II

116TH CONGRESS
1ST SESSION

S. 2182

To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 18, 2019

Mr. MARKEY (for himself and Mr. BLUMENTHAL) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Security and Privacy in Your Car Act of 2019'' or the ''SPY Car Act of 2019''.

SEC. 2. CYBERSECURITY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—Chapter 301 of title 49, United States Code, is amended by inserting after section 30128 the following:

"§ 30129. Cybersecurity standards

''(a) DEFINITIONS.—In this section:

''(1) CRITICAL SOFTWARE SYSTEMS.—The term 'critical software systems' means software systems that can affect—

''(A) the control by the driver of the vehicle movement; or

''(B) the safety features of the vehicle.

''(2) DRIVING DATA.—The term 'driving data' includes any electronic information collected about—

''(A) the status of a vehicle, including the location and speed of the vehicle; and

''(B) any owner, lessee, driver, or passenger of a vehicle.

''(3) ENTRY POINT.—The term 'entry point' includes a means by which—

''(A) driving data may be accessed, directly or indirectly; or

''(B) a control signal may be sent or received either wirelessly or through wired connections.

''(4) HACKING.—The term 'hacking' means the unauthorized access to electronic controls, critical software systems, or driving data, either wirelessly or through wired connections.

''(b) CYBERSECURITY STANDARDS.—

''(1) REQUIREMENT.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which regulations are promulgated pursuant to section 2(c)(2) of the SPY Car Act of 2019 shall comply with the cybersecurity standards under paragraphs (2) through (4).

''(2) PROTECTION AGAINST HACKING.—

''(A) IN GENERAL.—All entry points to the electronic systems of each motor vehicle manufactured for sale in the United States shall be equipped with reasonable measures to protect against hacking attacks.

''(B) ISOLATION MEASURES.—The measures referred to in subparagraph (A) shall incorporate isolation measures to separate critical software systems from noncritical software systems.

''(C) EVALUATION.—The measures referred to in subparagraph (A) shall be evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.

''(D) ADJUSTMENT.—The measures referred to in subparagraph (A) shall be adjusted and updated based on the results of the evaluation under subparagraph (C).

''(3) SECURITY OF COLLECTED INFORMATION.—All driving data collected by the electronic systems that are built into motor vehicles shall be reasonably secured to prevent unauthorized access—

''(A) while the data is stored onboard the vehicle;

''(B) while the data is in transit from the vehicle to another location; and

''(C) in any subsequent offboard storage or use of the data.

''(4) DETECTION, REPORTING, AND RESPONDING TO HACKING.—Any motor vehicle manufactured for sale in the United States that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.''.

(b) CIVIL PENALTIES.—Section 30165(a)(1) of title 49, United States Code, is amended by inserting ''30129,'' after ''30127,''.

(c) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Administrator of the National Highway Traffic Safety Administration (referred to in this subsection as the ''Administrator''), after consultation with the Federal Trade Commission, shall issue a notice of proposed rulemaking to carry out section 30129 of title 49, United States Code.

(2) FINAL REGULATIONS.—Not later than 3 years after the date of enactment of this Act, the Administrator, after consultation with the Federal Trade Commission, shall promulgate final regulations to carry out section 30129 of title 49, United States Code.

(3) UPDATES.—Not later than 3 years after final regulations are promulgated pursuant to paragraph (2) and not less frequently than once every 3 years thereafter, the Administrator, after consultation with the Federal Trade Commission, shall—

(A) review the final regulations promulgated pursuant to paragraph (2); and

(B) update the final regulations, as necessary.

(d) CLERICAL AMENDMENT.—The table of sections for chapter 301 of title 49, United States Code, is amend-

ed by inserting after the item relating to section 30128 the following:

''30129. Cybersecurity standards.''.

SEC. 3. CYBER DASHBOARD.

(a) IN GENERAL.—Section 32302 of title 49, United States Code, is amended by adding at the end the following:

''(e) CYBER DASHBOARD.—

''(1) IN GENERAL.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are promulgated pursuant to section 3(b)(2) of the SPY Car Act of 2019 shall display a 'cyber dashboard' as a component of the label required to be affixed to each motor vehicle under section 3 of the Automobile Information Disclosure Act (15 U.S.C. 1232).

''(2) FEATURES.—The cyber dashboard required under paragraph (1) shall inform consumers, through an easy to understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements under section 30129 of this title and in section 27 of the Federal Trade Commission Act.''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Administrator of the National Highway Traffic Safety Administration (referred to in this subsection as the ''Administrator''), after consultation with the Federal Trade Commission, shall issue a notice of proposed rulemaking for the cybersecurity and privacy information required to be displayed under section 32302(e) of title 49, United States Code.

(2) FINAL REGULATIONS.—Not later than 3 years after the date of enactment of this Act, the Administrator, after consultation with the Federal Trade Commission, shall promulgate final regulations to carry out section 32302(e) of title 49, United States Code.

(3) UPDATES.—Not less frequently than once every 3 years, the Administrator, after consultation with the Federal Trade Commission, shall—

(A) review the final regulations promulgated pursuant to paragraph (2); and

(B) update the final regulations, as necessary.

