wiley

PRESS RELEASE

Wiley Rein *Amicus* Brief Urges Supreme Court to Grant Certiorari in Hacking Case, Arguing Class Action Litigation Could Harm Nation's IoT Cybersecurity Policy

October 31, 2018

Press Contact
Patricia O'Connell
T: 202.719.4532
poconnell@wiley.law

Washington, DC – On October 29, Wiley Rein LLP submitted a brief to the Supreme Court of the United States on behalf of *amici curiae* CTIA–The Wireless Association, Cause of Action Institute, and the Association for Unmanned Vehicle Systems International. The brief urges the Court to grant *certiorari* and reaffirm the importance of the standing doctrine in a hacking suit. The petitioners are challenging the Seventh Circuit's denial of an interlocutory appeal regarding a federal court's certification of class litigation against an automaker whose "smart car" system was found vulnerable to hacking.

The brief was filed in support of the petitioners in *FCA US LLC v. Brian Flynn.* Wiley Rein partners Megan L. Brown and Peter S. Hyun, of counsel Matthew J. Gardner, and associates Bethany A. Corbin and Krystal B. Swendsboe co-authored the brief, along with John J. Vecchione of Cause of Action Institute and Thomas C. Power, Jackie McCarthy, and Melanie Tiano of CTIA–The Wireless Association.

Some courts ignore or misapply Supreme Court precedents when evaluating Article III standing related to cybersecurity, the brief argues. Article III of the Constitution is a limit on judicial power, curtailing federal court jurisdiction to actual cases or controversies,

Related Professionals

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Krystal B. Swendsboe
Partner
202.719.4197
kswendsboe@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Telecom, Media & Technology

with a bedrock requirement that a plaintiff have standing. The brief states: "This lawsuit attempts to sidestep Article III's case or controversy requirement, which demands that litigants have standing. If successful, plaintiffs will unleash a wave of litigation over speculative and potential harms. This threatens to stifle innovation."

The brief concludes: "Class action litigation should not drive the nation's IoT cybersecurity policy. The Seventh Circuit's approval of class certification is legally flawed and will have adverse consequences across the nation. This Court should grant the Petition."

The case stems from Fiat Chrysler's challenge of an Illinois federal court's certification of three state-based classes of consumers who claimed that Jeep Cherokees "Uconnect" infotainment systems could be hacked and remotely controlled.

To read the *amicus* brief filed by Wiley Rein, click here.

Wiley Rein's Telecom, Media & Technology and Cybersecurity practices are leading in the area of connected devices, helping clients develop "bring to market," licensing, and compliance strategies for connected devices of all kinds. The firm has played a key role in shaping the discussion of emerging IoT issues and has been featured in pivotal events discussing IoT liability, such as last week's U.S. Chamber Legal Reform Summit. The Practice covers emerging technology and security trends at its blog, WileyConnect.com, where regular podcasts on technology law, IoT policy, and cybersecurity issues are also hosted.