite/aboutus/facts/municipal-benefits.

22   For a list of municipal fiber-to-the-home networks, see "Municipal FTTH Networks," *MuniNetworks.org*, Feb. 6, 2017, https://muninetworks.org/content/municipal-ftth-networks.

23   David Talbot, Kira Hessekiel, and Danielle Kehl, "Community-Owned Fiber Networks: Value Leaders in America," January 2018, https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2018-01-10-Pricing.Study_.pdf

24   Nick Russo, Danielle Kehl, Robert Morgus, and Sarah Morris, "The Cost of Connectivity 2014," New America Foundation Open Technology Institute, Oct. 30, 2014, https://www.newamerica.org/oti/policy-papers/the-cost-of-connectivity-2014/.

25   Claire Cain Miller, "Why the U.S. Has Fallen Behind in Internet Speed and Affordability," *New York Times*, Oct. 30, 2014, http://www.nytimes.com/2014/10/31/upshot/why-the-us-has-fallen-behind-in-internet-speed-and-affordability.html.

26   Rick Huijbregts, "Why we need free Wi-Fi in our cities," *Cisco Canada Blog*, Oct. 17, 2013, http://canadablog.cisco.com/2013/10/17/why-we-need-free-wi-fi-in-our-cities/.

27   "Our view: Broadband vs. ice cream," editorial, *The Roanoke Times*, April 26, 2016, http://www.roanoke.com/opinion/editorials/our-view-broadband-vs-ice-cream/article_415456a0-982e-5530-9351-5f497b65ff29.html, quoted by *MuniNetworks.org*, "Community Broadband Quotes," https://muninetworks.org/quotes.

28   "Benchmarks By Industry," American Customer Satisfaction Index , http://www.theacsi.org/index.php?option=com_content&view=article&id=148&Itemid=213. See also Stephanie Mlot, "Comcast is America's Most Hated Company," *PC Magazine*, Jan. 12, 2017, https://www.pcmag.com/news/350979/comcast-is-americas-most-hated-company.

29   Karl Bode, "The Best and Worst ISPs According to Consumer Reports," *DSL Reports*, June 20, 2017, https://www.dslreports.com/shownews/The-Best-and-Worst-ISPs-According-to-Consumer-Reports-139796.

30   For discussions of different approaches to public-private partnerships, see "BroadbandUSA: An introduction to effective public-private partnerships for broadband investments," National Telecommunications & Information Administration, January 2015, https://www.ntia.doc.gov/files/ntia/publications/ntia_ppp_010515.pdf; Joanne Hovis and Marc Schulhof, Jim Baller and Ashley Stelfox, "The Emerging World of Broadband Public-Private Partnerships: A Business Strategy and Legal Guide," Coalition for Local Internet Choice, May 2017, https://www.benton.org/sites/default/files/partnerships.pdf; Patrick Lucey and Christopher Mitchell, "Successful Strategies for Broadband Public-Private

Partnerships," *MuniNetworks.org*, July 2017, https://ilsr.org/wp-content/uploads/downloads/2016/08/PPP-Report-2016-1.pdf.

31   Lisa Gonzalez, "EPB Fiber Optics Reaffirms Network Neutrality Commitment In Chattanooga," *MuniNetworks.org*, Dec. 19, 2017, https://muninetworks.org/tags-135.

32   Susan Crawford, "You Didn't Notice It, But Google Fiber Just Began the Golden Age of High Speed Internet Access," *Backchannel*, Mar. 3, 2016, https://backchannel.com/you-didn-t-notice-it-but-google-fiber-just-began-the-golden-age-of-high-speed-internet-access-67b3f775fb85.

33   Bill Estep, "Kentucky's high-speed internet project should be done by mid-2019, Bevin says," *Lexington Herald Leader*, Sept. 16, 2016, http://www.kentucky.com/news/state/article102210937.html; Phillip Brown, "Project Status Update," slide presentation, Kentucky Communications Network Authority, Feb. 1, 2018, https://kentuckywired.ky.gov/SiteCollectionDocuments/Presentations/1Feb%20H.Comm%20on%20Small%20Business%20%20InfoTech.pdf.

