

116TH CONGRESS
1ST SESSION

S. 2398

To amend the Federal Election Campaign Act of 1971 to ensure privacy
with respect to voter information.

IN THE SENATE OF THE UNITED STATES

JULY 31, 2019

Mrs. FEINSTEIN introduced the following bill; which was read twice and
referred to the Committee on Rules and Administration

A BILL

To amend the Federal Election Campaign Act of 1971 to
ensure privacy with respect to voter information.

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 “Voter Privacy Act of
5 2019”.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

8 (1) According to the Pew Research Center, 90
9 percent of Americans reported using the internet in

1 2019, which was an increase from 52 percent in
2 2000.

3 (2) Internet service providers, browsers,
4 websites, search engines, email providers, device
5 manufacturers, and certain social media companies
6 collect unique data on nearly every American's on-
7 line and increasingly offline activities, every day.

8 (3) One United States based search engine ad-
9 vertises its ability to track hundreds of categories of
10 data about specific individuals including age, gender,
11 occupation, income level, sexual orientation, national
12 origin, religion, medical conditions such as AIDs,
13 erectile dysfunction, bipolar disorder, eating dis-
14 orders, and sexually transmitted diseases, family in-
15 formation such as number of children, children with
16 special needs, infertility, and substance misuse, and
17 support for social issues such as reproductive rights,
18 unions and labor issues, and support for gun rights.

19 (4) Targeting services, such as certain large
20 search engines and social media platforms, maintain
21 sophisticated data profiles on nearly every American.
22 These targeting services are used by third parties to
23 target and deliver communications to specific indi-
24 viduals based on their sensitive personal information,

1 even if a third party does not control any individ-
2 ual's personal information.

3 (5) In testimony before the Committee on the
4 Judiciary of the Senate titled, "Understanding Dig-
5 ital Advertising Ecosystem and the Impact on Data
6 Privacy", the Committee received the following testi-
7 mony regarding behavioral advertising: "almost
8 every single time you visit a website: data about you
9 is broadcast to tens or hundreds of companies, which
10 lets advertisers compete for the opportunity to show
11 you an ad. Advertising is necessary, and this sounds
12 OK. But wait until you hear what information about
13 you is in that big broadcast: it can include your –
14 inferred sexual orientation, political views, whether
15 you are Christian, Jewish, or Muslim, etc., whether
16 you have AIDs, erectile dysfunction, or bi-polar dis-
17 order. It includes what you are reading, watching,
18 and listening to. It includes your location, sometimes
19 right up to your exact GPS coordinates. And it in-
20 cludes unique ID codes that are as specific to you
21 as is your social security number, so that all of this
22 data can be tied to you over time. This allows com-
23 panies you have never heard of to maintain intimate
24 profiles on you, and on everyone you have ever
25 known."

1 (6) Online surveillance techniques are becoming
 2 more sophisticated. According to the Center for In-
 3 formation Technology Policy at Princeton Univer-
 4 sity, new website tracking software can provide real-
 5 time surveillance of an individual's online activity:
 6 “Unlike typical analytics services, that provide ag-
 7 gregate statistics, these scripts are intended for re-
 8 cording and playback of individual browsing ses-
 9 sions, as if someone is looking over your shoulder.”.

10 (7) The volume of data now publicly available
 11 and attributable to a specific individual permits re-
 12 searchers to infer private information about that in-
 13 dividual that the individual never disclosed publicly.

14 (8) According to a study from researchers at
 15 Cambridge University and Microsoft Research, an
 16 individual's social media posts, pictures, and profile
 17 information can be combined to reliably infer that
 18 individual's latent personality traits, including open-
 19 ness, conscientiousness, extraversion, agreeableness,
 20 and neuroticism. Prior to internet-based data track-
 21 ing, the only way to obtain that type of sensitive
 22 psychological data would have been for an individual
 23 to elect to respond to a detailed personality question-
 24 naire.

