



Perspectives from FSF Scholars
October 26, 2026
Vol. 21, No. 44

**Combating Malicious Attacks on Communications Infrastructure:
Lessons From Maryland's New Law**

by

Kathy Sanchez *

I. Introduction and Summary

On October 7, 2026, U.S. Senators from California and Missouri announced bipartisan legislation to combat theft and vandalism against communications infrastructure.¹ The Combating Critical Infrastructure Vandalism Act, HB 1100, is part of broader efforts across the nation to address malicious attacks on communications networks. At the federal level, existing law criminalizes damage to communications infrastructure operated or controlled by the federal government without addressing attacks more broadly against privately owned infrastructure.²

¹ S.5617 was introduced September 30, 2026 by Sens. Eric Schmitt (R-MO) and Alex Padilla (D-CA): U.S. Senate, "S. 5617 – Combating Critical Infrastructure Vandalism Act of 2026: All Actions," 119th Congress, September 30, 2026, <https://www.congress.gov/bill/119th-congress/senate-bill/5617/all-actions?s=1&r=1&hl=S.+5617>; The Senators announced the legislation on October 7, 2026 in a press release: U.S. Senator Eric Schmitt, "Senator Schmitt Leads Bipartisan Effort to Protect Broadband Infrastructure From Theft and Vandalism," Press Release, <https://www.schmitt.senate.gov/media/press-releases/senator-schmitt-leads-bipartisan-effort-to-protect-broadband-infrastructure-from-theft-and-vandalism/>.

² 18 U.S.C. § 1362, <https://www.govinfo.gov/content/pkg/USCODE-2024-title18/html/USCODE-2024-title18-partI-chap65-sec1362.htm>.

States are also responding to attacks on wireless and broadband infrastructure. Many legislative efforts focus on increasing criminal penalties in response to the substantial social and private costs of service disruptions, which can far exceed the value of stolen or damaged materials. In October 2026 Maryland's new law took effect, making it part of a growing number of states addressing these crimes.³

Ultimately, a multi-pronged approach is essential to deterring crime and holding offenders accountable. Swift investigation, arrest, and prosecution, combined with cooperation between law enforcement and proactive communications service providers, offers a more promising path to deterring infrastructure attacks than simply enacting lengthy maximum prison sentences and burdensome business regulations.

Rather than simply enacting harsh criminal penalties alone or heavy-handed, costly requirements on businesses, policymakers should also prioritize the investigation and prosecution of infrastructure crimes and cooperation with service providers. New laws should be tailored to reduce crime without imposing unnecessary costs on taxpayers or businesses. These are factors that other statehouses considering similar laws and Congress should weigh carefully.

II. Maryland's New Law

HB 1100 has two parts: a new criminal offense for damaging telecommunications infrastructure and new language regarding purchases of scrap metal.

The law creates a misdemeanor offense for "recklessly or willfully and maliciously defac[ing], damag[ing], or destroy[ing] telecommunications infrastructure," punishable by up to six months in prison and a \$500 fine. It does so by expanding Maryland's existing criminal statute protecting gas, water, and electrical infrastructure to cover telecommunications infrastructure and equipment.

Previously, offenders could be charged with theft, vandalism, breaking and entering, and other applicable crimes, as well as be ordered to pay restitution, all depending on the facts of the case. Detailed examples:

- Misdemeanor theft valued between \$100 and less than \$1,500 carries a maximum penalty of six months' imprisonment and a fine up to \$500.⁴
- Misdemeanor vandalism damages valued less than \$1,000 carries a maximum penalty of 60 days' imprisonment and a fine up to \$500.⁵

³ 2026 House Bill 1100, https://mgaleg.maryland.gov/2026RS/Chapters_noln/CH_546_hb1100e.pdf.

⁴ Maryland Criminal Law §7-104(g)(2), <https://mgaleg.maryland.gov/mgawebsite/laws/StatuteText?article=gcr§ion=7-104>.

⁵ Maryland Criminal Law §6-301(c), <https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gcr§ion=6-301>.

