Privacy Legislation Trends Connected Car Cos. Should Watch

Reed Freeman

Ali Jessani

Law360 (December 16, 2019, 4:31 PM EST) --

The automobile industry has been racing full speed ahead in recent years on its quest for increased connectivity and automation, but it may soon find itself swept up in the wave of privacy and data security laws and regulations proliferating around the world.

California's Consumer Privacy Act, set to go into effect on Jan. 1, is an illustrative example of how regulators are now viewing data privacy and cybersecurity, with its focuses on: (1) an expansive definition of "personal information"; (2) providing individuals with numerous data privacy rights akin to the European Union's General Data Protection Regulation; and (3) having "reasonable" cybersecurity controls in place to prevent the unauthorized access to or acquisition of personal information or sensitive personal information.

This shifting privacy and cybersecurity framework may especially affect the connected car industry because of the vast amount of information that vehicle manufacturers and developers already collect and pass, directly or indirectly, to third parties — including advertisers and insurance companies. The transition toward greater connectivity and automation will only increase the amount of information processed and shared, which, in turn, will lead to more legislative, regulatory and brand scrutiny.

This article highlights the privacy and cybersecurity trends that the connected car industry and ecosystem should be paying attention to, especially as automobiles continue to become increasingly connected to the internet and to each other.

Why should the connected car industry care about data privacy and cybersecurity?

From information regarding who you are, where you have been, where you are going, how fast you drive, how hard you turn, to what music you listen to, connected cars already collect a wide array of information. One study by McKinsey & Co. found that modern cars may collect as much as 25 gigabytes of data per hour.[1] This information is immensely valuable to advertisers, insurance companies, application developers, data brokers and other third parties who may be willing to pay top dollar for it.

McKinsey further estimates that the automobile data industry could be worth as much as $750 billion by 2030.[2] Much of this monetization will be driven by connectivity and automation: Connected and autonomous vehicles will require new technology (such as Wi-Fi, lidar units, radar sensors and cellular connectivity), as well as the ability to cooperate with other vehicles and infrastructure, which will increase the volume amount of information collected, stored and transferred by vehicles.

More connectivity through Wi-Fi and cellular technology also means more potential points of entry for hackers, who could try to remotely access vehicles to steal sensitive information and wreak potential havoc by taking over vehicles entirely. This makes data breaches in the connected car context particularly dangerous: In addition to data exfiltration, hackers could potentially cause physical damage to people and infrastructure by targeting connected cars for the purpose of harming drivers, passengers and others.

Despite potentially dire privacy and cybersecurity consequences, information collected by connected cars is currently largely unregulated. In the U.S., the Federal Trade Commission can enforce privacy and cybersecurity violations against connected car companies through its authority under Section 5 of the FTC Act,[3] and there are self-regulatory bodies, such as the Alliance for Automobile Manufacturers, that have developed data privacy and security standards.[4]

There is not, however, a general regulatory framework that governs privacy and cybersecurity in the connected car context like there is for other industries that process large amounts of information, like financial institutions and health care providers.

The CCPA (and the other state and perhaps federal laws that it will inspire as soon as 2020) will change all of that. It will require all businesses that collect personal information from California residents to provide those residents with certain data privacy rights, such as the right to access their information,[5] the right to opt-out of the sale of their personal information[6] and the right to delete their personal information.[7]

"Personal information" under the CCPA is defined broadly, and the categories of information listed as examples of personal information covered under the law include many categories that connected cars already collect, such as biometrics (face scans, iris scans, fingerprints, etc.) unique identifiers, internet or other network activity and geolocation data.[8]

And, while the CCPA is only enforceable by the California attorney general for its privacy provisions, it creates a private right of action for consumers (directly or through their representatives in the plaintiffs' bar) whose personal information is subject to a data breach as a result of a business's failure to maintain reasonable security procedures and practices.[9]

The CCPA is the first comprehensive data privacy law in the United States, but it is very much unlikely to be the last. At least 10 other states considered similar bills in 2019, and though none of the scope of CCPA became law this term, many more states — including Illinois, New Jersey, Rhode Island and Washington — are likely to try again in 2020. There is also a renewed push in Congress regarding a comprehensive national data privacy and security bill.[10]

The legislation proposed on both the federal and state level, as well as recent laws enacted by states (including the CCPA), highlight a few common principles, which will likely become the basis for future laws as well.

As connected car companies speed toward an automated future, they should be especially cognizant of these trends because the shift to automation will require even more connectivity and data accumulation, squarely placing them under

the purview of data privacy and cybersecurity legislation. Accounting for these trends will allow manufacturers and industry stakeholders to mitigate the regulatory risks associated with data collection, storage and dissemination.

What data privacy and cybersecurity trends should connected car companies be aware of?

1. The definition of personal information is expanding.

Other states that pass comprehensive data privacy laws may deviate from the CCPA when it comes to specifics, but one element that they will almost certainly incorporate is the CCPA's expansive definition of personal information.