1 (9) According to a study published by the Na-
 2 tional Academy of Sciences, computers can predict
 3 an individual's latent personality traits better than
 4 humans. Specifically, researchers found that a com-
 5 puter needed only 10 social media impressions to
 6 better predict an individual's responses to a person-
 7 ality questionnaire than a coworker, 70 for a cohabi-
 8 tant or friend, 150 for a family member, and 300
 9 for a spouse.

10 (10) Communications tailored to an individual's
 11 unique personality traits are designed to manipulate
 12 cognitive function rather than to persuade via ap-
 13 peals to rational decision making. A forthcoming
 14 publication by Julie E. Cohen titled "Between Truth
 15 and Power" describes the phenomenon as follows
 16 "The operation of the digital information environ-
 17 ment has begun to mimic the operation of the collec-
 18 tion of brain structures that mid-twentieth-century
 19 neurologists christened the limbic system and that
 20 play vital roles in a number of precognitive func-
 21 tions, including emotion, motivation, and habit-for-
 22 mation," and observed that "today's networked in-
 23 formation flows are optimized to produce what social
 24 psychologist Shoshana Zuboff calls instrumentarian
 25 power: They employ a radical behaviorist approach

1 to human psychology to mobilize and reinforce pat-
2 terns of motivation, cognition, and behavior that op-
3 erate on automatic, near-instinctual levels and that
4 may be manipulated instrumentally”.

5 (11) According to numerous studies, messages
6 tailored to an individual’s unique personality traits
7 are materially more effective at altering an individ-
8 ual’s behavior.

9 (12) A recent study published in the National
10 Academy of Sciences found that it is possible to con-
11 duct psychological manipulation efforts online that
12 are targeted and customized to each individual’s
13 unique personality traits on a national scale.

14 (13) Candidates, campaigns, and political orga-
15 nizations are increasingly using online data to infer
16 personality traits and other psychological character-
17 istics regarding specific United States persons, using
18 that nonpublic information to target psychologically
19 manipulative communications and using algorithms
20 and other automated processes to automatically re-
21 fine communications over time to improve their ef-
22 fectiveness.

23 (14) According to a study titled “Voter Privacy
24 in the Age of Big Data”, political entities “assemble
25 a vast array of [personally identifiable information]

1 into detailed dossiers on practically every American
2 voter in order to target voters with individualized
3 messages . . . Most voters are ignorant of the steps
4 taken to create these dossiers and know even less
5 about related targeting practices.”.

6 (15) The study further found that “Political
7 databases hold records on almost 200 million eligible
8 American voters. Each records contains hundreds if
9 not thousands of fields derived from voter rolls,
10 donor and response data, campaign web data, and
11 consumer and other data obtained from data bro-
12 kers, all of which is combined into a giant assem-
13 blage . . . Ubiquitous personal identifiers (name,
14 address, telephone numbers, email addresses, IP ad-
15 dresses, cookies, mobile devices IDs, and other
16 unique IDs) allow campaigns to link and integrate
17 these diverse data sets, while data mining and so-
18 phisticated statistical techniques allow them to en-
19 gage in highly strategic and cost-effective analysis
20 and targeting,” and that “Campaign insiders and
21 paid consultants who not only view voter microtar-
22 geting as highly effective but also have assigned it
23 a crucial role in determining the outcome of the past
24 three presidential campaigns.”.

1 (16) The political consulting firm Cambridge
2 Analytica reportedly used a database of 220,000,000
3 Americans, including thousands of unique data
4 points on each individual and inferred personality
5 trait analysis, to conduct “psychological operations
6 changing people’s minds not through persuasion but
7 through ‘informational dominance’, a set of tech-
8 niques that includes rumor, disinformation and fake
9 news”. Cambridge Analytica reportedly worked in 44
10 United States elections in 2014 and another 50 in
11 2016, including on behalf of 2 major Presidential
12 campaigns.

13 (17) In *Sorrell v. IMS Health Inc.*, the Su-
14 preme Court invalidated a Vermont State law re-
15 garding restrictions on the use of personal informa-
16 tion as violating the First Amendment. The court
17 held that the government’s prohibition “disfavor[ed]
18 . . . speech with a particular content,” namely mar-
19 keting, and “disfavor[ed] specific speakers, namely
20 pharmaceutical manufacturers” because it interfered
21 with the manufacturers’ attempts to persuade recipi-
22 ents to use their products. Psychological targeting
23 techniques seek to manipulate, not to persuade.