Now, the new offense may be charged and prosecuted alongside other applicable crimes, depending on the facts of the case. In a simple example, an offender convicted of both misdemeanor theft and telecommunications infrastructure damage could face up to six months in prison and \$500 in fines for each offense. If the court orders the sentences to run consecutively, that offender could now face one year in prison, \$1,000 in fines, and be ordered to pay restitution.

The law also amends the state's business code to clarify requirements on businesses that purchase scrap metal. The goal is to make it harder for thieves to sell stolen infrastructure materials through legitimate recycling businesses.

III. The Costs of Infrastructure Attacks Extend Far Beyond Repairs

Maryland's law and proposals like it are focused on addressing a serious threat to communities and service providers. Media attention often focuses on copper theft and the resale of stolen copper because of its prevalence, but perpetrators damage and steal all kinds of communications infrastructure. In the process, they cause service outages and force companies to spend money on repairs rather than on improving service for customers. Thieves may cut fiber-optic lines and other equipment while trying to reach the materials they want. Other commonly stolen items include batteries, fuel, and electronics.⁶

The consequences are substantial. According to a study commissioned by the nation's leading communications trade associations, infrastructure-related outages between June and December 2024 conservatively totaled at least \$38 million in costs on society – many times the actual value of the stolen and damaged materials.⁷ CTIA – The Wireless Association – reported nearly 16,000 theft and vandalism incidents nationwide over a one-year period between 2024 and 2025.⁸ In Maryland, state police reported about 51 cases of Verizon telephone wire incidents in 2025 in Cecil County alone, a state hotspot for these crimes.⁹

Damaged networks can disconnect people when they need reliable communications most, preventing them from accessing Internet or phone services for work, reaching family members, or calling 911 in an emergency. Outages also force providers to divert resources from improving service quality, limiting their ability to reduce costs and improve services for customers.

⁶ Jeff Baumgartner, "Network Theft Is Up, and So Are Arrests," *Light Reading*, October 6, 2026, <https://www.lightreading.com/broadband/network-theft-is-up-and-so-are-arrests>.

⁷ Edward J. Lopez, "The Real Costs of Communications Outages Due to Infrastructure Theft or Vandalism," October 2025, https://www.ncta.com/wp-content/uploads/2025/10/Economic-Impact-Study_1001_2025.pdf.

⁸ Jeremy Crandall, written testimony submitted to the House Economic Matters Committee, Maryland General Assembly, March 2, 2026, https://mgaleg.maryland.gov/cmte_testimony/2026/ecm/1ZpXjf3VR6qeYjsqET1BZmMmQVIb_CXw8.pdf.

⁹ Mallory Sofastaii, "Copper Thieves Keep Knocking Cecil County Residents Offline," *WMAR-2 News*, September 8, 2026, <https://www.wmar2news.com/matterformallory/copper-thieves-keep-knocking-cecil-county-residents-offline>.

IV. Service Providers Are Already Doing Their Part to Combat Malicious Destruction

Beyond making constant repairs, service providers are taking proactive steps to combat these crimes. These measures include actively monitoring cables with trackers, bolting manhole covers, surveillance, and using security personnel, according to Alisha Remek of AT&T, in a July 2026 *TMT With Mike O’Rielly* episode.¹⁰

Providers are also investing in technology innovation to address the persistent attacks, as Jonathan Spalter of USTelecom explained in the same *TMT* episode.¹¹ For example, some providers are using AI frontier models to geolocate attacks and respond in real time. Furthermore, providers are working to more quickly retire networks that demand much of the industry’s copper in the first place.

Still yet, Ms. Remek reported that AT&T’s successful deterrence efforts involve close partnerships with local police, sheriff’s departments, and district attorneys.¹² These partnerships allow service providers to share information about emerging crime patterns and theft hotspots. Metal theft task forces are among the most helpful partnerships.