Instead of protecting specific information collected in specific contexts (such as how the Gramm-Leach-Bliley Act regulates personal information collected by financial institutions), comprehensive data privacy laws, like the CCPA and the GDPR, aim to protect any and all information collected that relates to, and that can be reasonably connected to, identifiable individuals.

This, of course, has a drastic effect on the connected car industry because of the amount of information today's cars can collect. To the extent that connected cars collect information on particular consumers in a manner that is not deidentified or aggregated, they will be subject to the comprehensive data privacy laws of the future, including the CCPA.

Connected car companies should also be aware that, in addition to attempting to pass comprehensive privacy laws, states are also increasingly looking to regulate specific subsets of information they deem to be more sensitive. Many of these laws intersect with information collected by connected and autonomous cars.

Texas,[11] Illinois[12] and Washington,[13] for example, have laws specifically governing the collection of biometric information, and this is likely to increase materially in coming years.

These laws may affect manufacturers developing level 3 (conditional automation),[14] level 4 (high automation)[15] or level 5 (full automation)[16] vehicles because they may use biometrics for a number of different reasons, such as to determine whether a user is focusing on the road so that they may take control of the vehicle during an emergency or to allow users to utilize hand gestures in order to make commands to the vehicle. This trend will also likely continue and could include other information necessary for connected and autonomous cars, such as geolocation information.

Finally, connected car companies should note that the definition of personal information is also expanding in the states' data breach notification laws. All 50 states have some form of a breach notification requirement,[17] and states are now looking to expand the information covered under these laws, which could include more information collected by connected cars.

New York, for example, passed the Stop Hacks and Improve Electronic Data Security Act earlier in 2019,[18] which expanded the definition of "private information" protected under the law to include biometrics. California[19] and

Washington[20] also added biometrics to their breach notification laws. Other states may follow suit and protect more information through their breach statutes.

2. The focus is increasingly on providing consumers with individual rights.

Another principle that the CCPA borrowed from the GDPR and that will likely be incorporated into future comprehensive data privacy laws and regulations is its focus on providing consumers with individual data privacy rights. The trend here is to allow the consumer to decide what information is important to them and to give them control regarding if and how this information is maintained and shared by the entity in charge of its collection. Other international comprehensive privacy laws are trending toward this paradigm.

What this means for connected and autonomous car manufacturers and their application developers is that they should design cars and applications of the future with this framework in mind. Manufacturers and developers may, for example, be required to comply with requests to delete information that they receive from consumers. Incorporating "privacy by design" principles will allow manufacturers to develop vehicles that can readily comply with such requests.

Manufacturers should also think about what consumer rights may be unique to autonomous vehicles when it comes to data collection and can look at state laws already in effect for guidance. California, for instance, requires AV manufacturers to either obtain written approval from the owner or lessee of an autonomous in order to collect information that is not necessary for the safe operation of the vehicle or to anonymize that information.[21] Like the CCPA, California's privacy standards for autonomous vehicles may drive the national conversation around the issue once highly automated vehicles begin to hit the road.

3. When it comes to cybersecurity, be reasonable.

While the CCPA is primarily a data privacy statute, it creates a private right of action for consumers "whose nonencrypted and nonredacted personal information[22] ... is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[23]

Neither the CCPA nor the draft regulations promulgated by the California attorney general define what constitute reasonable security procedures and practices. While the lack of guidance here is troublesome,[24] it is also telling as to what lawmakers expect from entities when it comes to data protection, which is that there is not a one-size-fits-all answer to cybersecurity and that companies need to be proactive in identifying and mitigating potential risks.

Though the CCPA's private right of action for data breaches has caught businesses' attention, it is one of many laws that requires companies to be reasonable when it comes to cybersecurity. The FTC has long advocated for companies to implement reasonable and appropriate data security measures and has used its Section 5 authority to bring enforcement actions against companies that have failed to do so. Its recent consent order with DealerBuilt — an auto dealer software

provider — is an example of why car manufacturers, auto dealers and their service providers need to take data privacy and security seriously.[25]

Reasonableness is also blended into international laws, such as the GDPR, which requires data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.[26]

Other recently enacted cybersecurity laws that could intersect with the connected car industry also implement a reasonableness standard. In addition to updating its definition of "private information," New York's SHIELD Act requires businesses that own or license computerized data that includes private information to "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information."[27]

California[28] and Oregon[29] both recently passed Internet of data security laws that, effective Jan. 1, will require internet of things manufacturers to equip connected devices with "reasonable security features." These laws indicate that, when it comes to cybersecurity, lawmakers will continue to put the onus on businesses to incorporate reasonable security mechanisms instead of identifying specific compliance measures.

Start planning now.

New regulations do not need to be a cause for concern if your business is proactive in terms of addressing its potential regulatory obligations. We recommend that the connected car industry take the following first steps to prepare for the CCPA and other international privacy and cybersecurity laws it may be subject to:

1. Map your data.

Understanding whether you have specific obligations under various privacy laws and providing consumers with their individual rights requires being aware of what data you have in the first place. Documenting and monitoring and your data collection practices will allow you to assess your regulatory obligations, as well as to take the first step toward compliance.