24 (18) In *Citizens United v. FEC*, the Supreme
25 Court invalidated the Federal Election Campaign

1 Act’s prohibition on corporate independent expendi-
2 tures on the grounds that “the First Amendment
3 does not allow political speech restrictions based on
4 a speaker’s corporate identity”. Allowing individuals
5 to control the use of their own personal information
6 in the context of an election does not restrict the po-
7 litical speech of any person based on their identity.

8 (19) In *Buckley v. Valeo*, the Supreme Court
9 invalidated the Federal Election Campaign Act’s ex-
10 penditure limitations, finding that they “impose di-
11 rect and substantial restraints on the quantity of po-
12 litical speech”. Allowing individuals to control the
13 use of their own personal information in the context
14 of an election does not limit the any person’s quan-
15 tity of political speech.

16 **SEC. 3. SENSE OF CONGRESS.**

17 It is the sense of Congress that—

18 (1) the Federal Government has a compelling
19 interest in protecting voters from surveillance and
20 manipulation; and

21 (2) the Voter Privacy Act of 2019 is the most
22 narrowly tailored approach to protecting voters from
23 psychological manipulation online, however the Fed-
24 eral Government’s interest would justify additional
25 prohibitions if this Act is insufficient.

1 **SEC. 4. VOTER DATA PRIVACY.**

2 (a) IN GENERAL.—Title III of the Federal Election
3 Campaign Act of 1971 (52 U.S.C. 30101) is amended by
4 adding at the end the following new subtitle:

5 **“Subtitle B—Privacy of Voter’s**
6 **Personal Information**

7 **“SEC. 351. DEFINITIONS.**

8 “In this subtitle:

9 “(1) COVERED ENTITY.—The term ‘covered en-
10 tity’ means—

11 “(A) any candidate, political committee,
12 national committee, connected organization, or
13 political party (as those terms are defined in
14 section 301);

15 “(B) any political organization under sec-
16 tion 527 of the Internal Revenue Code of 1986;
17 and

18 “(C) any person that obtains an individ-
19 ual’s personal information for the purpose of
20 conducting—

21 “(i) a public communication as de-
22 fined in section 301(22), except for pur-
23 poses of this subtitle such term includes a
24 communication by means of any paid inter-
25 net or paid digital communication;

1 “(ii) an electioneering communication
2 as defined in section 304(f)(3);

3 “(iii) any communication that would
4 be an electioneering communication as de-
5 fined in such section if such section were
6 applied—

7 “(I) by taking into account com-
8 munications made over the internet;

9 “(II) without regard to subpara-
10 graph (A)(i)(III) of such section with
11 respect to communications described
12 in subclause (I) of this clause; and

13 “(III) by treating the facilities of
14 any online or digital newspaper, mag-
15 azine, blog, publication, or periodical
16 in the same manner as the facilities of
17 a broadcasting station for purposes of
18 subparagraph (B)(i) of such section;

19 “(iv) an independent expenditure as
20 defined in section 301(17); or

21 “(v) a generic campaign activity as
22 defined in section 301(21).

23 “(2) TARGETING SERVICE.—The term ‘tar-
24 geting service’ means any interactive computer serv-
25 ice, as defined in section 230(f)(2) of the Commu-

1 nications Act of 1934 (42 U.S.C. 230(f)(2)), that al-
2 lows a third party to target communications to an
3 individual based on that individual’s personal infor-
4 mation.

5 “(3) INDIVIDUAL.—The term ‘individual’ means
6 a natural person, however identified, including by
7 any unique identifier.

