COMMITTEE ON
ENERGY & COMMERCE
DEMOCRATS
RANKING MEMBER FRANK PALLONE, JR.
NEWS

**FOR IMMEDIATE RELEASE**
July 11, 2018

**CONTACT**
CJ Young – (202) 225-5735

# Doyle Remarks at Communications Privacy Hearing

**Washington, D.C.** – *Communications and Technology Ranking Member Mike Doyle (D-PA) delivered the following opening remarks today at a Subcommittee on Communications and Technology hearing on "Protecting Customer Proprietary Network Information in the Internet Age:"*

Thank you, Chairman Blackburn, for holding this hearing – and thank you to the witnesses for appearing before us today.

Digital privacy in our modern era has never been more important, and as our society becomes increasingly connected it will become even more important. I believe that we can and must do more to protect American's privacy and sensitive information. This Committee's hearing with Facebook's CEO Mark Zuckerberg showed how concerned our members are with the practices of one of the world's largest tech companies.

What that hearing made clear was that the FTC does not have the manpower or authority to adequately enforce its own consent decree against Facebook, let alone pro-actively police this fast-evolving space. To solve this problem and to give the American people the protections they are demanding, we are going to need a comprehensive solution that includes more resources, more manpower, more authority to go after bad actors, and the ability to set rules of the road for the digital economy. Facebook demonstrated all too well that after-the-fact enforcement authority can't help us when the damage has already been done.

Europe's implementation of its GDPR rules, as well as California's recently and quite quickly passed privacy law, are clear indications that people at home and abroad recognize the need for strong privacy protections. We in Congress and on this Committee need to take that to heart as we address this pressing issue.

Now, with regard to today's hearing and the topic before us, CPNI or Customer Network Proprietary Information: The FCC enforces CPNI rules under Section 222 of the Communications Act. This section restricts how telecommunications carriers can use and share customer data related to their service. This section and the authority it grants the

Commission are some of the strongest privacy laws we have in this country and are intended to give consumers a modicum of protection.

These rules were expanded in 2016 to include broadband services as well. Those rules too were simple, but effective. The three components were: first if your broadband provider wanted to use your data, it had to ask your permission, second it had to take reasonable steps to protect that data, and third it needed to notify you if your data was breached.

These rules were an expansion of the FCC's existing CPNI rules and would have meaningfully enhanced our nation's privacy laws. Chairman Blackburn cosponsored and successfully led the effort to repeal these simple, sensible rules; as of yet there has been no replacement. The majority cannot claim that it values privacy when one of its signature achievements this Congress is the repeal of these meaningful rules.

Americans around the country are shouting for more not less privacy protections; whether it is through ballot initiatives or billboards, people want more control over their digital lives. That is why it's so concerning that the FCC is doing so little to enforce existing protections under Section 222. Thanks to work done by Senator Wyden and his staff, we recently discovered that the real-time location of hundreds of millions of cell phones were being made available by our nation's wireless carriers without consumer's consent.

At least one company, Securus, used their access to this data to create a service for tracking and locating nearly every cell phone in real time. On top of that Securus forced families calling prisons to consent to have their location tracked as a condition for talking on the phone with their incarcerated family member. That seems like no choice at all.

Location Smart, the data aggregator that made this data available, had such poor security on their website that, according to a researcher at CMU, individuals could lookup real-time location data with little effort. The carriers, it seems, trusted but did not verify that consumers were giving consent to be tracked, and that gross negligence on their part exposed the supposedly protected sensitive data of hundreds of millions of people.

These revelations are deeply troubling, but what's more troubling is the lack of knowledge by the FCC of what appeared to be a pervasive practice in the wireless industry. Similar to the Facebook incident, we still don't even know the extent of this breach and who may have had access to this data.

Madam Chairman, I would respectfully request that this Committee hold a hearing on this incident to understand how it happened and to hold the responsible parties accountable. With that I yield back the remainder of my time and look forward to the testimony of our witnesses.

###