Communications Daily

FTC Seen Having Role

Privacy, Cybersecurity Guidance for Self-Driving Cars Need Details, Say Experts

TOP NEWS | 23 Sep 2016 | Ref: 1609160038

New federal privacy and cybersecurity guidance, part of a larger Department of Transportation safety framework to help car manufacturers speed up testing and deployment of autonomous vehicles (see 1609200039), need more details to see if they'll be a privacy success, experts told us Thursday. They expected companies that commit to privacy principles such as transparency, choice and data security would be subject to FTC and National Highway Traffic Safety Administration (NHTSA) oversight and enforcement.

"More work needs to be done," said Ryan Calo, an assistant professor at the University of Washington School of Law. Further detail, whether industry best practices, a more formal mechanism or even through the courts, is needed to address some issues, he said. If a self-driving car is hacked, which causes an accident, could a passenger sue a manufacturer for poor security if it's in violation of DOT guidance? he asked. "This is a broad framework. It is not specific enough guidance to actually be operationalized by companies."

The report outlines privacy elements that NHTSA wants manufacturers to build into their autonomous vehicle development plans. They include giving consumers clear data privacy and security notices or agreements aligned with the White House Consumer Privacy Bill of Rights. Carmakers should give consumers choice over data collection, use, sharing, retention and deconstruction, including geo-location, biometric and driver behavior information that could personally identify them. The privacy and cybersecurity guidance (spelled out on pages 19-20) say manufacturers should use only data consistent with why it was collected and should retain a minimum amount of data for as long as needed "to achieve legitimate business purposes." They should also de-identify sensitive data where practical, take steps to protect it, maintain data accuracy, provide operators and owners a way to review and correct information, and institute privacy and data protection audits.

Lauren Smith, policy counsel for Future of Privacy Forum, said the guidance was a "great first step" in creating accountability for carmakers. It's voluntary, but there will be a 60-day comment period and expert convenings to get more specific input to turn the guidance into a mandate for companies to submit safety assessments, she said. Her sense is, she said, that industry is optimistic about the guidance, but more details are

needed around transparency, choice and data minimization. "There's going to be some back and forth on that to figure out what is practical in a world that involves the Internet of Things where more data may be essential to powering certain features," she said. "Those will be longer deliberations but folks are generally positive."

Smith said companies could be held accountable if they agree to privacy principles developed in 2014 by the Alliance of Automobile Manufacturers and the Association of Global Automakers. She said she sensed that NHTSA would provide the rulemaking to provide the standard, with the FTC holding companies accountable for the content of those standards. Darrell West, director of Brookings Institution's Center for Technology Innovation, emailed that he thought enforcement is with NHTSA. "It has the power to order recalls and issue regulations related to privacy," he said. Regarding "egregious violations," he said the agency has considerable power to force action and has also clarified that it plans to "carefully" oversee software.

John Simpson, Consumer Watchdog's privacy expert, said the DOT "acknowledging that this is a huge issue" is a positive step. NHTSA asserted it has enforcement power to remove vehicles for safety issues under current regulations and the link between cybersecurity and safety is "clear" since vehicles can be hacked and made unsafe, said Simpson. The link between privacy and safety would be "a little hard to make" so the agency may need additional enforcement authority, he said. He agreed the FTC should have an enforcement role. "You've got a situation where you would have two federal agencies involved potentially in enforcement oversight in privacy, which I think would be a good thing. The more the merrier," he added.

One area that needs more clarity is applying guidance to cars with lower levels of autonomy, said Smith. While the guidance is aimed at "highly automated vehicles" falling under the Society of Automotive Engineers scale of Levels 3 through 5 -- meaning automated systems that can perform some to all driving tasks -- she said DOT wanted to see those elements, including privacy and cybersecurity, applied to below Level 3. "It's not clear how that would be enforced," she said.

written by Dibya Sarkar