8 “(4) PERSONAL INFORMATION.—

9 “(A) IN GENERAL.—Subject to subpara-
10 graph (B), the term ‘personal information’
11 means information that identifies, relates to,
12 describes, is capable of being associated with, or
13 could reasonably be linked, directly or indi-
14 rectly, with a particular individual or household
15 that includes—

16 “(i) identifiers such as internet pro-
17 tocol address, email address, account
18 name, social security number, driver’s li-
19 cense number, passport number, or other
20 similar identifiers;

21 “(ii) characteristics of any protected
22 class under title VII of the Civil Rights Act
23 of 1964 (42 U.S.C. 2000e et seq.);

24 “(iii) commercial information, includ-
25 ing records of personal property, products

1 or services purchased, obtained, or consid-
2 ered, or other purchasing or consuming
3 histories or tendencies;

4 “(iv) biometric information;

5 “(v) internet or other electronic net-
6 work activity information, including brows-
7 ing history, search history, and informa-
8 tion regarding consumer’s interaction with
9 an internet website, application, or adver-
10 tisement;

11 “(vi) geolocation data;

12 “(vii) health insurance information;

13 “(viii) audio, electronic, visual, ther-
14 mal, olfactory, or similar information;

15 “(ix) professional or employment-re-
16 lated information;

17 “(x) education information; and

18 “(xi) inferences drawn from any of
19 the information identified in this subpara-
20 graph to create a profile regarding an indi-
21 vidual reflecting the individual’s pref-
22 erences, characteristics, psychological
23 traits, psychographic modeling, predisposi-
24 tions, behavior, attitudes, intelligence,
25 abilities, and aptitudes.

1 “(B) EXCLUSIONS.—

2 “(i) IN GENERAL.—The term ‘per-
3 sonal information’ does not include the fol-
4 lowing:

5 “(I) Publicly available informa-
6 tion.

7 “(II) Deidentified information.

8 “(III) Aggregate polling informa-
9 tion.

10 “(ii) DEFINITIONS.—For purposes of
11 clause (i):

12 “(I) PUBLICLY AVAILABLE IN-
13 FORMATION.—The term ‘publicly
14 available information’ means informa-
15 tion obtained from a Federal, State,
16 or local voter registration database
17 that is lawfully made available to the
18 public.

19 “(II) DEIDENTIFIED INFORMA-
20 TION.—The term ‘deidentified infor-
21 mation’ means information that can-
22 not reasonably identify, relate to, de-
23 scribe, be capable of being associated
24 with, or be linked, directly or indi-
25 rectly, to a particular individual.

1 “(III) AGGREGATE POLLING IN-
2 FORMATION.—The term ‘aggregate
3 polling information’ means informa-
4 tion that relates to a group or cat-
5 egory of individuals, from which indi-
6 vidual identities have been removed,
7 that is not linked or reasonably
8 linkable to any known individual, in-
9 cluding via a device or other unique
10 identifier.

11 “(5) BIOMETRIC INFORMATION.—The term ‘bi-
12 ometric information’ means an individual’s physio-
13 logical, biological, or behavioral characteristics, in-
14 cluding an individual’s deoxyribonucleic acid (DNA),
15 that can be used, singly or in combination with each
16 other or with other identifying data, to establish in-
17 dividual identity. Biometric information includes im-
18 agery of the iris, retina, fingerprint, face, hand,
19 palm, vein patterns, and voice recordings, from
20 which an identifier template, such as a faceprint, a
21 minutiae template, or a voiceprint, can be extracted,
22 and keystroke patterns or rhythms, and sleep,
23 health, or exercise data that contain identifying in-
24 formation.

1 “(6) HEALTH INSURANCE INFORMATION.—The
2 term ‘health insurance information’ means an indi-
3 vidual’s insurance policy number or subscriber iden-
4 tification number, any unique identifier used by a
5 health insurer to identify a person, or any informa-
6 tion in the individual’s application and claims his-
7 tory.

8 “(7) CATEGORIES OF PERSONAL INFORMA-
9 TION.—The term ‘categories of personal informa-
10 tion’ means the enumerated categories of informa-
11 tion described in clauses (i) through (xi) of para-
12 graph (4)(A), except as modified pursuant to regula-
13 tions or guidance of the Commission pursuant to
14 section 359(b).

15 “(8) VERIFIABLE REQUEST.—The term
16 ‘verifiable request’ means a request made by an indi-
17 vidual that a covered entity can reasonably verify,
18 pursuant to regulations adopted by the Commission
19 pursuant to section 359, to be the individual about
20 whom the covered entity has collected information.

