wiley

NEWSLETTER

Massachusetts Ballot Initiative Raises Privacy and Data Security Concerns for Connected Devices

November 2020

Privacy in Focus®

On November 3, Massachusetts voters approved the adoption of a ballot measure amending state law to require auto manufacturers to facilitate access to and sharing of an expanded set of user data with independent repair shops.

Specifically, the ballot measure requires manufacturers that sell vehicles with telematics systems in Massachusetts to equip them with a new standardized open access data platform. Beginning with model year 2022, vehicle owners and independent repair facilities will be able to retrieve a vehicle's mechanical data and run diagnostics through a mobile-based application. The ballot initiative raises potential privacy and data security concerns that extend not only to vehicles, but to other connected devices that are likely to be targets of similar proposals going forward.

The Massachusetts Right to Repair Initiative Raises Privacy and Data Security Concerns

The Massachusetts Right to Repair Initiative, Question 1, is part of the "right-to-repair" debate – which has been the subject of significant state legislative activity and Federal Trade Commission (FTC) attention over the last several years. Nearly a decade ago, Massachusetts passed a first-of-its-kind law that gave car owners and independent repair shops the ability to access mechanical information by plugging into the vehicle's On-Board Diagnostics (OBD) port.[1] The 2012 law exempted the vehicle's telematics

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

systems – systems that collect and wirelessly transmit mechanical data to a remote server.[2] Telematics data systems are highly proprietary and vary by manufacturer; however, common features include collision notification, emergency assistance, roadside assistance, vehicle diagnostics, media streaming, and geofencing. These features often rely on the vehicle's GPS, Bluetooth, or Wi-Fi-generated data, which can provide specific and historical location and other personal information.

As cars become more computerized, consumer advocates have urged the adoption of a standardized open platform to better enable consumers to patronize independent repair shops. But the measure also raises novel privacy and data security risks by enabling access to detailed consumer data by independent repair facilities that may not have adequate cybersecurity protections in place. As similar legislation is considered that would apply to other connected devices, manufacturers and other stakeholders must pay careful attention to privacy and security concerns.

Existing Right to Repair Law

Existing Massachusetts law, Chapter 93J,[3] requires manufacturers to "provide [independent repair facilities and dealerships] the same diagnostic and repair information ... which the manufacturer makes available to its dealers and authorized motor vehicle repair facilities" necessary to diagnose and repair a consumer's car. However, the law limits access to a vehicle's non-diagnostic data, including "telematics services"[4] and immobilizer or security-related electronics functions[5] – the latter of which are instead accessed through a "secure data release model system used by the National Automotive Service Task Force or other known, reliable and accepted systems."[6]

The Massachusetts Right to Repair Initiative

Starting with model year 2022, the ballot initiative will require:

Open Access Data Platform. The initiative will require "manufacturers of motor vehicles sold in Massachusetts to equip any such vehicles that use telematics systems [ ] with a standardized open access data platform."[7]

Mobile Application-Based Control. Additionally, owners of vehicles equipped with telematics systems and independent repair facilities will be "provided with *expanded access* to mechanical data" through a mobile device application. The mobile app will facilitate remote, real-time, bi-directional access whereby a remote actor "would be able to retrieve mechanical data from and send commands to [] the vehicle."[8]

Consumer Notice. The initiative requires the Attorney General to establish a "motor vehicle telematics system notice" for consumers providing:

- an explanation of motor vehicle telematics and its purposes;
- a description summarizing the mechanical data collected, stored, and transmitted by a telematics system;
- the prospective owner's ability to access the vehicle's mechanical data through a mobile device; and

- an owner's right to authorize an independent repair facility to access the vehicle's mechanical data for vehicle diagnostics, repair, and maintenance purposes.

Dealers will be required to provide and collect acknowledgment of receipt of the notice from auto vehicle buyers and lessees. Failure to comply with the notice requirements would subject dealers to applicable sanctions. Motor vehicle owners and independent repair facilities could enforce this law through state consumer protection laws and recover civil penalties of the greater of treble damages or $10,000 per violation.

Privacy and Data Security Risks

The initiative raises significant issues around protecting the privacy and security of consumer data. Auto repair facilities without robust security processes may leave consumer data – and the vehicles themselves – vulnerable to cybersecurity threats. Indeed, the National Highway Traffic Safety Administration (NHTSA), in response to a request from Massachusetts legislators, highlighted this point.[9] Noting that its "primary interest focuses on cybersecurity vulnerabilities that present potential vehicle safety consequences," it wrote that "[t]he requirement to establish universal and standardized access requirements increases the scale of risks of any potentially successful cybersecurity attack ... [such] that a single successful malicious cyberattack could have much wider scale of consequences."[10] The agency further noted that on whole, "the ballot initiative would prohibit manufacturers from complying with both existing Federal guidance and cybersecurity hygiene best practices."[11]

More broadly, independent repair facilities may not have the training or technical safeguards to protect sensitive data that is accessed from the vehicle – including location information – while manufacturers may be able to require authorized repair facilities to follow certain safeguards. At the same time, technical improvements to improve privacy and security of vehicle information, in light of the mandatory open data platform, may be difficult to implement by the time the law goes into effect.

What's Next?

Massachusetts is the lone state to have adopted an auto "right-to-repair" law, but there is precedent for its effects to be wide-reaching. Notably, Massachusetts's initial right-to-repair law went to effect in 2013, and by 2014, the industry agreed in a memorandum of understanding to expand its provisions to cover the entire country.[12] It remains to be seen what action, if any, the state legislature will take and whether the industry will take a similar course following the passage of the Massachusetts Right to Repair Initiative.

Outside the context of vehicles, similar "right-to-repair" proposals that would apply to consumer electronics more broadly have been raised for consideration in a myriad of states during 2019-2020 legislative session – at least 17 state legislatures considered legislative proposals, including Massachusetts, Minnesota, Vermont, New York, Washington, Georgia, Hawaii, Oklahoma, Alabama, Maine, Missouri, Colorado, Maryland, New Hampshire, California, and Idaho, and New Jersey. And the FTC is still expected to weigh in with recommendations from its 2019 workshop on "repair restrictions." While state legislative proposals differ in some respects, they raise similar issues about uncontrolled access to sensitive data stored on devices, that

can pose privacy and security threats to consumers. IoT device manufacturers – and others – concerned about protecting device security through the product lifecycle should closely monitor developments on the "right-to-repair" front.

Wiley's Privacy, Cyber & Data Governance team counsels clients on data security compliance, risk management, and regulatory and policy approaches to privacy and cybersecurity. Please reach out to the author for further information.

---

[1] H. 4362 (July 31, 2012).

[2] *Id.*

[3] H. 3757 (Nov. 26, 2013). The Massachusetts legislature enacted H. 3757 to reconcile H. 4362 that was passed in advance of a ballot initiative.

[4] *Id.*

[5] *Id.*

[6] *See* Massachusetts Information for Voters, 2020.

[7] *Id.*

[8] *Id.*

[9] *See Testimony in Response to Mass. Joint Cmte. on Consumer Protection and Prof. Licensure*, NHTSA (July 20, 2020).

[10] *Id.*

[11] *Id.*

[12] Memorandum of Understanding (Jan 15, 2014)

© 2020 Wiley Rein LLP