How Does the Internet Work?
# Table of Contents

2  Introduction

4  Me and My ISP

10  An Email’s Journey To You

13  Bandwidth

16  The Network of Networks

22  What’s Your Tier Got To Do With Me?

24  Why Net Neutrality and Data Privacy Matter

25  Privacy, Security, and Vulnerable Communities

27  Why Community Networks Matter for Digital Equity

32  Who Owns the Internet? (An Index)

40  What to Expect When You’re Expecting a Community Network

42  Get Involved
Introduction

The internet seems invisible, but it is actually a massive infrastructure that spans around the world aboveground, belowground, at times through the air, and into your devices. In technical terms, the Internet is a global computer network providing access to a variety of information and communication facilities and functions. That global network consists of millions of interconnected networks all using standardized communication protocols.

In other words, it is a bunch of hardware (data centers, wires, and devices) and software (commands or instructions) that guide bits of information to travel from one place to another. It is a complex, linked set of systems allowing information to travel around the globe in the blink of an eye. It has opened up so many possibilities and has changed the way we communicate, work, and even think.

The Internet plays a major role in your day-to-day life whether you have a home connection or not. In many places in the United States, government resources such as food stamps, healthcare, and job applications are only available online. Public education systems have begun to distribute homework online. The workplace has changed drastically through the possibility of remote work and applications like Lyft and Uber, or platforms like Facebook and Twitter. Then there are tools like GPS, smartphone applications, and artificial intelligence systems like Siri or Alexa, that rely on the internet's data and infrastructure to work. This is called the Internet of Things, or IoT. IoT opens up the possibility for “smart cities” and futuristic technologies like self-driving cars to become a reality. There is so much the internet touches and so much we touch through the internet, it's important to understand how it works, how it is governed, and where you have agency within it.

In the process of creating this booklet we learned that Internet infrastructure was built and is governed by a series of business agreements, federal and local policies, and is influenced by you, the consumers and producers of the content that lives on it. It is an interwoven system of systems (or network of networks) that include people, equipment, buildings, businesses, electricity, signals, and, yes, tubes and wires. At its best, the internet is a massive decentralized system that connects us to each other and creates a hotbed of data that maps our human existence.

After years of tenacious work building community wireless networks with residents in Detroit and New York City, we realized the agency we have is in teaching and learning, then building the infrastructure and policies we need to maintain a healthy integration of interconnected technologies in our lives and communities -- one that does not feel like it is controlled by gatekeepers we can't access. Our work has taught us that in order to have more of a say in how we communicate with each other, we need to understand the internet's physical infrastructure, where we fit into it, and how we can influence it.

Our current internet has been shaped by political and economic forces over time, including historical forces of inequity and oppression that became embedded in its physical form. But that is not how it has to be. The existing telecommunications industry does not prioritize equity, so many people -- especially those living in historically poorer or underserved areas -- are left paying astronomical prices for low-quality internet connections. These days the internet is as important as healthy food, clean water, and housing. It should be accessible to everybody. By demystifying the internet we can inspire people to build their own infrastructure, or just to advocate for better conditions wherever they live. This booklet serves as a place for you to begin your education. Even if you're not ready to build, you can think about how to change how the internet is distributed or designed in your community.

The authors and editors of this booklet are a group of artists, technologists, educators, and mediamakers invested in redefining technology to be more equitable, democratic, and participatory, and to contribute to building a more just society. We hope you enjoy our interpretation of how the internet works. Happy reading!
Our journey starts when you sign up for an internet connection with a local **Internet Service Provider (ISP)**. An ISP is a company or entity that provides subscribers with access to an internet signal.

Maybe you live in an area with different options for service providers, or maybe you live in an area that only has one or two providers. Either way, when you sign a contract with a service provider, you are essentially signing up for a connection to that ISP's internet infrastructure of wires and tubes, or its **network**. That ISP's network is likely connected to another ISP's network, making a network of networks that your messages travel through to get to their destination.

Here is how networks of networks work together to let your stories travel through the internet.

Your connection comes from a local ISP's network of wires and tubes. It's easy for you to connect with anyone connected to that network because you’re all using the same wires and tubes.

But not everyone you communicate with is connected to the same network.

There can be lots of networks within your town.

There are also lots of networks crisscrossing your city, your state, and even the globe. This network of networks -- and the big global data “backbones” that interconnect them all -- offer many paths for data to travel through.

But how are we able to communicate between networks and across the globe? We can't put emails on planes, trains, or ships. Let's take a look at how ISPs connect to each other and how data moves from one network to another.
Someone has signed up for service from their local ISP. They can easily communicate with other people nearby on that network using the devices, tubes, and wires owned by that ISP.

Yay! They are connected! But what about a person who has a contract with a different ISP on the same block? They are both connected to their ISP’s **Point of Presence (PoP)**, but not to each other. PoPs are where single ISPs house their own internet infrastructure.

PoPs (also called “internet hotels,” data centers, or switches) are where an ISP’s wires all come together. From the PoP, the wires branch out and wind their way through your neighborhood to bring data to and from your door (people call this “the last mile”). PoPs can be windowless buildings your downtown, or a small metal cabinet on a street or in a housing development.

We can connect different networks through things called **Internet Exchanges (IX)**. This is a diagram of what they do.

Yay! The person who has a contract with ISP1 is now connected to the nearby person who has a contract with ISP2.

**key nugget**

Internet Exchanges (IX): IXs are where multiple ISPs plug into each other. ISPs and municipalities own and maintain IXs. There are also companies (data centers) that specialize in owning and renting out space at IXs so that different ISPs can connect.

An **Internet Exchange point** allows for ISPs to exchange internet traffic between their networks. This is what makes the internet decentralized. Everyone needs everyone else’s network to create a worldwide network.
Things get a bit more complicated when you want to connect with someone farther away. Our friend in Chicago isn’t connected to their Detroit friend even if they both have a contract with the same ISP. They are too far away to be connected via the same wires and tubes.

Think about how many highways you have to travel to get across the country. Usually, your route uses many different highway systems to get to your destination. These regional highways systems are joined together by ramps and sometimes have tolls.

A Regional Internet Exchange does a similar thing in connecting faraway friends online who share the same ISP.

The Regional IX can also connect two friends who live in different cities AND have different ISPs.

These exchange points are important places that your data flows in and out of. They seem complicated, but up close, an exchange is just a bunch of computers that have the ability to process large quantities of data all at once and direct the data along the path to its destination. It is amazing to think that all of the data in all of our computers rely on little boxes -- or servers -- to get from one place to the next. IXs are the locations where the tubes and wires that span across the globe underground are brought together to connect traffic among different networks.

These exchanges are usually owned by companies, and can be accessed by individuals with the right resources. If you are interested in building a community network and want to know more about where your internet comes from, start by looking for the nearest Internet Exchange Point in your area. If there is one in your town or city, you’re in luck! Get to know the folks who own it and see if you are able to plug into it. We’ll go more into this later, but for now it’s important to know that there are hubs like Internet Exchanges that allow ISPs’ networks to connect to each other. The millions of exchanges and ISPs around the world create the World Wide Web.

A Regional Internet Exchange is a massive information relay point between cities and regions where large-scale backbone lines or big pipes and tubes come together. These are usually large, specially-designed, secure and climate-controlled buildings owned by private companies.
Now that we know the internet is series of physical pathways for data to travel through, let’s look at how an email moves through that system to get from one computer to another.

Imagine our Chicago friend writes an email inviting their Detroit friend to a birthday party. They go to their browser window, log into their email provider using the Internet Protocol HTTPS, (HTTPS://example.com), write an email, then hit “send.”

**Internet Protocols (IP)** are agreed upon, standard formats that all internet-connected devices use to talk to each other. For content to be visible and findable on the internet, it must follow standard protocols. You can think of IP as a language used to direct data as it races around the internet's tubes and exchange points. Two important protocols are secure hypertext transfer protocol (HTTPS, or the digital language internet traffic is coded in), and domain name service (DNS, or addressing and wayfinding tools), which direct traffic around the internet.

Once the send button is pushed, the email program translates the data into small bursts, or “packets,” of 1s and 0s. 1s and 0s are the letters in the data alphabet. They are lined up to create sentences, or sequences that computers can understand. The sequences of 1s and 0s carry the directions on how to assemble and present the message once it hits its destination.

Each packet is labeled with a destination address attached (just like a letter in the real world) called an Internet Protocol address. An **IP address** is a numerical label assigned to each device connected to a computer network.

**An Email’s Journey To You**

There are two kinds of IP addresses: public and private. Think of public like the address of the house, and private is the way to get to specific folks in the house.*

*We’ll be comparing the internet to the postal system a lot.*
The email is translated into packets of data, which are transmitted from Person 1’s computer through their internet connection, which in many cases is wireless. The packets travel through the wifi signal to your wireless router. Then the information is translated by the modem to travel as electrical waves along a physical cable or fiber optic cable to an ISP1’s Point of Presence (PoP) in the neighborhood, which is where the ISP’s wires all come together. From there it goes to an IX, where ISP1 and ISP2 meet. Each device plays a role in translating and sending the information forward.

At the IX, Person 1’s email packets travel through a physical connection (usually a fiber optic cable) running between the two networks’ servers (computers with lots of memory) that live in server cabinets inside the IX.

The packets are sent back along ISP2’s cables until they reach Person 2’s computer by following the IP address. Person 2’s computer reassembles the packets into an email. And all this happens in a matter of milliseconds. Success! Person 2 is going to the party!

For the internet to work its magic in milliseconds, it matters how reliable and fast those connections are. To understand how we get fast connections, we have to talk about bandwidth.

Everything you do on the internet is made of data. Data is a series of numbers: zeros and ones. The more data, the more zeros and ones. And all data takes up space as its electrical signals or “waveforms” pass through the cables that connect us.

Different things you do on the internet take up more or less space. You can imagine an email is like a letter -- it doesn't take up a lot of space. An email with an image attached is a little bigger, like a manila envelope. And maybe downloading a video is like a giant crate.

On the internet, the amount of data your connection to the internet can handle in a given amount of time is called bandwidth. Bandwidth is measured in bits per second. Bits are just those zeros and ones.

We can imagine that post office trucks are like bandwidth. A local postal van can handle a limited amount of data. That's like a low-capacity connection. A truck that takes the mail from the local post office to the regional post office can handle more. And the big distribution trucks can handle the most. That's a high-capacity internet connection.
Your internet speed depends on the capacity of the internet connection AND the kinds of wires, tubes, and connections your data travel on. There are three kinds connections: fiber optic, coaxial cable, and copper DSL. These are like roads.

A **fiber optic cable** is like a super-fast highway. The electrical signals move through fiber optic cables literally at the speed of light.

Highways can get clogged with traffic, but they can also allow for tons of packets.

A **coaxial cable** is like a county road that gets backed up and slow at rush hour. It takes time to squeeze data through a smaller-capacity tube -- in reality, waveforms or electrical impulses have to physically vibrate across a bunch of wires, and that can slow things down.

A **DSL copper wire** is a slender little wire that transmits longer wavelengths more slowly. It’s like a bumpy country road. Packets can fall off the truck and get lost, leading to jumpiness, jittering, and dropped connections.

If you’ve purchased a high-speed connection (a big truck’s-worth of data), but the cable or copper wire network you’re on can’t handle that amount of data, you’re not getting your money’s worth. Also, if you have low bandwidth, a big package won’t fit, or will take a long time to get where it’s going.

This is why bandwidth is important. It’s not right for some people to have shitty internet and other people to have super-fast awesome internet, especially if they’re paying the same price. That makes some voices louder than others, and creates disparities in what different people can do in our digital world.
The Network of Networks

Now that we've got the basics, let's get deeper into the business relationships between different networks. We can better understand how this all works by comparing sending an email to sending a letter through the postal service. The relay systems used to move a physical letter from one town to another are similar to how the internet uses data centers and protocols to route emails around the internet. That said, the post office doesn't rip up your letter and reassemble it in your mailbox (but who knows what the future has in store for us).

Once the email packets enter the ISP's Points of Presence (which are like local post offices), they then move through larger ISPs' infrastructure well beyond your local provider's location. The Internet Exchange (IX) is like a post office hub or distribution center that relays packets to their next destination in the network of networks.

When you send a letter, you have to pay a toll or buy a stamp to get your letters through the distribution centers. The internet works in the same way. Service providers pay a fee to connect to other networks at the big connection sites so that they can use someone else's infrastructure to get traffic to and from their customers. Moving your traffic through different providers' infrastructure is called transit.

Transit is how you can connect to people on other networks locally, regionally, and globally.
Cellphone networks share infrastructure with fixed internet services. All those wireless signals end up going in the ground, too, so they’re also part of the “network of networks.”

Sometimes, messages travel through enormous underwater cables. These are called the backbone of the internet.

When Internet Service Providers give other ISPs access to their network for free, it’s called peering. Peering allows customers on both ISPs’ networks to be connected directly. It’s like two local post offices having an agreement that you can always send letters to people in each other’s towns for free without any stamps.

Peering is core to what makes the internet so fluid and shared, but when it works it’s mostly about the relationship two companies have with each other. The more ISPs that connect with each other without tolls, the more resources and faster speeds their customers have access to. It can be a win-win situation, but business tactics can get in the way. Peering and paying for interconnection via different ISPs can be hard to navigate. It’s an active marketplace where negotiations matter and lots of different businesses are competing.

To navigate the various internet deals out there, it helps to understand the different Tiers of ISPs, which have different-sized networks and assets.
**Tier 1 networks** are huge, own lots of infrastructure worldwide, and can reach every other network on the internet without purchasing transit. They are directly connected to the internet backbone, or own parts of it. The **backbone** is the main artery for the internet that travels under the sea and through the woods.

**Tier 2 networks** have peering agreements with other networks, but still purchase transit or pay fees to reach at least some portion of the internet. They have the highest-speed connections to Tier 1 networks. They usually cover a specific region and their customers are either smaller ISPs or large companies, like medical centers and governments, that require major internet speeds and extreme reliability to get their work done. If you are trying to get a connection for a community network you can start by looking for the nearest Tier 2 provider in your area. They can give you access to Tier 1 infrastructure, or, in other words, provide a point of entry to the global internet for a smaller network. Another term used to describe this purchase is buying a “backhaul link” to the internet backbone. **Backhaul** can refer to both the physical infrastructure and the contracts covering your connection to the backbone.

**Tier 3 networks** generally purchase transit from other networks to reach the global internet, focusing on the retail market in local places. This is the network that gets you to that **last mile**, into neighborhoods and homes. If you are building a community network, you could work up to becoming a Tier 3 local network! Once you begin distributing IP addresses, you are acting as an ISP. Places all around the world are thinking about how this way of providing internet can be community-owned and operated. If you don't want to start an ISP you could simply share your internet connection with your neighbors. This is still a form of a Tier 3 network!
What’s Your Tier Got To Do With Me?

If you are thinking about building a community network, here are tips on navigating your relationship to other tiers and internet providers.

You might think your only option is to buy service from whatever retail-facing Tier 3 ISP is in your neighborhood (like Cablevision, Cox, Comcast, or Verizon), but that's not true! You have options in terms of who you purchase service from.

There may be a nonprofit Tier 2 ISP in your state whose mission is to help community networks connect to the internet backbone. A few examples are NYSERNet in New York State, Maine Fiber, and Network New Hampshire Now, which run publicly-owned fiber optic networks as an alternative to purchasing Tier 1 or 2 backhaul for communities.

Or you may have a relationship with a university or hospital that participates in Internet2 (a national 501(c)(3) non-profit network run by a consortium of educational and research institutions).

You may also be lucky enough to live in a state with cooperatively-owned electric utilities, like Missouri or Tennessee. These electricity distribution systems have fiber optic backbones that can also carry telecommunications traffic, if co-op members agree. (There are tips on page 40 and 41 on how to find these kinds of providers).

Lastly, community networks may purchase transit or space in IXs from multiple ISPs.

Some considerations as you figure out how you will connect to the backbone:

- Tier 1 connections are the most expensive and high-capacity on the internet. You need to be near an IX to get access to their services, so this option may not be available for folks in rural areas or smaller towns.
- Tier 2 ISPs may be able to provide business-class, shareable service at a lower cost than Tier 1 providers, but community networks will still have to pay for Tier 2 traffic going through Tier 1 IXs. You may also need to pay for transit to get this connection to where you need it.
- Tier 3 networks may not be prepared, interested, or set up for customers who want to share or re-sell connections (though sometimes they are).
- Non-profit, publicly owned, or utility co-ops may be more open to negotiating around peering or transit agreements as well as how they treat customer data.