34   Christopher Mitchell, "Solving Middle Mile Availability Does NOT Solve Last Mile Problems," *MuniNetworks.org*, Sept. 21, 2010, https://muninetworks.org/content/solving-middle-mile-availability-does-not-solve-last-mile-problems.

35   Lisa Gonzalez, "Publicly Owned Conduit: Network Neutrality Can-Do Tool," *MuniNetworks.org*, Jan. 19, 2018, https://muninetworks.org/content/publicly-owned-conduit-network-neutrality-can-do-tool.

36   Federal Communications Commission, "Declaratory Ruling, Report and Order, and Order," WC Docket No. 17-108, Dec. 14, 2017, para. 194, https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf.

37   Joanne S. Hovis, "Closing the Digital Divide: Broadband Infrastructure Solutions," testimony before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology, Jan. 30, 2018, http://docs.house.gov/meetings/IF/IF16/20180130/106810/HHRG-115-IF16-Bio-HovisJ-20180130-U5002.pdf.

38   See for example https://openwireless.org/, a website that promotes the "open wireless movement," and offers advice and software for offering bandwidth to the public.

39   See for example, Verizon, "Verizon Online Terms of Service," Version 16-2, July 24, 2016, http://www.verizon.com/about/sites/default/files/Internet_ToS_07242016.pdf.

40   Only providers of internet infrastructure itself must remain in compliance with CALEA, the Communications Assistance for Law Enforcement Act. The act imposes no requirements on end users. And neither the customers running open access points from their routers, nor the city or other ISP providing the underlying internet infrastructure, are required to be able to identify particular internet users under CALEA.

41   "Telus cuts subscriber access to pro-union website," *CBC News*, July 24, 2005, http://www.cbc.ca/news/canada/telus-cuts-subscriber-access-to-pro-union-website-1.531166.

42   Zachary M. Seward, "The inside story of how Netflix came to pay Comcast for internet traffic," *Quartz*, Aug. 27, 2014, http://

qz.com/256586/the-inside-story-of-how-netflix-came-to-pay-comcast-for-internet-traffic/.

43   David Kravets, "AT&T: Holding Facetime Hostage is No Net-Neutrality Breach, *Wired*, Aug. 22, 2012, http://www.wired.com/2012/08/facetime-net-neutrality-flap/.

44   Jay Stanley, "Trump's FCC Nukes Network Neutrality: What Happens Now?" ACLU Free Future blog, Dec. 14, 2017, https://www.aclu.org/blog/free-speech/internet-speech/trumps-fcc-nukes-network-neutrality-what-happens-now.

45   Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence in the Wake of NSA Internet Monitoring," *Journalism and Communication Quarterly* 93, Mar. 8, 2016, p. 1, http://m.jmq.sagepub.com/content/early/2016/02/25/1077699016630255.full.pdf?ijkey=1jxrYu4cQPtA6&keytype=ref&siteid=spjmq; Pen America, "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor," PEN American Center, Nov. 12, 2013, http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; Elizabeth Dwoskin, "Survey: People Don't Want to Talk Online About the NSA," *Wall Street Journal,* Aug. 26, 2014, http://blogs.wsj.com/digits/2014/08/26/survey-people-dont-want-to-talk-online-about-the-nsa/; Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkley Technology Law Journal* 31, Apr. 27, 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645; Alex Marthews and Catherine Tucker, "Government Surveillance and Internet Search Behavior," *SSRN,* Feb. 17, 2017, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564; "Declaration of Sascha Meinrath," First Unitarian Church of Los Angeles v. National Security Agency, No. 13-cv-03287, 2014 WL 4693046 (N.D. Cal.), https://www.eff.org/files/2013/11/06/allplaintiffsdeclarations.pdf.

46   Lee Rainie and Aaron Smith, "Social Networking Sites and Politics: Main Findings," *Pew Research Center*, Mar. 12, 2012, http://www.pewinternet.org/2012/03/12/main-findings-10/.

47   Jay Stanley, "Why Broadband Carriers are a Menace to Privacy," ACLU Free Future blog, August 1, 2016, https://www.aclu.org/blog/free-future/why-broadband-carriers-are-menace-privacy.