V. Will the New Criminal Penalty Work?

Whether a new law will be effective depends on the intended goals. Criminal law generally serves several goals, including deterrence, incapacitation, and retribution. Of these, deterrence is the most promising in the case of Maryland’s new offense. A distinct criminal offense may discourage some would-be offenders, while a relatively short maximum sentence offers a way to hold offenders accountable without risking diminishing returns to public safety and substantial taxpayer costs associated with lengthy incarceration. Considering all three goals provides a framework for assessing how effectively the new offense might address the infrastructure attacks.

Deterrence: Enforcement Matters Most

Laws targeting infrastructure attacks could discourage, or deter, would-be offenders by signaling that the state takes communications infrastructure damage seriously and intends to prosecute it. The key question is whether the new law actually changes people’s perceptions of the likelihood and consequences of getting caught. If the creation of a new offense alone does help deter crime, states could realize some of the benefits of criminal enforcement without incurring substantial fiscal and social costs associated with lengthy prison sentences.

¹⁰ Free State Foundation, “TMT with Mike O’Rielly - Episode 42: Protecting Critical Infrastructure From Attacks,” posted July 24, 2026, YouTube, <https://youtu.be/139zDlIMsog?t=337>.

¹¹ Free State Foundation, “TMT with Mike O’Rielly - Episode 42: Protecting Critical Infrastructure From Attacks,” posted July 24, 2026, YouTube, <https://youtu.be/139zDlIMsog?t=817>.

¹² Free State Foundation, “TMT with Mike O’Rielly - Episode 42: Protecting Critical Infrastructure From Attacks,” <https://youtu.be/139zDlIMsog?t=402>.

Research generally shows that the likelihood of being caught and punished often matters more than the severity of the punishment alone. Increasing prison sentences often have diminishing returns to public safety. Long sentences do not necessarily translate into less future crime. This does not mean that increasing sentences is always unproductive in deterring crime. Rather, it means that simply increasing maximum penalties is unlikely to be an effective stand-alone strategy.

Maryland may be taking a more measured and efficient approach than other states by authorizing a relatively short maximum sentence of six months (and \$500 fine). Missouri and Oklahoma, for example, allow prison sentences of up to 10 years for similar offenses related to communications infrastructure damage.¹³ Creating distinct offenses that carry shorter sentences may be able to deter some infrastructure attacks without the greater fiscal and social costs associated with longer prison terms.

Incapacitation: The Benefits Depend on Who Is Committing the Attacks

The law's incapacitation benefits will depend on how many infrastructure attacks are committed by repeat offenders who would otherwise continue to pose a threat. Incapacitation prevents offenders from committing crimes in the community while they are incarcerated. A sentence imposed under Maryland's new offense could temporarily prevent an incarcerated offender from committing additional infrastructure crimes. But we do not know how many of these criminals in Maryland are habitual offenders and in organized criminal networks versus how many are more opportunistic.

Media outlets and service providers have indeed described organized crime as a significant contributor to the infrastructure attacks. For example, reporting by WTOP covered arrests in 2025 in an alleged copper wire theft ring operating in Virginia.¹⁴ And AT&T reported sophisticated operations, including using heavy machinery and coordinating multiple attacks at the same time, in California.¹⁵ Without readily available evidence establishing the extent of organized attacks in Maryland, the precise benefits of incapacitation via Maryland's new law are unknown.

Retribution Should Not Drive Policy

Retribution provides a way to address crimes where the existing available penalties appear inadequate compared to the damage caused. Although retribution is a common aspect of debates about crime and public safety, it should remain secondary to achieving the practical

¹³ Laura Barczewski, "Missouri Targets Copper Infrastructure Thieves With Harsher Penalties Amid Rising Theft Rates," *KSDK*, July 21, 2026, <https://www.ksdk.com/article/news/local/missouri-targets-copper-infrastructure-thieves-with-harsher-penalties-amid-rising-theft-rates/63-8a7fb75a-3da5-41a4-bf26-92012c294263> <https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=481112>.

