FACT SHEET

Broadband Privacy: Myth vs. Reality

Myth	Reality
1. Internet Service Providers (ISPs) are selling customers' sensitive personal information, like financial information and Social Security numbers.	It is illegal to sell or share consumers' sensitive personal information. Additionally, ISPs have publicly recommitted to following privacy practices modeled after the FTC's well-tested approach, which governs only privacy for the rest of the internet ecosystem. Those principles specifically prohibit sharing "sensitive" info, such as precise geolocation data, unless customers have submitted an "opt-in" form. Health and children's data also are protected under additional federal laws that remain fully in force. There's also existing privacy law at the FCC (Section 222 of the Communications Act) which remains in effect.
2. When Congress rejected ISP-only rules through the Congressional Review Act, consumers lost privacy protections over their data.	Since the rules never took effect, consumers haven't lost anything. Congress rejected uneven rules that would have created separate and unequal only privacy regimes. This directly goes against consumers' strong belief that there should be one high standard for consumer protections across the entire internet.
3. You can buy someone's Social Security number or web browsing history.	It is illegal for an ISP or anyone else to sell such sensitive information to the public.
4. ISPs know more about your online behavior than other online companies.	Thanks to wide use of encryption technologies, ISPs only know which websites subscribers might be visiting, not the content of those sites. A study last year by a privacy expert who served in the Obama and Clinton administrations found that ISP access to customer data was neither comprehensive nor unique since social networks or ad networks have far more visibility into what consumers are looking at online.

Broadband Privacy: Myth vs. Reality

	Myth	Reality
5.	Consumers can't opt-out of allowing their ISP to share their browsing data for online marketing purposes.	Consistent with the rest of the internet ecosystem, all major ISPs allow subscribers to "opt out" of practices that would allow providers to collect and share their non-sensitive data for marketing purposes.
6.	This rule was adopted by the FCC under the Obama administration because ISPs were inappropriately tracking consumers online.	There were no egregious consumer complaints that prompted the FCC to adopt special ISP-only privacy rules. The FTC has long been the cop on the beat protecting consumers' online privacy, bringing more than 150 privacy and data security enforcement actions against ISPs, online search, content and e-commerce sites. Two years ago, the FCC stripped the FTC of its jurisdiction over broadband providers and began pursuing this bifurcated path. Fortunately, FCC Chairman Ajit Pai and FTC Chair Maureen Ohlhausen have rejected that approach and jointly expressed their support for "a comprehensive and consistent framework."
7.	A recent court decision (FTC v. AT&T Mobility) affirmed the FTC has no ability to enforce online privacy protections on ISPs, so now there is no agency that can protect consumer privacy.	In addition to the many existing privacy protections detailed above, the FTC is appealing this court decision. While the court has said that the FTC couldn't take ISPs to court because they are now "common carriers," the leaders of the FCC and FTC have promised to work together on ensuring any new FCC broadband privacy rules work hand-in-hand with how the FTC enforces the law—so consumers have consistent and strong privacy protections across all of their online experiences.

USTELECOM
THE BROADBAND ASSOCIATION