Before the Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Expanding Consumers' Video Navigation Choices	)	MB Docket No. 16-42
	)	
Commercial Availability of Navigation Devices	)	CS Docket No. 97-80

Is the FCC Inviting the World's Cyber Criminals into America's Living Rooms?

April 20, 2016

Comments of

Bruce Levinson
Senior Vice President—Regulatory Intervention
Center for Regulatory Effectiveness
1601 Connecticut Avenue, NW
Washington, DC 20009
202.265.2383
www.theCRE.com

Is the FCC Inviting the World's Cyber Criminals into America's Living Rooms?

In October 2012, the Chairman and Ranking Member of the House Intelligence Committee issued a joint statement warning American companies that were doing business with the large Chinese telecommunications companies Huawei and ZTE to "use another vendor."

The bipartisan statement explains that the Intelligence Committee's Report,

> *highlights the interconnectivity of U.S. critical infrastructure systems and warns of the heightened threat of cyber espionage and predatory disruption or destruction of U.S. networks if telecommunications networks are built by companies with known ties to the Chinese state, a country known to aggressively steal valuable trade secrets and other sensitive data from American companies.*

The Report also explains that "modern critical infrastructure is incredibly connected, everything from electric power grids to banking and finance systems to natural gas, oil, and water systems to rail and shipping channels. All of these entities depend on computerized control systems. The risk is high that a failure or disruption in one system could have a devastating ripple effect throughout many aspects of modern American living."

The Report's first recommendation is that "US government systems and US government contractors, particularly those working on sensitive systems, should exclude any Huawei or ZTE equipment or component parts." The Report's second recommendation is that "U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects."

The Federal Communications Commission's AllVid set-top box proposal, if finalized, would likely prohibit industry from following the Intelligence Committee's recommendations since the FCC rule would require that Huawei and ZTE, along with other companies based in countries engaging in cyber-attacks against the United States, be given open access to your television.

Under the FCC proposal, multichannel video programming distributors (MVPD) would be required to open their data systems so that anyone could make a device which would have access to pretty much all consumer cable data such as the programming customers have paid for and the programming that family members watch. The rule would also, in many cases, provide access to the customer's internet connection and connected devices.

The value of the consumer data that could be compromised by AllVid is far more than may be apparent. Although few people are overly concerned that foreign powers may learn that they watch ESPN, as the Ashley Madison hack revealed, even an email address can disclose unintended personal information.

Bad guys, whether or not they are state-sponsored, don't rely on data from only a single seemingly innocuous source, instead hackers assemble information from multiple sources, such as health records and personnel records to develop detailed personalized portraits of millions of Americans. Meanwhile, Russian hackers are expanding their customer service hours to make identity theft, blackmail and other cyber crimes easier than ever.

The FCC's proposal to “unlock” the set top box would also at least partially unlock the intellectual property being broadcast. AllVid is not the first FCC rulemaking to raise intellectual property protection concerns. The FCC proposal does, of course, include an extensive discussion of security measures that would be required by the rule. Anyone who thinks that the proposed security measures would be sufficient to protect the entertainment industry's intellectual property, however, should try a few basic Google searches such as hacking kids' toys to get a sense of how vulnerable consumer electronics are to harmful unauthorized access.

The House Intelligence Committee has recommended that American companies refuse to allow telecommunications equipment made by certain foreign companies to connect to their system even if doing so would be economically advantageous. The FCC should not issue any rule which would undermine the ability of MVPDs to adhere to the Intelligence Committee’s recommendation.