21 “(9) COLLECT OR COLLECTED.—The terms
22 ‘collect’ or ‘collected’ mean, with respect to an indi-
23 vidual, any personal information that is gathered di-
24 rectly from that individual.

1 “(10) RECEIVED.—The term ‘received’ means
2 any individual’s personal information that is not col-
3 lected by a covered entity directly from that indi-
4 vidual, including any personal information that is
5 bought, rented, licensed, acquired, or accessed, by a
6 covered entity from any third party.

7 “(11) OBTAINED.—The term ‘obtained’ means
8 any personal information that is either collected or
9 received.

10 “(12) PROCESSING.—The term ‘processing’
11 means any operation or set of operations that are
12 performed on personal information or on sets of per-
13 sonal information, whether or not by automated
14 means.

15 “(13) THIRD PARTY.—The term ‘third party’
16 means a person who is not—

17 “(A) the person that collects an individ-
18 ual’s personal information directly from that in-
19 dividual; or

20 “(B) a person to whom a covered entity
21 discloses an individual’s personal information
22 for processing pursuant to a written contract,
23 provided that the contract prohibits the person
24 receiving the personal information from—

1 “(i) selling or transferring the per-
 2 sonal information to a third party; or

3 “(ii) retaining, using, or disclosing the
 4 personal information for any purpose other
 5 than for the specific purpose of performing
 6 the services specified in the written con-
 7 tract.

8 **“SEC. 352. VOTER’S RIGHT OF ACCESS.**

9 “(a) IN GENERAL.—An individual shall have the
 10 right to direct a covered entity that obtains an individual’s
 11 personal information to disclose to that individual the cat-
 12 egories of personal information and specific pieces of per-
 13 sonal information the covered entity has obtained with re-
 14 spect to the individual.

15 “(b) REQUIREMENT.—A covered entity that receives
 16 a verifiable request from an individual to access that indi-
 17 vidual’s personal information pursuant to subsection (a),
 18 shall provide the requested information in accordance with
 19 subsection (e).

20 “(c) VERIFIABLE REQUEST.—A covered entity shall
 21 provide the information specified in subsection (a) only
 22 upon receipt of a verifiable request.

23 “(d) TIMING.—A covered entity shall comply with all
 24 verifiable requests made pursuant to subsection (a) within

1 a reasonable period after receiving such a request, but not
2 later than 10 calendar days after receiving such a request.

3 “(e) CONTENTS.—Each request under subsection (a),
4 with respect to the personal information of the requesting
5 individual, shall include the following:

6 “(1) The categories of personal information ob-
7 tained regarding that individual.

8 “(2) The specific sources from which the per-
9 sonal information was obtained.

10 “(3) The specific third party or third parties to
11 whom the personal information has been transferred
12 or disclosed.

13 “(4) The period for which the personal informa-
14 tion will be stored by the covered entity.

15 “(5) The existence of the right of an individual
16 to request a copy of that individual’s specific pieces
17 of personal information under subsection (f).

18 “(6) The existence of the right of an individual
19 to request erasure of that individual’s personal infor-
20 mation under section 353.

21 “(7) The existence of the right to request prohi-
22 bition of the transfer of personal information to any
23 third party under section 354.

24 “(8) Information regarding the right to lodge a
25 complaint with the Commission under section 309(a)

1 as described in section 356 regarding any potential
2 violation of this subtitle.

3 “(f) SPECIFIC PIECES OF PERSONAL INFORMA-
4 TION.—In addition to the information provided under sub-
5 section (e), upon specific, verifiable request an individual
6 shall have the right to access all of that individual’s spe-
7 cific pieces of personal information obtained by a covered
8 entity.

9 “(g) FORMAT.—A covered entity shall provide infor-
10 mation as required under this section to the requesting
11 individual in a concise, and easily accessible form, using
12 clear and plain language. The information required under
13 this subsection may be delivered by mail or electronic mail,
14 or made available via a secured internet website.

15 “(h) COST.—A covered entity that receives a
16 verifiable request from an individual shall provide informa-
17 tion required under this section free of charge.

