Privacy in Connected and Automated Vehicles

By Philip Barnes, May 2018

Smartphones on Wheels

Today's vehicles are packed with technologies that control, monitor, and record a variety of information. Data points include speed, acceleration, braking, geolocation, tire pressure, engine diagnostics, and the radio station. When connected and automated vehicles (CAVs) arrive in the coming years, the volume of data generated by automotive technology will increase further. CAVs, along with their infotainment displays, will substitute for the smartphone in your pocket and will be equally functional as data generators and receivers. As with smartphones, CAVs will create privacy and consumer protection concerns.

A New Data Frontier

Connected vehicles generate location and vehicle performance data (often called telematics), but could also include detailed personal information about passengers. Biometric data includes height, weight, facial features, pulse rate, fingerprints, and voice tone. Biometric data enables vehicle features and services such as keyless entry or validation of purchases on touchscreens.

Both telematic and biometric information is tremendously valuable to a wide range of public and private bodies. Governments and private developers are interested in vehicle trajectory data to better inform transportation planning, land use, and urban development decisions. Marketers desire data that reveal spending habits and behaviors to target personalized advertisements. Vehicle data collection and analysis could become a $450 to $750 billion dollar industry in the United States by 2030.[1]

Privacy Concerns

There are legitimate concerns when public and private sector bodies have access to one's telematic and biometric data. Analysis of a vehicle's location can reveal whether an individual frequents a religious center, union hall, or shooting range. Analysis of biometric data can determine personal health information. Even still, many individuals voluntarily allow for personal data collection if they receive a beneficial service in return, such as lower insurance premiums or time-saving routing suggestions that avoid traffic congestion. Public opposition and privacy concerns arise when personal data are shared with third-parties and used in unintended and unknown ways.[2, 3]

Governance Frameworks

The Federal Trade Commission is the federal agency responsible for consumer protection, including privacy. The Consumer Protection Unit within the Delaware Department of Justice has state authority to protect citizens against fraud. Although the FTC recognizes the potential for privacy issues in connected vehicles, neither body has yet to outline dedicated standards or procedures for vehicle privacy.[4]

The Alliance of Automobile Manufacturers and the Association of Global Automakers, two industry trade groups, stepped into the governance void in 2014 and developed a voluntary and self-regulatory set of seven "Privacy Principles" that affiliated automakers commit to follow.[5] Two key principles are "Transparency" and "Choice." Transparency means giving owners clear and meaningful information about data collection, use, and sharing. Choice means giving owners options to control the extent of data collection, use, and sharing. The Privacy Principles are widely cited in the literature and are the dominant framework governing CAV data and consumer privacy in the United States.

Rhetoric or Reality?

The national Government Accountability Office (GAO) analyzed fifteen automakers' vehicle privacy statements and interviewed company representatives to determine the extent to which vehicle manufacturers protect consumer privacy and adhere to their own standards.[6]

The GAO found that automakers' privacy statements are easily available, but they are not written in plain language. The GAO also noted the absence of clear information on data sharing and use practices, and instead found vague wording in privacy statements that make it unclear what limits, if any, apply to data sharing and use. These conditions are inconsistent with the "Transparency" Privacy Principle.

Vehicle owners consent to data collection during purchase and when subscribing to in-vehicle apps or services. However, the GAO found that most owners do not read lengthy consent forms and simply sign or click "accept" out of convenience. Automakers give consumers little control over the degree of data sharing: users can opt-in and receive vehicle services, or opt-out of the service entirely if they are not willing to share vehicle data. There are few options besides all-in or all-out. This is inconsistent with the "Choice" Privacy Principle.

High Stakes

At present, consumer privacy in connected vehicles is largely regulated by the automobile industry. The industry will likely push the boundaries of data collection and usage to capture a share of the growing market worth hundreds of billions of dollars. At the same time, public skepticism toward CAV technology is already very high. A recent survey shows that 82% of Delawareans are "very concerned" or "somewhat concerned" about the security of vehicle data.[7] A single high profile example of data mismanagement or invasion of privacy will provoke a swift backlash and delay deployment. The stakes for earning and maintaining public trust are extremely high.

About the Institute for Public Administration

The University of Delaware's Institute for Public Administration (IPA) addresses the policy, planning, and management needs of its partners through the integration of applied research, professional development, and the education of tomorrow's leaders.

180 Graham Hall | Newark, DE 19716-7380
302-831-8971 | ipa@udel.edu | www.ipa.udel.edu

End Notes

[1] Bertoncello et al., 2016
[2] Brown, 2016
[3] Bloom et al., 2017
[4] Federal Trade Commission, 2018
[5] Alliance of Automobile Manufacturers Inc., Association of Global Automakers Inc., 2014
[6] Government Accountability Office, 2017
[7] American Automobile Association, 2018
For the full work cited visit: www.sppa.udel.edu/ipa/serving-delaware/transportation/cav