Big Money for Broadband, A Risky Connection for You

ISPs sell your personal data and put profits ahead of privacy. Regulations can help.

Claire Park

Shopping for something online, streaming a video, or scrolling through an article all pose severe risks to personal privacy, as websites, platforms, apps, and tech companies collect massive amounts of data on their users. Just getting online in the first place, however, poses a great risk as well. Internet service providers (ISPs) are uniquely positioned to take advantage of personal data, as they have near-total access to all traffic flowing over their networks. Broadband providers routinely collect data on users' locations, web browsing, app usage history, and more. In some cases, ISPs also collect data on content their users run across. New advancements in network technology, including private and public mesh networks, introduce new wrinkles to protecting privacy online that make the need for protections all the more urgent. People must be able to access the internet without giving up their privacy.

What Information Can ISPs Collect, and What Are They Doing With It?

Like other businesses, ISPs can collect information required for them to provide service. This includes a customer's name, age, address, and financial information. As telecommunications carriers, they also have access to information regarding the quantity, technical configuration, type, destination, location, and amount of use of service. Most of all, ISPs have unique access to the content of all unencrypted internet traffic across their network. They can track every website and service that the subscriber visits or has visited, and how often, when, and where people are going online.

This access to web browsing history allows ISPs to infer additional information about their customers. For instance, ISPs can use search traffic to figure out political viewpoints, gender, purchasing habits, time spent on streaming platforms and which ones.

Providers can also redirect and monetize users' searches. In 2011, researchers at Berkeley found that internet service providers were doing just that, redirecting traffic intended for major search engines instead to third party proxies for the sake of generating revenue. Users wanting to read *The Wall Street Journal* and searching for "wsj," for instance, would instead be redirected to a page offering subscription deals for the newspaper. ISPs were monitoring and tampering with search traffic, sending information to marketing companies who then redirected queries to the appropriate retail website and gave ISPs a cut of the proceeds.

Beyond just using inferential data for profit, ISPs have been legally allowed to directly share and sell users' personal information without explicit consent for advertising purposes since 2017. Only three states have legislation requiring ISPs to keep information private unless the customer expressly consents to its sharing. ISPs have additionally tried to make further profits off of their customers by illegally selling consumer location data to data brokers, who then sold that information to a wide variety of actors, including law enforcement and bounty hunters.

Recently, the Federal Trade Commission (FTC) released a report showing that ISPs collect huge amounts of sensitive data on consumers, then use that data in ways that can severely harm people. The report emphasized that the vertically integrated nature of the telecommunications industry (ISPs not only provide a service, but are also involved in the production and distribution of content, advertising, and analytics) allows providers to collect a large volume of highly granular data across product lines. This uniquely enables ISPs to track one person's search history to what they're streaming, and then use that data to classify and then advertise targeted content to individual consumers. As the agency explains, "A consumer could get an ad on her work computer related to an intimate or sensitive video she watched on her personal laptop, habits revealed by her wearable device, or retail purchases.". The FTC also noted the dangerous industry trend of selling consumers' granular location data, with public reports showing that this information can end up in the hands of car salesmen, property managers, bail bondsmen, bounty hunters, and others. The clear potential for harm these sales create emphasizes the need for consumer protections against the collection and use of personal data.

An Internet Connection Isn't a Luxury, but a Necessity—So Is People's Privacy While Online

The COVID-19 pandemic reiterated the essential role the internet plays in our daily lives, including work, school, medicine, and social life. Students without home internet connections, for instance, were left out from online learning and couldn't attend virtual classes without leaving home. Internet usage within the United States has steadily increased over the last two decades, with 85 percent of those in the U.S. now reporting they go online daily. As people navigate their lives online, protecting consumers' right to their information and privacy is a must. Consumers shouldn't have to choose between privacy and online access, especially when the latter is increasingly becoming mandatory.

The lack of competition in the broadband marketplace makes it even more difficult for people to safeguard their privacy. At least 83.3 million Americans can only access broadband through one provider, so even if there are providers interested in better protecting privacy, many wouldn't be able to choose them.

People should be able to feel secure that their personal data, including financial information, location, health history, and more, are safe, and be empowered to protect it—not just on particular digital platforms or websites, but from the moment they connect to the internet.

Further Advancements in Network Technology Pose New Concerns for People's Privacy and Safety

Due to the high degree of monopolization in the broadband marketplace, most consumers are familiar with big-name ISPs, such as Comcast, Verizon, and Charter/Spectrum. These are longstanding, traditional networks built on cable and/or fiber infrastructure that uses wires and cables to provide internet service from one point to another, usually a home or business. People purchase internet service directly from these

companies, entering into service agreements that dictate terms and conditions, and are regulated by existing local, state, and federal telecommunications laws. Less ubiquitous satellite and fixed wireless service providers, such as HughesNet or Starry, feature different kinds of network technology (satellites with service stations and terminals on the ground or towers and buildings with antennas coupled with microwave technology, respectively), but they also enter into direct agreements with consumers for the explicit service of getting them online, and are therefore regulated as internet service providers.

The discussion around appropriate legal classification of ISPs and corresponding non-privacy regulations is itself fraught, but the emergence of new network technology, such as mesh networks, introduces a lack of regulatory clarity. Generally, networks used at home or at work operate by routing devices through one central access point. In a mesh network, different Wi-Fi access points can find other routes to other devices. With multiple points of connection, each node can send, receive, and relay information on behalf of other connected devices. Should one or a few connection points fail, the data can take another path through the other connected nodes in a mesh network. Some examples of this technology in use are community mesh networks in San Rafael, California and the Red Hook neighborhood of Brooklyn, New York.

More recently, companies other than traditional ISPs have begun employing mesh network technology. Amazon, for instance, launched Amazon Sidewalk, a mesh network that pulls bandwidth from an Amazon user's internet service using Amazon devices including smart speakers and video cameras. Apple also has rolled out AirTag, a tracking device that uses connections to the Bluetooth network of Apple devices ("Find My" network).

These networks pose new potential threats to consumer privacy and safety, while also raising questions for the current legal framework protecting consumer privacy. For example, on the consumer privacy front, Amazon's Sidewalk mesh network will, at a minimum, give the company access to device IDs, internet network health status, bandwidth caps, and other metadata. In terms of consumer safety, both Amazon products and Apple's AirTags may be abused to track and stalk people, promoting abusive behavior. Reporters have shown how AirTags can easily be planted into others' bags, in cars, or on a person themself to track an individual's exact location. Amazon could connect its new Sidewalk technology to its Ring home doorbell surveillance cameras, creating neighborhood-wide video surveillance systems that could lead to more police violence, greater racial profiling, and potentially insecure storage of video footage that could be shared and used widely beyond people's knowledge across many cities and regions.

Comprehensive Privacy Legislation Would Protect People and Their Personal Information Online

Some regulations and statutes do exist to protect consumer privacy from telecommunications providers, such as those around customer proprietary network information (CPNI) enacted by the Federal Communications Commission (FCC). These regulations require carriers to adequately protect their subscribers' CPNI, which includes current charges, directory assistance charges, usage data, calling patterns, destination and location of data, and more. CPNI regulations also limit the use of such information for marketing services that customers are already subscribed to, or use of the information to prevent customers from switching providers.

CPNI rules, however, have their limitations. As a previous report from OTI pointed out, the definition and rules for CPNI were created in the era of telephone, and do not encapsulate new categories of information and information processes that exist with broadband internet. In 2016, the FCC therefore adopted a Broadband Privacy Order with a broader definition of "sensitive" information, including web browsing, app usage histories, and other consumer information which could be mined to reveal further details, including demographic data, financial status, political viewpoints, and more. The Order required that ISPs have their customers' permission before collecting personal information, and also heightened protections against harmful "pay-for-privacy" arrangements that force consumers to forfeit their privacy or pay premiums for more privacy-protective service that many wouldn't be

able to afford. Unfortunately, Congress repealed the Broadband Privacy Order less than a year later, leaving only the original CPNI regulations in effect.