2. Update your privacy policy.

The FTC already uses its Section 5 authority to bring enforcement actions against companies who mislead consumers through their privacy policies. Updating your privacy policy to accurately reflect your data collection and sharing practices will not only help you evade FTC scrutiny but will be necessary for comprehensive privacy laws like the CCPA and GDPR.

3. Identify potential sources of risk.

If you are not subject to any privacy regulations currently but fear you may be in the future and don't know where to start in terms of mitigating your greatest sources of risk, a good place to look might be what the third parties you share information with are doing with the data. Are they using it in ways that are typical and would be expected by the consumer or are their data practices likely to raise a suspicious eye by regulators? Understanding the answer to this question will begin to inform you of your potential privacy compliance risk.

4. Develop and maintain an information security plan.

Being able to show that you have identified potential risks to your business and have proactively taken steps to mitigate those risks is a necessary element toward implementing what could be considered reasonable security measures. A regulator or a court is far more likely to be on your side if you have a plan in place instead of showing up empty-handed after suffering a data breach.

Conclusion

The rapidly changing nature of privacy and cybersecurity laws should not slow down connected car manufacturers as they transition to autonomous vehicles, especially because of the numerous societal benefits associated with highly automated vehicles. Keeping these principles in mind will allow manufacturers to develop the cars of the future without having to stop for regulators.

Reed Freeman is a partner and co-chair of the cybersecurity and privacy practice group at WilmerHale.

Ali Jessani is an associate at the firm.

[1] McKinsey, What's Driving the Connected Car (September 2014), available at: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car.

[2] McKinsey, Monetizing Car Data (September 2016), available at: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx.

[3] See 15 U.S.C. § 45(a)(1).

[4] The Alliance of Automobile Manufacturers' Consumer Privacy Protection Principles are available at: https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

[5] Cal. Civ. Code § 1798.100; Cal. Civ. Code § 1798.110; Cal. Civ. Code § 1798.115.

[6] Cal. Civ. Code § 1798.120.

[7] Cal. Civ. Code § 1798.105.

[8] See Cal. Civ. Code § 1798.140(o)(1).

[9] See Cal. Civ. Code § 1798.150(a)(1).

[10] Both Democrats and Republicans in the Senate have released drafts of comprehensive data privacy bills in recent weeks. See Consumer Online Privacy Rights Act (proposed by Senator Maria Cantwell), available at: https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf; Senator Roger Wicker staff discussion draft, available at: https://aboutblaw.com/NaZ.

[11] Tex. Bus. & Com. Code § 503.001.

[12] 740 ILCS §§ 14/1 et. seq.

[13] Rev. Code Wash. §§ 19.375.010-40.

[14] These categories refer to the levels of automation developed by the Society of Automotive Engineers and adopted by the National Highway and Transportation Safety Administration ("NHTSA"). A Level 3 vehicle is one that is considered to have "Conditional Automation," which means that the automated driving system ("ADS") will control the dynamic driving task with the expectation that the human driver will respond appropriately at a request to intervene. See U.S. Department of Transportation, Preparing for the Future of Transportation: Automated Vehicles 3.0 (October 2018), available at: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

[15] A Level 4 vehicle is one that has "High Automation," which means that the ADS controls all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene. A human driver is essentially only required to take control of the vehicle in case of an emergency.

[16] A Level 5 vehicle is one that is considered to have "Full Automation," which means that the ADS controls the dynamic driving task under all roadway and environmental conditions.

[17] See National Conference of State Legislatures, Breach Notification Laws, available at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[18] NY Sen. Bill S5575B (2019-2020), available at: https://www.nysenate.gov/legislation/bills/2019/s5575.

[19] Cal. Assembly Bill 1130 (2019-2020), available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130.

[20] Wash. House Bill 1071 (2019), available at: http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/House/1071-S.SL.pdf.

[21] See 13 CCR § 228.24.

[22] We should note here that the definition of "personal information" that falls under the CCPA's private right of action is narrower than the definition of "personal information" that is otherwise covered under the law. "Personal information" in the breach context for the CCPA is defined under Cal. Civ. Code 1798.81.5(d)(1)(A).

[23] Cal. Civ. Code § 1798.150(a)(1).

[24] Businesses may be able to use previous guidance from the California AG and the FTC to determine what constitute reasonable security features. See California Department of Justice, California Data Breach Report 2012-2015 (February 2016), available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf; FTC, Start with Security: A Guide for Business (June 2015), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[25] The FTC's consent order with DealerBuilt is available at: https://www.ftc.gov/system/files/documents/cases/172_3051_dealerbuilt_final_consent_agreement_6-12-19.pdf.

[26] GDPR, art. 32(1).

[27] N.Y. Sen. Bill S5575B (2019-2020), available at: https://www.nysenate.gov/legislation/bills/2019/s5575.

[28] Cal. Sen. Bill 327 (2017-2018), available at: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

[29] Ore. House Bill 2395 (2019), available at: https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled.