FREE STATE FSF FOUNDATION

Perspectives from FSF Scholars
January 29, 2025
Vol. 20, No. 7

Stopping the Theft and Destruction of Broadband

by

Michael O'Rielly *

I. Introduction

By and large, America's broadband providers, in cooperation and coordination with various government agencies, do a great job preparing and responding to constant external threats. The reality is that there is no shortage of individuals, rogue groups, nation states, and others seeking to cause harm to Internet users, broadband networks, and in some cases, the collective critical communications infrastructure. Yet, when harmful activity that is just as significant and problematic but involves intentional theft or damage of communications facilities, weak or ineffective federal and state laws let perpetrators escape justice.

Irrespective of motive, bad actors are seeking to damage networks for profit or malicious purposes, which is creating havoc on critical communications infrastructure. Such activities leave consumers without important service connectivity, expose providers to liability from residual hazards at theft sites, and create extensive and expensive work for companies to reconnect cutoff consumers and protect their networks. This needs to change as broadband vandals should face significant criminal penalties for the harm being caused, especially to American consumers. To effectuate this, clear laws – at both the federal and state levels – that

cover all modern critical infrastructure/facilities with increased penalties must be in place. Correspondingly, strong enforcement efforts need to be made more of a priority.

A recent report (*Joint Industry Report*) prepared and sponsored by the nation's major communications trade associations – namely, NCTA, CTIA, USTelecom, and NTCA – exposes the expansive theft and vandalism to broadband infrastructure, the impact of these attacks, and potential ways to combat the problem.[1] In addition, the industry representatives held a summit in November that examined the scope of the issue and the importance of taking quick action. Considering how infrequently these trade associations land on an identical policy page, it should signify the gravity of the situation.

II. A Growing Problem

Nearly every month, a news story highlights communications infrastructure being stolen for the resale value of the underlying materials or to inflict network shutdowns. Here are just a few instances:

- KTTC Rochester MN, "UPDATE: Spectrum Service Restored, RPD Investigating Vandalism," January 2025
- WHTM Harrisburg, "Residents in Parts of Central Pennsylvania Were Left Without Internet After Thieves Vandalize Tower," December 2024
- KOMO Seattle News, "Copper Wire Thieves Knock Out Phone and Internet Services for Hundreds of Customers," July 2024
- Spectrum News 1, "AT&T Offers $10K Reward for Information on DFW Copper Cable Thefts," October 2024
- Jefferson County Leader, "Festus Man Arrested for Alleged Fiber Cable Theft," October 2024
- The Advocate, "People in a Louisiana town lost internet. Then police caught somebody stealing the cables," September 2024
- Fox 26 Houston, "Polk County Crime: Authorities Investigating Incidents of Above Ground Fiber Optic Lines Being Cut," January 2024
- The New York Times, "Metal Thieves are Stripping America's Cities," July 2024

Some thieves seem interested particularly in copper lines because the metal currently is desirable and lucrative on the black market, with prices increasing more than 60% over the last four years.[2] Future copper prices are expected to increase even further as noted in a recent Financial Times piece citing industry sources, "Global demand is expected to rise by 70 per cent from 2021 levels by 2050."[3]

But many thieves are so technologically illiterate that they often cut fiber optic cables and attack cell sites with the misguided belief of immense copper hauls. In fact, the demand for copper has forced fiber installers to "educate" would-be criminals about the absence of any copper.[4]

Additional awareness and educational outreach could also benefit the recycling industry. The *Joint Industry Report* suggests that any comprehensive solution must also address the demand side of copper transactions. On point, scrap metal dealers may need to be held accountable for their part in perpetuating the market for stolen copper. Thieves may think twice if there was nowhere to sell their ill-gotten gains. Accordingly, it would be valuable for policymakers to examine existing laws to ensure there is an effective process for policing the sale and purchase of scrap metal that is vigorously enforced with appropriate penalties.

Consider the data points contained in the *Joint Industry Report*: during just a three month period in 2024, an industry survey found that there were 3,929 theft and vandalism incidents that affected over 325,000 citizens.[5] Extrapolating this data would generate over 16,000 incidents and 1 million broadband subscribers being impacted yearly by such criminal practices for just the sampled companies. In reality, these numbers would be increased by several factors if all affected and impacted companies were included.

III. Significant and Demonstrable Harm

Whatever the underlying reason, theft and impairment of copper and fiber broadband lines are causing massive harm to consumers and businesses. The act of cutting a broadband line disrupts service for residential and business locations, thereby blocking the use of this critical technology. That means consumers lose the ability to reach loved ones, communicate with emergency personnel in times of crisis, work remotely, enhance educational opportunities, and so much more. Connected businesses lose customers and work productivity. Indeed, the underpinning of the energy grid, financial systems, and transportation networks is threatened when communication lines go down. For providers, the cost for replacement lines and lost revenue can be substantial, but each theft requires staff time and truck rolls that could be used to expand or upgrade the network elsewhere. Whether it is bringing broadband to unserved areas or upgrading existing customers, broadband thefts delay deployment timelines and sidetrack network management.

Significantly, for areas where broadband is being deployed to the unserved for the first time with government subsidies, federal broadband programs and recipients face a double whammy. Not only do such thefts and needless attacks cause the projects subsidized by approximately $100 billion in U.S. government broadband funding[6] — via ARPA, BEAD and other programs[7] — to be more expensive, but can result in long delays for consumers who may be prevented from being reached and connected. Specifically, the costs and effectiveness of federal broadband funds are put at greater risk when thieves steal or destroy broadband. Imagine just one consequence: consumers without access were led to believe that they would receive broadband within some time frame, only to be later told that all broadband builds will be delayed by months or years because the needed broadband was subsequently stolen or now uneconomical. In other instances, broadband at some newly connected households is in jeopardy for being ripped out by criminals, leaving providers in these economically challenged areas with even higher connection costs.

Likewise, broadband networks are rightfully treated as part of America's critical infrastructure. Given that almost every aspect of daily life is connected in some way via broadband and fiber

optics, the theft of components in multiple areas can weaken an overall network or the entire system. And theft or intentional damage in critical areas can hamper or cripple networks, providing an exposure map for terrorists and those intending to harm the United States. Unfortunately, theft of or damage to broadband network components is not presently treated in federal law in the same manner as damage to other critical infrastructure, like energy, railroads, or mass transit.

IV. A Solution

One way to elevate and hopefully alleviate this situation is to impose enhanced criminal penalties on those damaging or stealing broadband lines. For instance, existing federal law (18 U.S.C. 1862) already provides discretionary fines up to $250,000 or ten years in prison for willfully or maliciously injuring or destroying communications facilities operated or controlled by the U.S. or used or intended to be used for military or civil defense functions. But this provision doesn't specifically mention privately-owned communications facilities, like broadband lines. Because of that, there is currently no recourse under federal law for this rising network vandalism.

A logical and appropriate fix would be to enact a targeted expansion of this provision to cover the injuring or destroying of private broadband networks. Or to enact a separate but similar provision covering communications networks as exists for pipelines and other critical infrastructure. Who would oppose that and what would be their justification?

Similarly, it would be incredibly appropriate for individual states, especially those with varied and meager penalties, to enact stronger enforcement actions and properly classify critical communications network infrastructure that is inclusive of all broadband network facilities. A few states – Florida, South Carolina, and North Carolina – currently have been held out as potential models given their comprehensive approaches and strong interest in preventing harm to their communities, citizens, and overall safety. And at the same time, it would be helpful for federal and state law enforcement, including U.S. attorneys and state prosecutors, to devote more time, attention, and prosecutorial resources to this issue.

V. Conclusion

Certain criminal elements in America see the physical broadband infrastructure as an easy and painless way to fast cash. Without governmental action, the pain inflicted by these bad actors and crooks will increase and spread to more markets. Given the preeminent role that broadband plays in American society, however, policymakers should counter this by immediately enacting and imposing stronger penalties on such lawbreakers.

* Michael O'Rielly, a former FCC Commissioner, is an Adjunct Senior Fellow at the Free State Foundation, an independent, nonpartisan free market-oriented think tank located in Rockville, Maryland. He is the host of the "TMT with Mike O'Rielly" podcast. The views expressed in this *Perspectives* do not necessarily reflect the views of others on the staff of the Free State Foundation or those affiliated with it.

[1] "Protecting The Nation's Critical Communications Infrastructure from Theft & Vandalism," 2024.
[2] Jerico Casper, Broadband Breakfast, "Telecom Industry Summit Puts Focus on Harms from Copper Theft," November 19, 2024.
[3] Yasemin Craggs Mersinoglu, Financial Times, "Telecoms Groups Forecast to Reap $10bn Windfall from Recycled Copper," January 1, 2025.
[4] See Reddit: https://www.reddit.com/r/mildlyinteresting/comments/br3dd7/giant_spool_of_fiber_optic_cable_had_to_display/
[5] Joint Industry Report, pg. 8.
[6]Nokia, "U.S. Broadband Funding Explained."
[7] ARPA is an acronym for the American Rescue Plan Act of 2021; BEAD is an acronym for Broadband Equity Access and Deployment program.