Since the repeal, the FCC has rarely taken enforcement actions against ISPs. In 2020, after sustained political pressure and attention from Congress, the FCC proposed over $200 million in fines against AT&T, T-Mobile, Sprint, and Verizon for selling access to their customers' location information without protecting against unauthorized access to that information by law enforcement and bounty hunters. The action was an anomaly, however, and reiterates the need for rules that would inhibit ISPs from selling any personal information without users' consent in the first place.

New kinds of networks require revisiting current approaches to internet regulation to protect consumers. Internet regulation currently focuses on centralized points of control, such as traditional ISPs. For instance, if an internet service provider collects information on users' sleep habits through metadata on their network, and uses that information for targeted advertising or discriminatory pricing on sleep aids knowing users' preferences, the invasion of consumer privacy lies with the ISP.

Finding the one to blame for an invasion of privacy is much more difficult with a wireless mesh network, as the action might be committed by a number of different machines and nodes, making it technically and legally difficult to point out who is liable for violating rights to privacy. For instance, the network in San Rafael uses 20 different antennas attached to different buildings with different ownership throughout the city, and is run by a group of different city and county departments, as well as companies.

One regulatory solution that could work—in the case of community mesh networks, at least—might be for policymakers to codify the informal norms already present in the network; for example, by requesting that each mesh network or wireless community network adopt a code of conduct. Mesh network and wireless community network users already rely on manifestos, informal norms, and general principles agreed upon by those connected and in the community to guide their behavior and actions on the networks. Upon entering and getting connected, people adopt the rules of the network and its underlying principles and ideas, and could technically be excluded from the network should they violate the rules. Of course, should someone collect personal information and invade others' privacy using the network, its decentralized structure makes it hard to find fault with one user or even the network itself. This is especially true if those networks adopt terms and conditions shielding them from liability, just as ISPs do now. However, in the case of community-driven networks built to prioritize connecting the community over profit might mean that an internal regulatory system would adequately address any issues with bad faith users.

The current legal framework for protecting consumer privacy by "notice and consent" mechanisms must change. Notice and consent, or notice and choice, only requires that private entities notify individuals and ask for their permission before collecting and utilizing their personal data. In the case of ISPs, providers don't even have to do this if the information has been 'anonymized,' even though much research shows that anonymized data can very easily be re-identified to a single person. This framework is also unhelpful in light of technological developments towards decentralized networks that make it difficult to point out which entity is specifically responsible for a violation.

Legislation Should Be Rights-Based to Safeguard Personal Information Even With Changes in Technology

Protecting privacy online—whether from the actions and behaviors of broadband providers, or specific platforms and websites—requires comprehensive privacy legislation that consistently empowers individuals with explicit user rights over their data, and provides strict limits on how private entities handle that data. A rights-based approach to privacy enables people to exercise autonomy over their personal data, specifying what actions an individual can take to control how others collect or use it. Notice policies and terms of service agreements only serve to inform individuals of what will happen to their data. Granting rights to users empowers them to limit access to their personal information and control how it may be used.

A rights-based approach also empowers users regardless of what kind of network they use. Even if the network is decentralized, a rights-based approach creates specific guidelines about what can and cannot be done with personal information so that user privacy is better protected by default.

Distinct guidelines and restrictions for companies and organizations around the collection, use and sale of data also places the burden on all those involved in building a network to adopt better privacy-enhancing practices. These restrictions would fundamentally reset the starting point for what data practices are allowed, recognizing that those collecting and processing data are better poised than end users to see how these tools and practices can be harmful.

Mesh networks vary widely, including in their underlying technology, who builds them, and in their payment schemes (or lack thereof). Given such wide differences from traditional models of internet service delivery, privacy rules specific to internet service providers or even "broadband" might be insufficient to protect people on mesh networks. Enacting comprehensive privacy legislation that would protect consumer privacy from all kinds of entities—whether they be platforms, data brokers, or ISPs—is therefore preferable. Legislation with guidelines and user rights to data that apply across all kinds of technology would also be future-proof—applicable to changes and iterations in technology.