SEC. 4. PRIVACY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—The Federal Trade Commission Act (15 U.S.C. 41 et seq.) is amended by inserting after section 26 (15 U.S.C. 57c–2) the following:

"SEC. 27. PRIVACY STANDARDS FOR MOTOR VEHICLES.

"(a) DEFINITIONS.—In this section:

"(1) COVERED MOTOR VEHICLE.—The term 'covered motor vehicle' means a motor vehicle that—

"(A) is manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are promulgated under section 4(b) of the SPY Car Act of 2019; and

"(B) collects driving data.

"(2) DRIVING DATA.—The term 'driving data' has the meaning given the term in section 30129(a) of title 49, United States Code.

"(b) REQUIREMENT.—Each covered motor vehicle shall comply with the requirements described in subsections (c) through (e).

"(c) TRANSPARENCY.—Each manufacturer of a covered motor vehicle shall provide to each owner and lessee of the covered motor vehicle a clear and conspicuous notice, in clear and plain language, of any collection, transmission, retention, or use of driving data collected from the covered motor vehicle.

''(d) CONSUMER CONTROL.—

''(1) IN GENERAL.—Subject to paragraphs (2) and (3), an owner or lessee of a covered motor vehicle may opt out of the collection and retention of driving data by the covered motor vehicle.

''(2) ACCESS TO NAVIGATION TOOLS.—If an owner or lessee of a covered motor vehicle opts out of the collection and retention of driving data under paragraph (1), the owner or lessee shall not, to the extent technically possible, lose access to any navigation tool or other feature or capability.

''(3) EXCEPTION.—Paragraph (1) shall not apply to driving data stored as part of the electronic data recorder system or other safety systems on board the motor vehicle that are required for post-incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.

''(e) LIMITATION ON USE OF PERSONAL DRIVING INFORMATION.—

''(1) IN GENERAL.—No manufacturer, including an original equipment manufacturer, may use any information collected by a covered motor vehicle for the purpose of advertising or marketing without the

affirmative, express consent of the owner or lessee of the covered motor vehicle.

''(2) REQUESTS.—Any request for the consent under paragraph (1) by a manufacturer—

''(A) shall be clear and conspicuous;

''(B) shall be made in clear and plain language; and

''(C) may not be a condition for the use of any nonmarketing feature, capability, or functionality of the covered motor vehicle.

''(f) ENFORCEMENT.—A violation of this section shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B).''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Federal Trade Commission, after consultation with the Administrator of the National Highway Traffic Safety Administration (referred to in this subsection as the ''Administrator''), shall issue a notice of proposed rulemaking, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act.

(2) FINAL REGULATIONS.—Not later than 3 years after the date of enactment of this Act, the Federal Trade Commission, after consultation with the Administrator, shall promulgate final regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act.

(3) UPDATES.—Not less frequently than once every 3 years, the Federal Trade Commission, after consultation with the Administrator, shall—

(A) review the final regulations promulgated under paragraph (2); and

(B) update the final regulations as necessary.

SEC. 5. CYBERSECURITY TOOLS AND CYBER COORDINATOR.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Federal Highway Administration.

(2) CYBER INCIDENT.—The term ''cyber incident'' has the meaning given the term ''significant cyber incident'' in Presidential Policy Directive–41 (July 26, 2016, relating to cyber incident coordination).

(3) TRANSPORTATION AUTHORITY.—The term ''transportation authority'' means—

(A) a public authority (as defined in section 101(a) of title 23, United States Code);

(B) an owner or operator of a highway (as defined in section 101(a) of title 23, United States Code);

(C) a manufacturer that manufactures a product related to transportation; and

(D) a division office of the Federal Highway Administration.

(b) CYBERSECURITY TOOL.—

(1) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Administrator shall develop a tool to assist transportation authorities in identifying, detecting, protecting against, responding to, and recovering from cyber incidents.

(2) REQUIREMENTS.—In developing the tool under paragraph (1), the Administrator shall—

(A) use the cybersecurity framework established by the National Institute of Standards and Technology and required by Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11739; relating to improving critical infrastructure cybersecurity);

(B) establish a structured cybersecurity assessment and development program;

(C) consult with appropriate transportation authorities, operating agencies, industry stakeholders, and cybersecurity experts; and

(D) provide for a period of public comment and review on the tool.

(c) DESIGNATION OF CYBER COORDINATOR.—

(1) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Administrator shall designate an office as a ''cyber coordinator'', which shall be responsible for monitoring, alerting, and advising transportation authorities of cyber incidents.

(2) REQUIREMENTS.—The office designated under paragraph (1) shall—

(A) provide to transportation authorities a secure method of notifying a single Federal entity of cyber incidents;

(B) monitor cyber incidents that affect transportation authorities;

(C) alert transportation authorities to cyber incidents that affect those transportation authorities;

(D) investigate unaddressed cyber incidents that affect transportation authorities; and

(E) provide to transportation authorities educational resources, outreach, and awareness on fundamental principles and best practices in cybersecurity for transportation systems.

○