

116TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Security and Privacy
5 in Your Car Act of 2019” or the “SPY Car Act of 2019”.

6 **SEC. 2. CYBERSECURITY STANDARDS FOR MOTOR VEHI-**
7 **CLES.**

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

1 **“§ 30129. Cybersecurity standards**

2 “(a) DEFINITIONS.—In this section:

3 “(1) CRITICAL SOFTWARE SYSTEMS.—The term
4 ‘critical software systems’ means software systems
5 that can affect—

6 “(A) the control by the driver of the vehi-
7 cle movement; or

8 “(B) the safety features of the vehicle.

9 “(2) DRIVING DATA.—The term ‘driving data’
10 includes any electronic information collected about—

11 “(A) the status of a vehicle, including the
12 location and speed of the vehicle; and

13 “(B) any owner, lessee, driver, or pas-
14 senger of a vehicle.

15 “(3) ENTRY POINT.—The term ‘entry point’ in-
16 cludes a means by which—

17 “(A) driving data may be accessed, directly
18 or indirectly; or

19 “(B) a control signal may be sent or re-
20 ceived either wirelessly or through wired con-
21 nections.

22 “(4) HACKING.—The term ‘hacking’ means the
23 unauthorized access to electronic controls, critical
24 software systems, or driving data, either wirelessly
25 or through wired connections.

26 “(b) CYBERSECURITY STANDARDS.—

1 “(1) REQUIREMENT.—All motor vehicles manu-
2 factured for sale in the United States on or after the
3 date that is 2 years after the date on which regula-
4 tions are promulgated pursuant to section 2(c)(2) of
5 the SPY Car Act of 2019 shall comply with the cy-
6 bersecurity standards under paragraphs (2) through
7 (4).

8 “(2) PROTECTION AGAINST HACKING.—

9 “(A) IN GENERAL.—All entry points to the
10 electronic systems of each motor vehicle manu-
11 factured for sale in the United States shall be
12 equipped with reasonable measures to protect
13 against hacking attacks.

14 “(B) ISOLATION MEASURES.—The meas-
15 ures referred to in subparagraph (A) shall in-
16 corporate isolation measures to separate critical
17 software systems from noncritical software sys-
18 tems.

19 “(C) EVALUATION.—The measures re-
20 ferred to in subparagraph (A) shall be evalu-
21 ated for security vulnerabilities following best
22 security practices, including appropriate appli-
23 cations of techniques such as penetration test-
24 ing.

1 “(D) ADJUSTMENT.—The measures re-
2 ferred to in subparagraph (A) shall be adjusted
3 and updated based on the results of the evalua-
4 tion under subparagraph (C).

5 “(3) SECURITY OF COLLECTED INFORMA-
6 TION.—All driving data collected by the electronic
7 systems that are built into motor vehicles shall be
8 reasonably secured to prevent unauthorized access—

9 “(A) while the data is stored onboard the
10 vehicle;

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

13 “(C) in any subsequent offboard storage or
14 use of the data.

15 “(4) DETECTION, REPORTING, AND RESPOND-
16 ING TO HACKING.—Any motor vehicle manufactured
17 for sale in the United States that presents an entry
18 point shall be equipped with capabilities to imme-
19 diately detect, report, and stop attempts to intercept
20 driving data or control the vehicle.”.

21 (b) CIVIL PENALTIES.—Section 30165(a)(1) of title
22 49, United States Code, is amended by inserting “30129,”
23 after “30127.”.

24 (c) RULEMAKING.—

1 (1) IN GENERAL.—Not later than 18 months
2 after the date of enactment of this Act, the Adminis-
3 trator of the National Highway Traffic Safety Ad-
4 ministration (referred to in this subsection as the
5 “Administrator”), after consultation with the Fed-
6 eral Trade Commission, shall issue a notice of pro-
7 posed rulemaking to carry out section 30129 of title
8 49, United States Code.

9 (2) FINAL REGULATIONS.—Not later than 3
10 years after the date of enactment of this Act, the
11 Administrator, after consultation with the Federal
12 Trade Commission, shall promulgate final regula-
13 tions to carry out section 30129 of title 49, United
14 States Code.

15 (3) UPDATES.—Not later than 3 years after
16 final regulations are promulgated pursuant to para-
17 graph (2) and not less frequently than once every 3
18 years thereafter, the Administrator, after consulta-
19 tion with the Federal Trade Commission, shall—

20 (A) review the final regulations promul-
21 gated pursuant to paragraph (2); and

22 (B) update the final regulations, as nec-
23 essary.

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

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

“30129. Cybersecurity standards.”.

3 **SEC. 3. CYBER DASHBOARD.**

4 (a) IN GENERAL.—Section 32302 of title 49, United
5 States Code, is amended by adding at the end the fol-
6 lowing:

7 “(e) CYBER DASHBOARD.—

8 “(1) IN GENERAL.—All motor vehicles manu-
9 factured for sale in the United States on or after the
10 date that is 2 years after the date on which final
11 regulations are promulgated pursuant to section
12 3(b)(2) of the SPY Car Act of 2019 shall display a
13 ‘cyber dashboard’ as a component of the label re-
14 quired to be affixed to each motor vehicle under sec-
15 tion 3 of the Automobile Information Disclosure Act
16 (15 U.S.C. 1232).

17 “(2) FEATURES.—The cyber dashboard re-
18 quired under paragraph (1) shall inform consumers,
19 through an easy to understand, standardized graph-
20 ic, about the extent to which the motor vehicle pro-
21 tects the cybersecurity and privacy of motor vehicle
22 owners, lessees, drivers, and passengers beyond the
23 minimum requirements under section 30129 of this
24 title and in section 27 of the Federal Trade Com-
25 mission Act.”.