¹⁴ Alan Etter, "3 Maryland Men Charged With Stealing Millions in Copper Materials Linked to Organized Crime, Deputies Say," *WTOP News*, December 30, 2025, <https://wtop.com/virginia/2025/12/three-men-charged-with-stealing-millions-in-copper-materials-linked-to-organized-crime-according-to-police/>.

¹⁵ Rahdeese Alcutt, "Copper Theft – What We're Missing," *AT&T Blog*, April 3, 2026, <https://about.att.com/blogs/2026/copper-theft.html>.

goals: deterring crime and incapacitating repeat offenders. Punishment may indeed provide a sense of justice for the communities and service providers affected by repeated attacks. However, retribution relies on subjective judgments about the moral seriousness of a crime. Therefore, to achieve the key public policy goal of protecting key communications infrastructure, lawmakers should prioritize preventing attacks and network disruptions rather than treating punishment as an end in itself.

VI. Any Business Requirements Should Be Narrowly Tailored

Maryland's new law imposes little burden on businesses. The new language clarifies documentation requirements for state-registered scrap metal dealers purchasing telecommunications equipment.¹⁶ Scrap metal dealers were already prohibited from purchasing materials unless sellers provided evidence of their legal authority to sell them. The new law specifies that, for telecommunications equipment, acceptable documentation may include a bill of sale, receipt, letter of authorization, or other evidence of lawful ownership or authority to sell. By expressly recognizing these forms of documentation, the law may reduce ambiguity and ease compliance for legitimate businesses. Because the law largely clarifies existing requirements, its effects on infrastructure damage will likely be limited. Existing requirements to document and report scrap metal purchases also remain in effect, with fines of up to \$500 for a first offense.

Fortunately, several burdensome proposals did not make it into the final law: a mandatory 30-day holding period for purchased materials; a requirement to pay for materials by check only; and a reporting requirement for telecommunications equipment that would have duplicated the existing requirements for scrap metal purchases more broadly. Although such measures were intended to make it harder for thieves to profit from stolen materials, they also would have imposed additional costs and inconvenience on legitimate businesses. Lawmakers should avoid imposing unnecessary compliance burdens on recycling businesses unless the requirements are narrowly tailored and likely to meaningfully reduce infrastructure theft and damage.

VII. Conclusion

There is no single solution to communications infrastructure theft and vandalism. The most promising response combines swift investigation, arrest, and prosecution; proactive steps by service providers; and consistent cooperation between law enforcement and service providers. To their credit, major broadband providers are already pursuing this approach. But providers cannot, nor should they, be expected to solve infrastructure attacks alone.

For lawmakers, this means understanding that enacting new offenses or authorizing longer sentences alone will not resolve the problem. A new offense could strengthen deterrence by giving prosecutors a more direct way to hold offenders accountable for damaging communications infrastructure. This is an important step. But its ultimate success depends on

¹⁶ Maryland Business Regulation §17-1009, <https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gbr§ion=17-1009&enactments=False&archived=False>.

deterrence via enforcement: law enforcement must investigate incidents, identify offenders, and pursue charges to demonstrate that infrastructure attacks carry real consequences. Without that follow-through, new laws may do little to change offenders' behavior.

Rather than relying on harsher penalties or the creation of burdensome new business regulations, policymakers should prioritize enforcement and cooperation with service providers. This approach offers a more promising path to reducing infrastructure attacks while, at the same time, mitigating unnecessary costs to taxpayers and legitimate businesses.

* Kathy Sanchez is a Research and Communications Specialist at the Free State Foundation, a free market-oriented think tank in Potomac, MD. 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.

Further Readings

Andrew Long, "[California Reward Programs Underscore Gravity of Copper Theft](#)," *FSF Blog* (August 14, 2026).

Michael O’Rielly, “[National Broadband Theft and Vandalism: A Sample of Destructive Acts Since January](#),” *Perspectives from FSF Scholars*, Vol.20, No. 25 (June 4, 2025).

Michael O’Rielly, “[Stopping the Theft and Destruction of Broadband](#),” *Perspectives from FSF Scholars*, Vol.20, No. 7 (January 29, 2025).