Regulatory Tools Beyond Comprehensive Privacy Legislation Can Protect People Online

Aside from comprehensive federal privacy legislation, there are some specific legislative changes that could help strengthen one's privacy from broadband companies. At the state level, OTI has published model state legislation that would protect consumers and their information—including name, address, financial data, Social Security and driver's license numbers, demographic information, geolocation, and other information that could be traced back to a specific consumer or device—from ISPs. In 2020, a federal district court upheld Maine's broadband privacy law modeled after OTI's model legislation—a victory for consumer privacy that may encourage other states to pass similar legislation protecting broadband consumers.

At the federal level, reclassifying broadband under Title II of the Telecommunications Act would give the federal government, through the FCC, greater authority over internet service providers and help the FCC enforce broadband privacy. Section 222 of the Act gives the FCC authority to create new broadband privacy rules in the future, to release guidelines and best practices for providers on protecting consumer data, and empowers consumers to file complaints before the FCC about their broadband service provider's control over their data in violation of Section 222. Provisions of Section 222 also expand its requirement of carriers to protect "proprietary information," extending it more broadly to "private information that customers have an interest in protecting from public exposure."

Whether Title II regulation applies to mesh networks is up for discussion, and depends on whether mesh networks can be defined and classified as telecommunications carriers. The FCC defines telecommunications as "the transmission, between or among points specified by the user, of information of the user's choosing without change in the form or content of the information as sent and received." A telecommunications carrier is a provider of telecommunications service, or the offering of telecommunications at a fee. A mesh network does allow for information of the user's choosing to be sent and received—an AirTag, for example, sends a Bluetooth signal that is then received by nearby devices in the Find My network, which then sends the location of an AirTag back to the original user. This service is additionally available for a fee, with a user paying for an AirTag and paying to have other devices that are on the Find My network. Some mesh networks, however, offer this service of data transmission on their networks without a fee, thereby missing one of the components of the definition of a telecommunications carrier.

The 2015 Open Internet Order, which classified broadband providers as telecommunications carriers, additionally defined broadband as "a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any

capabilities that are incidental to and enable the operation of communications service, but excluding dial-up internet access." Amazon's Sidewalk network would qualify as a telecommunications carrier under this definition, given that it is a mass-market retail service offered along with its retail products that allow its products to communicate with each other. A smaller community network like NYC Mesh, however, is not mass-market nor explicitly for retail purposes, and would therefore require additional consideration were the 2015 Open Internet Order to be reinstated.

We Need to Ensure That People's Privacy Is Protected as Soon as They're Connected Online, Including From Their Own Internet Service Providers

Consumers today can enforce very few of their rights to privacy, making it even more difficult to identify and hold liable those who invade their privacy. Internet service providers can collect data on an individual's actions and behavior all over the internet, and connect that information to their subscribers' real names, addresses, phone numbers, financial information, and more.

Absent comprehensive privacy legislation that protects consumers, ISPs and other companies will continue to monetize aggressive data collection. They may even try to charge people extra to keep their information private, leaving those who can't afford to pay more vulnerable than before. In 2013, AT&T introduced Internet Preferences, a program that analyzed their customers' internet browsing habits for targeted advertising for savings on service rates. People could either opt into this program to help AT&T serve targeted ads based on the data collected and get the lowest available rate on their internet service, or were expected to pay for their privacy with an additional $29 to $60 a month. While seemingly offering value and more control to consumers over their data, in reality pay-for-privacy schemes only serve to further profits for ISPs, who already collect and monetize virtually all the data they want about their customers. Meanwhile, low-income consumers—who are already disproportionately surveilled—will have no choice but to continue allowing ISPs to use and share their data to tailor advertising and marketing that may further limit their opportunities down the line.

It's high time for comprehensive privacy legislation that will protect people online whenever and however they're connected, whether from their traditional internet service provider, or a new private mesh network.