

[Summary] Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles

Cara Bloom, Joshua Tan, Javed Ramjohn, Lujo Bauer

Carnegie Mellon University

Cara Bloom:

Presented at USENIX Symposium on Usable Privacy & Security (SOUPS). July 2017. Santa Clara, CA.

Self-driving vehicles and other networked autonomous robots are emerging technologies that use sophisticated sensors to capture continuous data about the surrounding environment. In the public spaces where autonomous vehicles (AVs) operate there is little reasonable expectation of privacy and no notice or choice given, raising privacy questions for policymakers, technologists, and consumers. Robotic technologies are set to be the next wave of Internet of Things (IoT) devices and, unlike many IoT devices, many will not be owned by consumers directly, presenting a unique privacy policy challenge. This paper explores what consumers' reasonable expectations of privacy are in the context of corporate owned fleets of networked AVs, such as the Uber fleets already deployed in Pittsburgh, San Francisco, and Tempe.

In a study (n=302) of residents in cities with and without Uber AV fleets, we explore people's conceptions of the sensing and analysis capabilities of self-driving vehicles; their comfort with the different capabilities; and the effort, if any, to which they would be willing to go to opt out of data collection. We additionally collect comfort with non-privacy concerns (e.g. driving near an AV), demographic data, biases against AVs and Uber, and each participant's level of exposure to the technology to discover what factors explain discomfort and willingness to protect their information from such technologies in public.

We found that participants consider primary uses (necessary for autonomous driving) of AV sensors such as data collection, aggregation, storage, and analysis by the cars to be likely, and that participants express moderate comfort with these scenarios. Secondary use (non-necessary) scenarios such as the recognition, identification, and tracking of individuals or their vehicles received the lowest ratings of likelihood and highest discomfort. Generally

participants rated many potential capabilities as likely and also expressed high levels of discomfort, but those who thought the technology was more likely to have a privacy-invasive capability such as tracking were more likely to be comfortable with that capability. When asked how long they would spend in an online system to opt out of identifiable data collection by blurring images of themselves or their vehicles, 54% of participants would spend more than five minutes and over one third would spend more than ten minutes to protect their privacy.

Surprisingly, residents in a city with AVs (60% of participants had seen an AV compared to 3% from other cities) did not express significantly different discomfort or opt-out preferences. The only factor that was correlated with a significant increase in opt-out time was whether participants had received the privacy scenario priming questions, which participants noted had raised difficult questions they had not considered before.

If public attention surrounding AVs expands from safety and employment issues to privacy issues, our findings suggest that people's overall comfort with AVs may increase, but so might privacy-seeking behavior. Synthesizing both our findings on consumers' expectations and the effect of asking leading questions, we recommend that policymakers restrict secondary, non-necessary uses of AV-collected data as they are outside the scope of consumer expectation and cause high levels of discomfort. It is additionally recommended that technology companies that operate fleets of self-driving vehicles implement data-protection opt-out features to allow for differentiated privacy preferences.