Remember this diagram? As you’ve probably figured out by now, it’s really simplifying the story. Even if you send an email to your next-door neighbor, your data is passing through a lot of third parties along its journey. There is a fee in your contract with your ISP that covers the cost of using those other connections along the way.
Why Net Neutrality and Data Privacy Matter

The Federal Communication Commission’s (FCC) Open Internet Rules of 2015, known popularly as Net Neutrality, for the first time classified data and broadband as “common carriage” or utility-grade services, meaning that Internet Service Providers were not allowed to discriminate among kinds of digital traffic. According to these regulations, ISPs would not be permitted to cap, throttle, or prioritize data from particular users or clients, but would have to be “neutral,” meaning that more powerful or wealthy interests would not be able to edge out smaller, independent voices. A non-profit’s or small company’s website and traffic should be as accessible to users and as fast as that of internet behemoths like Amazon and Google.

These 2015 rules ushered in a set of related public-interest reforms, including a 2016 federal rulemaking to protect consumer privacy. On October 27, 2016, the FCC adopted the Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Act. Under these rules, telecommunications carriers were required to protect the confidentiality of customer data. Internet providers would be prohibited from collecting, storing, sharing, and selling certain types of customer information without opt-in user consent, forcing ISPs to be more transparent about when and to whom they would sell data. Providers could “no longer condition the provision of service on the surrender of privacy rights.”

Despite broad public support for the Open Internet (Net Neutrality) Rules and Protecting the Privacy of Customers Rules, under President Trump the FCC repealed both, creating uncertainty among consumers about their online safety and health and users’ overall ability to access services and information fairly and without discrimination or information control by the same companies that own the infrastructure.

Privacy, Security, and Vulnerable Communities

Thanks to data breaches, identity theft, stalking, and high-profile hacking, internet users are increasingly concerned about transacting their lives online. Flaws and exploits in interconnected systems have created vulnerability risks for governments, corporations, and consumers. The same technologies that can empower citizens and open opportunities for innovation and collaboration can also enable perverse incentives in the market and even the transgression of human rights through both corporate tracking and state surveillance. Communities of color are particularly vulnerable to digital profiling, predatory marketing, digital voter suppression and manipulation, and both corporate and state surveillance.

While customers have some choice with regard to providers and platforms like Facebook, Twitter, Amazon, or Netflix, anyone who wishes to use the internet must access it through an ISP. Yet ISPs do more than charge and collect fees for service; they also extract value from users’ engagement with digital services. As traffic (data) passes through their systems, ISPs have access to personally identifiable information (PII) and anonymized customer data, including browsing history, application and platform usage, geolocation and more. Valuable data for advertisers and other third parties include financial and credit histories, full or partial Social Security numbers, and home addresses, phone numbers, and other personal data. This is why it matters what kind of agreement you make with your local ISP or transit and backhaul providers.

Aside from privacy concerns, the loss of Net Neutrality could also mean that our information ecosystems become increasingly fragmented. Different ISPs, platforms, or media players could offer à la carte menus of information services to choose from, limiting the free flow of information and potentially spreading targeted messages to specific communities. As we lose our shared information commons, the news and information we depend on for democratic governance -- and empathy and cooperation with other human beings -- degrades. And ultimately this could mean that only the loudest voices backed by the most money can afford to make themselves heard.
In the last few years, many digital equity and justice advocates have fought back against flaws in our information systems by starting community networks with the goals of equity, building community wealth and resources, and providing free and fair access to information. Current developments in technology policy and culture like the development of artificial intelligence, the use of algorithmic decision-making, media consolidation, and corporate control of government are also driving the desire for healthier, more grounded, and equitable relationships between communities and technology.

The industry has fought back against municipal and community telecommunications ownership by asserting that government would have an unfair advantage in a competitive environment, using this logic to create bans on municipally-owned networks in at least 19 states. Telecommunications incumbents have also starved community networks of the data (or “backhaul”) connections that would enable them to build their own distribution networks, like locally-owned ISPs and broadband co-ops.

The current surge in community networking has the potential to push back on industry consolidation. Community networks can set new standards for equity, knowledge-sharing, and skill-sharing, and can generate a platform for creativity and community self-determination. But this is only possible with an understanding not just of technology, but also the social and political context of networks.