18 “(i) LIMITATION.—A covered entity shall not be re-
19 quired to provide an individual’s personal information to
20 the individual pursuant to this section more than two
21 times in a 12-month period.

22 “(j) PROHIBITION ON THIRD-PARTY REQUESTS.—
23 No third party shall submit a verifiable request to a cov-
24 ered entity on behalf of another individual. No individual

1 may authorize a third party to submit a verifiable request
 2 to a covered entity on their behalf.

3 **“SEC. 353. VOTER’S RIGHT OF ERASURE.**

4 “(a) IN GENERAL.—An individual shall have the
 5 right to direct a covered entity to delete any of that indi-
 6 vidual’s personal information obtained by a covered entity.

7 “(b) REQUIREMENT.—A covered entity that receives
 8 a verifiable request to delete an individual’s personal infor-
 9 mation pursuant to subsection (a)—

10 “(1) shall immediately cease processing such
 11 personal information, and as soon as practicable,
 12 permanently delete such information, except as pro-
 13 vided under subsections (c), (d), and (e); and

14 “(2) shall not, unless the covered entity receives
 15 written authorization from the individual, re-collect
 16 or otherwise obtain any of the individual’s personal
 17 information, except as provided under such sub-
 18 sections.

19 “(c) LIMITATION.—The requirement to delete per-
 20 sonal information in subsection (b) does not apply to pub-
 21 licly available information as defined in this subtitle.

22 “(d) RECORDS.—Notwithstanding subsections (a)
 23 and (b), a covered entity shall maintain such personal in-
 24 formation as is necessary to maintain adequate records of
 25 a request to delete information under subsection (a) or

1 to comply with section 352(e)(3) and section 354 of this
 2 subtitle. Any personal information retained consistent with
 3 this subsection shall not be processed for any other pur-
 4 pose, and shall be reviewable by the Commission.

5 “(e) CONFIRMATION.—A covered entity shall provide
 6 confirmation to the individual requesting deletion of per-
 7 sonal information under subsection (a) not later than 5
 8 days following the deletion of the information.

9 **“SEC. 354. VOTER’S RIGHT TO PROHIBIT TRANSFER.**

10 “(a) IN GENERAL.—An individual shall have the
 11 right to direct a covered entity not to sell or otherwise
 12 transfer any of that individual’s personal information ob-
 13 tained by a covered entity to any third party.

14 “(b) REQUIREMENT.—A covered entity that receives
 15 a verifiable request from an individual not to transfer that
 16 individual’s personal information pursuant to subsection
 17 (a), shall not transfer that personal information directly
 18 or indirectly to a third party.

19 “(c) NOTICE.—A covered entity that seeks to sell or
 20 transfer an individual’s personal information to any third
 21 party shall provide notice as required under section
 22 355(b)(3).

23 “(d) RECORDS.—Notwithstanding section 353, a cov-
 24 ered entity shall retain sufficient records, including any
 25 necessary personal information, to determine whether an

1 individual has directed the covered entity not to transfer
 2 that individual's data to a third party. Any personal infor-
 3 mation retained pursuant to this section shall not be used
 4 for any other purpose, and shall be reviewable by the Com-
 5 mission.

6 “(e) PROHIBITION ON TRANSFER OVERSEAS.—

7 “(1) OFFENSE.—It shall be unlawful for any
 8 covered entity to knowingly transfer outside of the
 9 United States any individual's personal information,
 10 publicly available information, or anonymized infor-
 11 mation as defined in this subtitle.

12 “(2) PENALTY.—Any person who violates para-
 13 graph (1) shall be fined under title 18, United
 14 States Code, imprisoned not more than 3 years, or
 15 both.

16 **“SEC. 355. NOTICE OF RECEIPT OF VOTER'S PERSONAL IN-**
 17 **FORMATION.**

18 “(a) NOTICE.—A covered entity that receives any in-
 19 dividual's personal information from a third party shall
 20 inform such individual as to the scope and purpose of re-
 21 ceiving such personal information.