1 (b) RULEMAKING.—

2 (1) IN GENERAL.—Not later than 18 months
3 after the date of enactment of this Act, the Adminis-
4 trator of the National Highway Traffic Safety Ad-
5 ministration (referred to in this subsection as the
6 “Administrator”), after consultation with the Fed-
7 eral Trade Commission, shall issue a notice of pro-
8 posed rulemaking for the cybersecurity and privacy
9 information required to be displayed under section
10 32302(e) of title 49, United States Code.

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

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

20 (A) review the final regulations promul-
21 gated pursuant to paragraph (2); and

22 (B) update the final regulations, as nec-
23 essary.

1 **SEC. 4. PRIVACY STANDARDS FOR MOTOR VEHICLES.**

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

5 **“SEC. 27. PRIVACY STANDARDS FOR MOTOR VEHICLES.**

6 “(a) DEFINITIONS.—In this section:

7 “(1) COVERED MOTOR VEHICLE.—The term
8 ‘covered motor vehicle’ means a motor vehicle that—

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

14 “(B) collects driving data.

15 “(2) DRIVING DATA.—The term ‘driving data’
16 has the meaning given the term in section 30129(a)
17 of title 49, United States Code.

18 “(b) REQUIREMENT.—Each covered motor vehicle
19 shall comply with the requirements described in sub-
20 sections (c) through (e).

21 “(c) TRANSPARENCY.—Each manufacturer of a cov-
22 ered motor vehicle shall provide to each owner and lessee
23 of the covered motor vehicle a clear and conspicuous no-
24 tice, in clear and plain language, of any collection, trans-
25 mission, retention, or use of driving data collected from
26 the covered motor vehicle.

1 “(d) CONSUMER CONTROL.—

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

6 “(2) ACCESS TO NAVIGATION TOOLS.—If an
7 owner or lessee of a covered motor vehicle opts out
8 of the collection and retention of driving data under
9 paragraph (1), the owner or lessee shall not, to the
10 extent technically possible, lose access to any naviga-
11 tion tool or other feature or capability.

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

19 “(e) LIMITATION ON USE OF PERSONAL DRIVING IN-
20 FORMATION.—

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

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

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

5 “(A) shall be clear and conspicuous;

6 “(B) shall be made in clear and plain lan-
7 guage; and

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

11 “(f) ENFORCEMENT.—A violation of this section shall
12 be treated as a violation of a rule defining an unfair or
13 deceptive act or practice prescribed under section
14 18(a)(1)(B).”.

15 (b) RULEMAKING.—

16 (1) IN GENERAL.—Not later than 18 months
17 after the date of enactment of this Act, the Federal
18 Trade Commission, after consultation with the Ad-
19 ministrator of the National Highway Traffic Safety
20 Administration (referred to in this subsection as the
21 “Administrator”), shall issue a notice of proposed
22 rulemaking, in accordance with section 553 of title
23 5, United States Code, to carry out section 27 of the
24 Federal Trade Commission Act.

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

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

11 (A) review the final regulations promul-
12 gated under paragraph (2); and

13 (B) update the final regulations as nec-
14 essary.

15 **SEC. 5. CYBERSECURITY TOOLS AND CYBER COORDI-**
16 **NATOR.**

17 (a) DEFINITIONS.—In this section:

18 (1) ADMINISTRATOR.—The term “Adminis-
19 trator” means the Administrator of the Federal
20 Highway Administration.

21 (2) CYBER INCIDENT.—The term “cyber inci-
22 dent” has the meaning given the term “significant
23 cyber incident” in Presidential Policy Directive–41
24 (July 26, 2016, relating to cyber incident coordina-
25 tion).

1 (3) TRANSPORTATION AUTHORITY.—The term
2 “transportation authority” means—

3 (A) a public authority (as defined in sec-
4 tion 101(a) of title 23, United States Code);

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

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

10 (D) a division office of the Federal High-
11 way Administration.

12 (b) CYBERSECURITY TOOL.—

13 (1) IN GENERAL.—Not later than 2 years after
14 the date of enactment of this Act, the Administrator
15 shall develop a tool to assist transportation authori-
16 ties in identifying, detecting, protecting against, re-
17 sponding to, and recovering from cyber incidents.

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

20 (A) use the cybersecurity framework estab-
21 lished by the National Institute of Standards
22 and Technology and required by Executive
23 Order 13636 of February 12, 2013 (78 Fed.
24 Reg. 11739; relating to improving critical infra-
25 structure cybersecurity);

1 (B) establish a structured cybersecurity as-
2 sessment and development program;

3 (C) consult with appropriate transportation
4 authorities, operating agencies, industry stake-
5 holders, and cybersecurity experts; and

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

8 (e) DESIGNATION OF CYBER COORDINATOR.—

9 (1) IN GENERAL.—Not later than 2 years after
10 the date of enactment of this Act, the Administrator
11 shall designate an office as a “cyber coordinator”,
12 which shall be responsible for monitoring, alerting,
13 and advising transportation authorities of cyber inci-
14 dents.

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

17 (A) provide to transportation authorities a
18 secure method of notifying a single Federal en-
19 tity of cyber incidents;

20 (B) monitor cyber incidents that affect
21 transportation authorities;

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

1 (D) investigate unaddressed cyber inci-
2 dents that affect transportation authorities; and

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