It is important for community networkers to remember that networks are not in themselves a solution to the problems of digital inequity, risk, harm, and information insecurity. In fact, unless community networks have strong and principled foundations and agreements, they can reproduce many of the same flaws and inequities that exist in the current market.

Creating functional, self-governed and owned networks takes years and a lot of knowledge, clear intention, and resources. Yet the process of cooperating to build a network can strengthen community ties, spread a knowledge base, demystify technology, and help us flip the script on our relationship with information gatekeepers.

Historically, the power and consolidation of the telecommunications industry has shaped our physical communications networks. Unlike most other kinds of utility infrastructure (like electricity, roads, and water), our communications systems -- from telegraph and telephones to radio and the internet -- have been provided by privately owned companies from the start.

The Federal Communications Commission (FCC) -- the national agency in charge of telecommunications in the US -- does not plan and build communications systems, but rather creates laws to encourage growth in the sector, with the goal of covering maximal service areas while generating corporate profit. Historically, the FCC has been tightly connected with and led by industry players, relying on the reach and power of monopolistic companies like Bell in the 20th century, and AT&T and Verizon now, to determine where and how to provide communications services.

Because telecommunications companies are not required by government to provide equitable service to all areas and residents, telecommunications services have rolled out unevenly, and mirror other historical inequities in investment, housing, and services.

The Master Switch (Tim Wu) tells the story of phone companies and “natural monopolies” in the US. AT&T and Verizon each control around 30-35% of the US telecommunications market, for a combined total of almost 70%.
Redlining is the name given to various practices involving the denial of services such as banking and insurance, or even housing, to residents of specific neighborhoods or urban areas on the basis of race, income, status, or class. - Jeffrey Shantz, Encyclopedia of White-Collar and Corporate Crime, 2013

Areas of the US that were redlined (zoned to prevent investment) in the 1930s and 1940s, like low-income neighborhoods in downtown Cleveland, Philadelphia, and Detroit, along with many majority-minority cities in the Southern US, have also been short-changed when it comes to investment in internet infrastructure, lagging behind in maintenance and modernization of their networks.

Recent research from the National Digital Inclusion Alliance (NDIA) indicate that AT&T has systematically underinvested in infrastructure in low-income neighborhoods in Cleveland, Detroit, and Toledo (Callahan, 2017; Callahan, 2017b).

AT&T failed to maintain or upgrade copper line networks in poorer neighborhoods that correspond geographically almost exactly to Federal Housing Administration redlined maps from the 1930s.
Areas that do not show potential for strong return on investment have broadband service running over older legacy infrastructure (built for earlier technologies like phone and cable TV). For example, in digitally-redlined areas, internet providers have not laid fiber optic lines, but instead rely on old copper wire phone networks for DSL service, or coaxial cable networks that are branched and spliced over and over again, diminishing speed and quality of service for users. (Remember, it takes time to squeeze a ton of data through a small-capacity tube.)

Copper DSL connections experience slowdowns and outages in heavy rains or flooding (already happening frequently in coastal cities like New York), and customers on overburdened coaxial cable connections experience slowness, latency, jittering, and dropped connections, especially at busy times of day. Yet they often pay the same rates as customers in better-served areas.

The lack of investment and competition in many under-invested communities results in high monthly fees for access to old legacy infrastructure, with limited options to upgrade for new bandwidth requirements and new technologies like fiber optic cable. This creates cycles of disinvestment, as infrastructural digital inequity reinforces layers of historical discrimination. The consequences of such inequalities build up as technologies evolve.

The friendly relationship between the FCC and industry also affects efforts to create transparency and publicly available data about networks, so it’s hard even for many local officials to know where there may be underserved areas within their own cities, towns, and counties. While the FCC does collect a tax on all telecommunications services called the Universal Service Fund -- earmarked for infrastructure development and subsidies for rural, low-income, and otherwise underserved communities -- the “Digital Divide” persists, with progress on closing the gap slowing and plateauing over the last half decade.

At the national level, the number of people adopting and using broadband services has hit a plateau, and even dropped 8% between 2016 and 2018 particularly among low-income, Latinx and Black communities. The access gap between White users and Latinx users is now 25%.

This all matters because internet is a now basic requirement of social, cultural, and economic participation. And increasingly, as ISPs like AT&T and Verizon acquire content providers and media platforms, they will control both the flow of information through physical systems (including your personal and private information), and also shape content and information itself.

The Pew Internet and American Life project is a great resource to research trends in internet use.
Who Owns the Internet? (An Index)

Part of the Internet
The internet is an interconnected network of networks. It includes different parts, owned by different entities.

<table>
<thead>
<tr>
<th>Personal or end-user “client” devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensors, beacons, monitors, and other automated devices</td>
</tr>
<tr>
<td>Translator devices</td>
</tr>
</tbody>
</table>

What It Does
Remember, every part of the internet needs power to work. There is a symbiotic relationship between power and communications networks. This means both political and economic power. It also means electricity!

Who Owns It

Your portal to the internet: devices that send and receive digital information (such as computers, smartphones, watches, tablets)

Individuals or public access points such as libraries, schools, or public computer centers

“Internet of Things” or IoT devices (such as smart thermostats, foot traffic monitors, surveillance cameras, or environmental sensors), which collect and send out a steady stream of data

Municipalities, researchers, corporations, businesses, and, increasingly, individuals

Interconnection devices (such as modems, routers, radios, and switches), which relay and convert digital traffic to and from different devices (wireless or fixed)

You may own your home router or modem, or lease it from your ISP; many translator devices are owned by ISPs, businesses, or institutions that have their own networks; ISPs and other telecom providers own the bulk of these
### Part of the Internet

<table>
<thead>
<tr>
<th>Protocol</th>
<th>What It Does</th>
<th>Who Owns It</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS: //</td>
<td>Agreed upon, standard formats that all internet-connected devices use to talk to each other. Two important protocols are secure hypertext transfer protocol (HTTPS), and domain name service (DNS), which direct traffic around the internet. For content to be visible and findable on the internet, it must follow standard protocols.</td>
<td>These are not owned by anyone, but are determined by international standard-setting bodies including the IEEE (Institute of Electrical and Electronics Engineers), ICANN (Internet Corporation for Assigned Names and Numbers), the Internet Governance Forum (United Nations), and ITU (International Telecommunications Union)</td>
</tr>
</tbody>
</table>

**Computers that store and “serve” up content (like web pages) in response to HTTP requests at any point on the internet. Translator devices transfer data (in the form of “packets” of digital information) to and from servers to “client” devices.**

ISPs have many servers to store data, but platform and cloud services like Google, Amazon, or Apple have immense “server farms” that store digital information from all over the internet, including “cloud” accounts. Your computer can also act as a server, if it is serving up data to other devices on a network.

**Anytime two or more computers are connected, you have a network. Often most computers within a home, business, or institution are connected, and can communicate with each other without having to send or receive information from the outside internet.**

A Local Area Network can be owned by whoever owns the translator devices on the network (such as a business or university), or you can own your own home network.
**Part of the Internet**

**Wide Area Network (WAN)**

**Transit**

**Points of Presence (PoPs)**

**What It Does**

When two or more networks are connected to cover a wider area, they form a wide area network.

Wired or wireless connections (fiber, cable, DSL/copper, or wireless relays) that allow different actors and owners to move traffic around among different networks. In many cases smaller network operators have to pay each larger ones for transit.

“Internet hotels,” data centers, or switches where ISPs have lines that come together to serve their local “last mile to the consumer,” translating data and relaying it to and from individual households and customers. Large PoPs often look like windowless buildings in the downtown of a town or city and also house many servers to store data locally, but a PoP can just be a small metal cabinet on a street or in a housing development.

**Who Owns It**

Most WANs have multiple owners across different segments, from the end users connecting their devices at the point of access to the translator devices and servers the information travels among and the lines (wires or wireless) that it travels along.

Transit networks are most commonly owned by ISPs, or by internet infrastructure “landlords” like Empire City Subway (which owns the conduits that internet lines run through under the streets of Manhattan) or by municipalities.

ISPs, municipalities, or communities that offer internet service must own or rent PoPs to serve more than a few customers.
Part of the Internet

Peering

When ISPs come to an agreement about sharing data across each other’s networks, they become “peers,” offering each other free transit or in-kind agreements.

Peering points

A physical location where two or more ISPs come together so digital traffic can pass back and forth between them. For example, your ISP connects with your friend’s ISP at a peering point so that you can send your friend an email.

Backbone

Huge high-capacity transit lines that can move large amounts of traffic among different WANs, including among regions, countries, and under the ocean.

Internet Exchanges

Peering places where transit and large-scale backbone lines or “pipes” come together. These information relay points can come in different sizes, e.g., massive regional internet exchange points that handle traffic from coast to coast and across the seas.

What It Does

Who Owns It

Peering is a form of cooperative ownership and sharing.

ISPs and municipalities own and maintain peering points. There are also companies (data centers) that specialize in owning and renting out space at peering points so that different ISPs can connect to each other.

Regional ISPs or privately-owned data centers.

Privately-owned operators, including huge corporations like Digital Realty.
What To Expect When You’re Expecting a Community Network

Here are a few questions to ask as you plan your community network and how it will fit into the larger physical infrastructure of the internet.

- Where is the nearest Internet Exchange point?
- Which backhaul and transit providers have space at the nearest IX?

Having a local IX allows for traffic to be delivered in a more efficient and cost effective way, thereby reducing the average per-bit delivery cost of their service. This can lower prices and improve routing efficiency, making a local network robust and fast. You can think about it like food miles. The farther food travels to your home, the less fresh it becomes, and transit delivery of that food drives the price up. The closer to home you are able to get your food, the fresher and likely cheaper it is. The internet works in the same way.

- Does your state have a statewide ban on municipal broadband ownership? (If so, don’t despair! It just means you have to go the super-local route, instead of partnering with your municipality on transit.)
- Who can you work with in your community to make something happen?
- Do you have a lot of love? Starting an ISP requires love and patience!

It’s important for you to know your options for getting backhaul. Remember, you are not limited to Tier 3 ISPs! There may be a better way for you to connect to the internet backbone.

- Is there a non-profit ISP in your state whose mission is to provide connectivity to community networks?
- Does your state have electric cooperatives? If so, do they have fiber backhaul you could use, and have the co-ops determined whether they wish to provide telecommunications backhaul?

- How does your library, recreation center, community nonprofit, or municipal government get their backhaul? Ask around!
- Do you know anyone at a university nearby? Can they ask their university where they get their backhaul? (Hint: go to the IT office)
- What kind of partnership would you and your community be interested in entering into with a university, a government, or a utility co-op? Chances are you have something that’s of interest to them (like the trust of local residents, the organizing chops to put together events and programs, or customers). Assume your power, not your powerlessness, when you enter conversations.

When you are choosing someone to get backhaul from, you can ask these questions:

- Do they provide net-neutral backhaul? Would they be willing to work with you on a mutually acceptable Memorandum of Understanding (MOU)?
- What are their terms of service, and would you have to pass those on to your users to avoid legal liability?
- Can you create a contract where you can resell data? If so, can they guarantee any promises you make to your users will be honored when the data leaves your network and passes through theirs?

In the Catalonia region, guifi.net is a network of networks featuring a “backhaul commons.” Members pay into the commons based on how much traffic they move through the system. So, if someone wants to build a network, and they commit to guifi.net’s network principles (inclusiveness, openness, and community participation in network construction and governance), they can use the backhaul commons (and contribute to it) as a resource, regardless of the type of network (and type of equipment, ownership, or governance model) they have.
Get Involved

If you want to learn more about the community wireless and technology movement, here are a few ways to get involved:

- **Hold critical conversations with your friends and family about technology and the future.** Get your family and friends to brainstorm ways which we can reimagine digital access and equity. Here is a link to our Teaching Community Technology Handbook. Check out the chapter on facilitation for ideas.

- **Let us train you in community technology!** If you feel your community is in need of a community wireless network, we might be able to train you! We are working on making our curriculum into a Digital Stewards knowledge base so you can learn how to be a steward on your own or have the materials you need to teach others!

- **Fight for Net Neutrality and digital privacy.** On December 14th, 2017, the FCC voted to reverse Net Neutrality. Call your representatives and ask them to fight for your right to privacy and a free and open internet. Talk to your local ISPs and ask them to commit to practicing net neutrality even if the federal government says they don't have to. Let us know how it goes and share any strategies you find helpful.