**"Responding to a Growing Threat: Defending Communications Infrastructure from Attack"**

***Copper Theft Crisis: Incident Management and Prosecutorial Collaboration Summit***

**El Segundo, CA (Via Video from Washington, DC)**

**FCC Commissioner Olivia Britt Trusty**

**October 7, 2025**

Good morning.

Thank you for inviting me to join this summit on infrastructure vandalism.

It is urgent.

It is necessary.

And it could not be more timely.

When I think about threats to our communications networks, my mind often jumps to sophisticated cyberattacks or foreign adversaries.

But increasingly, the danger is something far less high-tech and far more blunt: vandalism.

These are deliberate acts of destruction that cut off communities, put lives at risk, and cost millions of dollars to repair.

When a hospital can't connect to its patient records, when 911 callers hear nothing but silence, when an entire small town loses connectivity because someone saw dollar signs in copper wire, that is not a prank. That is not mischief. That is a direct attack on the lifeblood of our economy and our daily life.

Today, I want to sound the alarm. Because this is not a handful of isolated incidents. It is a growing epidemic, and it is hitting every part of the country.

**The Scope of the Problem**

The data alone should give us pause. Between May and December of 2024, there were at least 5,770 reported incidents of theft and vandalism against communications networks, disrupting internet service for more than 1.5 million Americans and causing millions of dollars in damage. (Industry Vandalism Report)

But statistics only tell part of the story. Let me give you real life examples of what this looks like on the ground.

**Case Studies – Real Consequences**

In Washington state, vandals ripped out copper cables, severing fiber in the process and leaving thousands of people without 911 access. For hours, callers dialing for help got nothing but silence (King5 News).

In Tacoma and Pierce County – also in Washington State – Comcast confirmed that vandalism to its network disrupted service for thousands of homes and businesses (Comcast Washington). Crews had to work overnight to replace the damaged lines, diverting resources away from expansion and upgrades.

In Wyoming, suspected vandals severed fiber-optic cables, causing a county-wide 911 outage and tens of thousands of dollars in damage (Oil City News).

In Colorado, a radio repeater tower used by firefighters was deliberately sabotaged, antennas broken, and guy wires cut, impairing emergency communications as crews battled a wildfire (KDVR).

And in the past year, we've seen AT&T and Charter face escalating assaults on their networks:

- In one particularly wrenching case in South Los Angeles, a 92 year old woman lost her landline, and, with it, her crucial lifeline, for months after copper thieves stole the wiring. Her family relied on caregiver calls just to check in on her, while her life-alert system and home cameras were down. Eventually, a combined LAPD and city taskforce made 82 arrests and recovered over 2,000 pounds of copper. (Los Angeles Times)
- In Van Nuys, California, vandals severed 13 fiber cables in June of this year, cutting through more than 2,600 individual strands and leaving over 50,000 residential customers and 500 businesses offline for as long as 30 hours. The outage disrupted 911 dispatch, hospitals, schools, a military base, financial institutions, courts, and even cell towers. Charter's Spectrum service called it nothing less than "domestic terrorism." (Charter Communications, TVTechnology).
- In Missouri, Spectrum has reported a 200% surge in felony-level attacks on its network in 2025, cutting off critical services and prompting the company to offer a $25,000 reward for leads. (Charter Communications)
- In central Indiana, AT&T offered a $5,000 reward after repeated copper thefts and vandalism knocked out service in multiple counties (WTHR).
- In Houston, thieves brazenly climbed towers to steal copper cabling, knocking out internet service for neighborhoods and prompting AT&T to warn that these were not petty thefts but public safety hazards (Click2Houston).

- And in Gwinnett County, Georgia, thieves stole nearly 4,000 feet of cable — the length of thirteen football fields, leaving families and businesses offline for nearly a full day (Atlanta News First).

These are not minor disruptions. They are major attacks on public safety, economic security, and national resilience.

**Why It Matters**

The damage from vandalism cascades outward in ways most people don't immediately see. When a fiber line is cut in search of copper, it doesn't just affect the neighborhood where the theft occurred. It can sever emergency communications across an entire county. It can shut down cellular coverage for thousands of people. It can delay financial transactions, medical appointments, and school lessons.

And it slows down our Build America agenda. Every time a fiber line is stolen or sabotaged, crews are pulled away from critical broadband expansion to make repairs. Every time copper thieves take down a tower, money earmarked for connecting unserved communities is instead spent patching holes.

This is why I say: vandalism is not just a property crime. It is an attack on the very effort to connect every American and close the digital divide.

**Beyond the Headlines**

Some might ask: is this really so different from other kinds of theft? After all, people have stolen copper for years.

