PUBLIC KNOWLEDGE URGES THE FCC TO ACT TO PREVENT AUTO INDUSTRY TROJAN HORSE

DSRC was envisioned as a safety service. The spectrum it utilizes was allocated on the basis that it would be used for saving lives. And yet, 40 MHz - more than half the 5.9 GHz band - is not exclusively for safety-of-life use. It also permits commercial use, for purposes ranging from mobile payments to targeted advertising and media streaming - whatever the auto industry dreams up. This sort of exclusive commercial allocation simply isn't a part of contemporary spectrum policy, particularly in the absence of any payment from the licensees. The auto industry got this spectrum for free, under the guise of public safety use. They now want to monetize it, leveraging mandatory safety tech in all new cars to do so.

Spectrum allocated for public safety purposes is never commercialized. First responders don't lease their valuable spectrum to wireless carriers to support more streaming video. The 5.9 GHz band was allocated to the auto industry almost 20 years ago on the condition that they would use it to save lives. The forthcoming DSRC mandate will do that; but it will also enable subversion of its intended use for public safety in favor of infotainment systems, mobile payments, and targeted advertising. None of these are public safety functions, and the FCC should prohibit their deployment by imposing a noncommercial condition on the use of the 5.9 GHz band.

Road Safety Shouldn't be put at Risk for the Sake of Commercial Services Which Lack Cybersecurity Protections

Cars aren't secure. This is a fact. Researchers have already demonstrated an ability to remotely access and seize control of cars,[1] even before the introduction of DSRC units. A forthcoming NHTSA rule proposes to mandate the inclusion of DSRC units in all new cars being sold. While the deployment of NHTSA's DSRC may save lives, and its standards do include cybersecurity and privacy-by-design, there are currently no protections in place to prevent abuse of this valuable spectrum for inappropriate or dangerous commercial uses.

Mandatory DSRC units, with commercial use permitted, will place an industry woefully ill-equipped and far behind the 8-ball on cybersecurity issues in charge of protecting an attack vector that, if unsecure, would allow a virus to hop from one car to the next, infecting vital safety systems like braking and steering. The auto industry describes what DSRC units do as simply exchanging "data", which they claim can't be used to transmit a virus. This assertion is laughably inaccurate, and demonstrates perfectly the risk inherent in permitting auto industry exploitation of this life-and-safety spectrum.

[1] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway - With Me In It*, Wired (Jul. 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Consumer Privacy Shouldn't Suffer for the Sake of the Auto Industry's Commercial Aspirations

Modern cars track speed and direction of travel, GPS coordinates, and a whole host of other information about consumers. Potential commercial uses of DSRC spectrum include mobile payments, infotainment systems, and targeted in-car advertising - all of which either contributes to or relies upon the exploitation of sensitive personal information about drivers. While this may be acceptable subject to robust disclosure and consent structures, the fact is that DSRC units will be mandated in every car. They won't be optional, meaning many of these commercial services won't be optional, either.

Consumer privacy of data as sensitive as personal payment details, and precise geolocation records, must be adequately protected. While, again, NHTSA DSRC includes robust privacy protections, the bulk of the 5.9 GHz band will be exploited by commercial use by an auto industry which recently described their privacy plans for commercial services as being "whatever the privacy policy of the application provider is . . . like Facebook."[2] This approach is problematic for several reasons, however: unlike with DSRC, Facebook isn't mandatory. Facebook isn't linked into your car, tracking you everywhere you go. By contrast, the degree of control that would be placed in the hands of the auto industry would be alarming, particularly when it is being imposed on consumers under the guise of "road safety."

Regardless of NHTSA's DSRC Mandate, the FCC Still Governs the Spectrum Being Used, and Must Ensure Consumers are Protected

Fortunately, over the past several years the FCC has established a strong practice of addressing cybersecurity and privacy concerns in its rulemakings. In the 5G Spectrum Frontiers order establishing the baseline rules for next-generation wireless networks, cybersecurity plans and privacy protections were required. The same was done in the tech transition, to ensure consumers are protected even during necessary network transitions. The FCC has ample authority over the full 75 MHz of spectrum in the 5.9 GHz band, and appears willing to move forward in addressing these issues.

Public Knowledge has petitioned the FCC to act to prevent commercial exploitation of this spectrum under the guise of protecting the public, and to ensure that the auto industry can't harm consumer privacy and cybersecurity along the way. Congress must support this effort and urge the Commission to move forward, securing these protections for the drivers and passengers of the next generation of connected cars.

---

[2] Margaret Harding McGill, *Latest privacy debate: Crash-avoidance Technology*, Politico (Jun. 28, 2016), https://www.politicopro.com/transportation/story/2016/06/latest-privacy-debate-crash-avoidance-technology-117891.