22 “(b) TIMING.—A covered entity shall provide notice
 23 required in subsection (a) to an individual within a reason-
 24 able period after receiving that individual's personal infor-
 25 mation, but not later than—

1 “(1) except as provided in paragraphs (2) and
 2 (3), 30 days after receiving such information, or if
 3 personal information is received in an anonymized
 4 format then 30 days after the personal information
 5 is connected to an identifiable individual;

6 “(2) if the personal information is to be used
 7 for a communication or targeted advertisement with
 8 an individual, at the time of the first communication
 9 with that individual; and

10 “(3) if the personal information is to be trans-
 11 ferred or sold to a third party, 14 days prior to that
 12 transfer or sale.

13 “(c) CONTENTS.—Notice required under subsection
 14 (a) shall include the following:

15 “(1) The identity and the contact information
 16 of the covered entity.

17 “(2) The categories of personal information re-
 18 ceived.

19 “(3) The purposes for which the personal infor-
 20 mation was received.

21 “(4) The period for which the personal informa-
 22 tion will be retained.

23 “(5) The existence of the right to request from
 24 the covered entity access to all specific pieces of per-
 25 sonal information under section 352(f).

1 “(6) The existence of the right of an individual
2 to request erasure of all that individual’s personal
3 information obtained by a covered entity under sec-
4 tion 353.

5 “(7) The existence of the right of an individual
6 to prohibit the transfer of that individual’s personal
7 information to a third party under section 354.

8 “(8) Information regarding the right to lodge a
9 complaint with the Commission under section 309(a)
10 as described in section 357 regarding any violation
11 of this subtitle.

12 “(d) FORMAT.—Notice required under subsection (a)
13 shall be provided in a concise and easily accessible form,
14 using clear and plain language.

15 “(e) COST.—Notice required under subsection (a)
16 shall be provided at no cost to any individual with respect
17 to whom a covered entity has received personal informa-
18 tion.

19 “(f) ADDITIONAL NOTICE.—A covered entity shall
20 not receive additional categories of personal information,
21 process personal information for an additional purpose, or
22 transfer personal information to an additional third party
23 without providing such persons notice consistent with this
24 section.

1 **“SEC. 356. VOTER’S RIGHT TO PROHIBIT TARGETING BASED**
2 **ON PERSONAL INFORMATION.**

3 “(a) IN GENERAL.—An individual shall have the
4 right to prohibit a targeting service from using that indi-
5 vidual’s personal information to deliver targeted commu-
6 nications to that individual—

7 “(1) on behalf of a covered entity; and

8 “(2) on behalf of all covered entities.

9 “(b) REQUIREMENT.—A targeting service that re-
10 ceives a verifiable request pursuant to paragraph (1) or
11 (2) of subsection (a)—

12 “(1) shall immediately cease providing access,
13 use, or processing of that individual’s personal infor-
14 mation to any or all covered entities with respect to
15 which such request is made, including for use in de-
16 livering targeted communications to that individual
17 based on that individual’s personal information; and

18 “(2) shall not provide any future access, use, or
19 processing of that individual’s personal information
20 to any or all covered entities with respect to which
21 such request is made, including for use in delivering
22 targeted communications to that individual based on
23 their personal information without express written
24 permission from that individual.

25 “(c) NOTICE.—

26 “(1) IN GENERAL.—

1 “(A) NOTICE BY COVERED ENTITY.—A
2 covered entity shall provide notice to a tar-
3 geting service of the covered entity’s status as
4 a covered entity under this subtitle, prior to ac-
5 cessing, using, or processing any individual’s
6 personal information provided by the targeting
7 service.

8 “(B) NOTICE BY TARGETING SERVICE.—A
9 targeting service shall provide notice to any in-
10 dividual whose personal information is accessed,
11 used, or processed, including for use in deliv-
12 ering a targeted communication based on that
13 individual’s personal information, by a covered
14 entity.

15 “(2) CONTENTS.—Notice required under para-
16 graph (1)(B) shall include—

17 “(A) the identity and the contact informa-
18 tion for the targeting service;

19 “(B) the identity and the contact informa-
20 tion of the covered entity;

21 “(C) the categories of personal information
22 accessed, used, or otherwise made available to a
23 covered entity, including any personal informa-
24 tion used to target an advertisement or other

1 information to that individual on behalf of a
2 covered entity; and

3 “(D) information on the right of an indi-
4 vidual to prohibit a covered entity or all covered
5 entities from using a targeting service to deliver
6 advertisements or other information to that in-
7 dividual based on that individual’s personal in-
8 formation under this section.

9 “(3) TIMING.—Notice required under para-
10 graph (1)(B) shall be provided by a targeting service
11 at the time of each targeted communication with an
12 individual by the targeting service on behalf of a
13 covered entity that is based on the individual’s per-
14 sonal information.

15 “(4) FORMAT.—Notice required under para-
16 graph (1)(B) shall be provided in a concise and eas-
17 ily accessible form, using clear and plain language.

18 “(d) CONFIRMATION.—A targeting service shall pro-
19 vide confirmation of an individual’s verifiable request to
20 prohibit targeted communications from a covered entity or
21 all covered entities based on that individual’s personal in-
22 formation not later than 3 days following receipt of a
23 verifiable request from that individual pursuant to sub-
24 section (a).

25 “(e) RECORDS.—

1 “(1) TARGETING SERVICE.—A targeting service
 2 shall maintain adequate records of any individual’s
 3 request under subsection (a) and, if applicable, any
 4 written permission provided under subsection (b)(2)
 5 to ensure such individuals do not receive targeted
 6 communications from a covered entity unless such
 7 written permission is provided.

8 “(2) COVERED ENTITY.—A covered entity shall
 9 maintain records of all notices provided to a tar-
 10 geting service as required under subsection
 11 (c)(1)(A).

12 “(3) REVIEW.—All records required under this
 13 subsection shall be reviewable by the Commission.

14 “(f) RULE OF CONSTRUCTION.—Nothing in this sec-
 15 tion shall be interpreted—

16 “(1) to prohibit a covered entity from using a
 17 targeting service to deliver information to an indi-
 18 vidual that is not based on that individual’s personal
 19 information; or

20 “(2) to prohibit a targeting service from using
 21 an individual’s personal information to deliver tar-
 22 geted communications to that individual on behalf of
 23 a third party that is not a covered entity.

1 **“SEC. 357. RIGHT TO LODGE A COMPLAINT.**

2 “An individual who believes a violation of this subtitle
3 has occurred may file a complaint with the Commission
4 pursuant to section 309(a).

5 **“SEC. 358. ENFORCEMENT.**

6 “Any person who knowingly and willfully commits a
7 violation of any provision of this subtitle shall be fined
8 under this title or imprisoned not more than 3 years, or
9 both.

10 **“SEC. 359. COMMISSION RULEMAKING.**

11 “(a) IN GENERAL.—Not later than 180 days after
12 the date of enactment of this subtitle, the Commission
13 shall conduct a rulemaking to implement the requirements
14 of this subtitle, including to provide guidance on the defi-
15 nition of a ‘verifiable request’, which will ensure individ-
16 uals can exercise their rights under this subtitle in a se-
17 cure manner.

18 “(b) UPDATING AS NEEDED.—The Commission shall
19 produce and update as needed guidance and regulations
20 relating to adding categories of personal information for
21 purposes of this subtitle in addition to those described in
22 section 351(4)(A), in order to address changes in tech-
23 nology, data practices of covered entities, and privacy con-
24 cerns.”.

25 (b) SEVERABILITY.—If any provision of this Act or
26 amendment made by this Act, or the application of a pro-

1 vision or amendment to any person or circumstance, is
2 held to be unconstitutional, the remainder of this Act and
3 amendments made by this Act, and the application of the
4 provisions and amendment to any person or circumstance,
5 shall not be affected by the holding.

6 (c) EFFECTIVE DATE.—The amendments made by
7 this Act shall apply with respect to personal information
8 obtained, stored, or processed on or after 360 days after
9 the date of enactment of this Act, and shall take effect
10 without regard to whether or not the Federal Election
11 Commission has promulgated regulations to carry out
12 such amendments.

○