But here's the difference: communications infrastructure is not just metal and wires. It is critical infrastructure, on par with our power grid, our water systems, and our transportation networks.

When copper is stolen from an abandoned building, it's scrap. When copper is ripped out of a live fiber line, it's sabotage and an attack because it puts lives at risk. It silences 911 calls, it disconnects hospitals, and it delays first responders from their life-saving work.

The Department of Homeland Security has already recognized communications systems as one of the nation's 16 critical infrastructure sectors. Yet, as these attacks multiply, our laws and penalties have not kept pace.

**The Legal Gap**

Today, there is a dangerous gap in federal law.

Existing statutes make it a federal crime to attack communications facilities that are owned or operated by the government. But the vast majority of America's networks are privately owned, and when those facilities are vandalized, accountability is often left to a patchwork of state laws.

That means the very networks that carry trillions of dollars in economic activity and some of our most sensitive communications are not explicitly protected under federal law.

I believe this must change. That is why I support efforts in Congress to amend the U.S. Code so that willful attacks against privately owned communications networks are treated as serious federal crimes, with penalties to match their severity.

This is not about partisan politics. This is about public safety, economic and national security, and basic reliability.

**Industry's Role**

But government cannot solve this problem alone. Industry has a responsibility too.

- **Harden the target:** Providers must invest in better physical security for fiber lines, substations, and towers. This means more cameras, tamper-proof housings, and alarms that trigger the moment infrastructure is cut.
- **Share data quickly:** Providers must share information with other providers quickly. When a line is cut in California, Indiana or Missouri, other providers should know right away, so they can monitor their networks for patterns and coordinate with law enforcement.
- **Support prosecution:** Providers must be ready to work hand-in-hand with prosecutors, offering the evidence needed to secure convictions.

I welcome the work industry is already doing to combat this problem. Charter is offering rewards of $25,000 for information on major attacks (Charter Communications). AT&T is also offering cash rewards for leads in Indiana (WTHR). These are strong steps in the right direction. But we need more.

**Law Enforcement and Partnerships**

Law enforcement has a role to play, too.

When Spectrum's network was slashed in California, 13 fiber cables severed in Van Nuys, it wasn't just a company's problem (Charter Communications). It was a public safety emergency.

We need local, state, and federal law enforcement to treat these incidents with the seriousness they deserve. That means stronger coordination between FBI field offices, state attorneys general, and local police departments. It means prioritizing these crimes in the same way we prioritize attacks on the power grid or water systems.

And it means educating judges and juries that these are not "cable outages." They are threats to life and safety.

**Public Awareness**

Finally, the public has a role.

Too often, when people hear about copper theft or network vandalism, they shrug it off as a nuisance, like graffiti or petty theft. But if more Americans understood that ripping out cable can cut off their own access to 911, disrupt their own children's online classes, or prevent firefighters from receiving dispatches, they might see these crimes in a different light.

That is why public awareness campaigns and consumer education are so important. Providers, industry groups, and government alike should be spreading the message:

Infrastructure vandalism is not a victimless crime. It is an attack on all of us.

The good news is that consumers can take certain steps to protect themselves. Here's how: households and businesses still relying on traditional copper lines should consider transitioning to modern alternatives, whether fiber, wireless, or other service options. These technologies are less vulnerable to copper theft, provide more reliable connectivity, and ensure that critical services like 911 and telehealth remain accessible when they are needed most. Moving away from copper is not just about better service, it's about public safety.

**Closing – A Call to Action**

So where do we go from here?

First, Congress must act. It is time to update federal law so that willful attacks on private communications networks are explicitly criminalized. The law should recognize that private ownership does not make these networks less essential to the public good.

Second, industry has a responsibility to harden defenses. Providers should invest in securing their assets, sharing intelligence with one another, and working closely with law enforcement.

Third, law enforcement officials must prioritize enforcement. It is imperative that prosecutors, police, and federal agencies treat these cases as critical infrastructure crimes, because that is exactly what they are.

And finally, the public must understand the stakes and transition to modern service options where possible. Infrastructure vandalism may look like copper theft or mischief, but in truth, it can mean the difference between life and death.

At the FCC, our Build America agenda is about more than laying fiber or deploying towers. It is about ensuring that every American can trust the networks that carry their voices, their data, and their livelihoods. That goal cannot be achieved if vandals are allowed to compromise our progress with impunity.

The bottom line is simple: if we are serious about connecting America, we must be serious about protecting America's networks.

Together, with government, industry, law enforcement, and the public, we can make sure that America's communications systems are not only the fastest and most widely available in the world, but also the most secure.

Thank you.