116TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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

A BILL

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

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 ''Voter Privacy Act of 2019''.

SEC. 2. FINDINGS.

Congress makes the following findings:

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

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

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

(3) One United States based search engine advertises its ability to track hundreds of categories of data about specific individuals including age, gender, occupation, income level, sexual orientation, national origin, religion, medical conditions such as AIDs, erectile dysfunction, bipolar disorder, eating disorders, and sexually transmitted diseases, family information such as number of children, children with special needs, infertility, and substance misuse, and support for social issues such as reproductive rights, unions and labor issues, and support for gun rights.

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

even if a third party does not control any individual's personal information.

(5) In testimony before the Committee on the Judiciary of the Senate titled, ''Understanding Digital Advertising Ecosystem and the Impact on Data Privacy'', the Committee received the following testimony regarding behavioral advertising: ''almost every single time you visit a website: data about you is broadcast to tens or hundreds of companies, which lets advertisers compete for the opportunity to show you an ad. Advertising is necessary, and this sounds OK. But wait until you hear what information about you is in that big broadcast: it can include your – inferred sexual orientation, political views, whether you are Christian, Jewish, or Muslim, etc., whether you have AIDs, erectile dysfunction, or bi-polar disorder. It includes what you are reading, watching, and listening to. It includes your location, sometimes right up to your exact GPS coordinates. And it includes unique ID codes that are as specific to you as is your social security number, so that all of this data can be tied to you over time. This allows companies you have never heard of to maintain intimate profiles on you, and on everyone you have ever known.''.

(6) Online surveillance techniques are becoming more sophisticated. According to the Center for Information Technology Policy at Princeton University, new website tracking software can provide real-time surveillance of an individual's online activity: ''Unlike typical analytics services, that provide aggregate statistics, these scripts are intended for recording and playback of individual browsing sessions, as if someone is looking over your shoulder.''.

(7) The volume of data now publicly available and attributable to a specific individual permits researchers to infer private information about that individual that the individual never disclosed publicly.

(8) According to a study from researchers at Cambridge University and Microsoft Research, an individual's social media posts, pictures, and profile information can be combined to reliably infer that individual's latent personality traits, including openness, conscientiousness, extraversion, agreeableness, and neuroticism. Prior to internet-based data tracking, the only way to obtain that type of sensitive psychological data would have been for an individual to elect to respond to a detailed personality questionnaire.

(9) According to a study published by the National Academy of Sciences, computers can predict an individual's latent personality traits better than humans. Specifically, researchers found that a computer needed only 10 social media impressions to better predict an individual's responses to a personality questionnaire than a coworker, 70 for a cohabitant or friend, 150 for a family member, and 300 for a spouse.

(10) Communications tailored to an individual's unique personality traits are designed to manipulate cognitive function rather than to persuade via appeals to rational decision making. A forthcoming publication by Julie E. Cohen titled ''Between Truth and Power'' describes the phenomenon as follows ''The operation of the digital information environment has begun to mimic the operation of the collection of brain structures that mid-twentieth-century neurologists christened the limbic system and that play vital roles in a number of precognitive functions, including emotion, motivation, and habit-formation,'' and observed that ''today's networked information flows are optimized to produce what social psychologist Shoshana Zuboff calls instrumentarian power: They employ a radical behaviorist approach

to human psychology to mobilize and reinforce patterns of motivation, cognition, and behavior that operate on automatic, near-instinctual levels and that may be manipulated instrumentally''.

(11) According to numerous studies, messages tailored to an individual's unique personality traits are materially more effective at altering an individual's behavior.

(12) A recent study published in the National Academy of Sciences found that it is possible to conduct psychological manipulation efforts online that are targeted and customized to each individual's unique personality traits on a national scale.

(13) Candidates, campaigns, and political organizations are increasingly using online data to infer personality traits and other psychological characteristics regarding specific United States persons, using that nonpublic information to target psychologically manipulative communications and using algorithms and other automated processes to automatically refine communications over time to improve their effectiveness.

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

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

(15) The study further found that ''Political databases hold records on almost 200 million eligible American voters. Each records contains hundreds if not thousands of fields derived from voter rolls, donor and response data, campaign web data, and consumer and other data obtained from data brokers, all of which is combined into a giant assemblage . . . Ubiquitous personal identifiers (name, address, telephone numbers, email addresses, IP addresses, cookies, mobile devices IDs, and other unique IDs) allow campaigns to link and integrate these diverse data sets, while data mining and sophisticated statistical techniques allow them to engage in highly strategic and cost-effective analysis and targeting,'' and that ''Campaign insiders and paid consultants who not only view voter microtargeting as highly effective but also have assigned it a crucial role in determining the outcome of the past three presidential campaigns.''.

(16) The political consulting firm Cambridge Analtyica reportedly used a database of 220,000,000 Americans, including thousands of unique data points on each individual and inferred personality trait analysis, to conduct ''psychological operations changing people's minds not through persuasion but through 'informational dominance', a set of techniques that includes rumor, disinformation and fake news.'' Cambridge Analytica reportedly worked in 44 United States elections in 2014 and another 50 in 2016, including on behalf of 2 major presidential campaigns.

(17) In Sorrell v. IMS Health Inc., the Supreme Court invalidated a Vermont State law regarding restrictions on the use of personal information as violating the First Amendment. The court held that the government's prohibition ''disfavor[ed] . . . speech with a particular content,'' namely marketing, and ''disfavor[ed] specific speakers, namely pharmaceutical manufacturers'' because it interfered with the manufacturers' attempts to persuade recipients to use their products. Psychological targeting techniques seek to manipulate, not to persuade.

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

Act's prohibition on corporate independent expenditures on the grounds that ''the First Amendment does not allow political speech restrictions based on a speaker's corporate identity''. Allowing individuals to control the use of their own personal information in the context of an election does not restrict the political speech of any person based on their identity.

(19) In Buckley v. Valeo, the Supreme Court invalidated the Federal Election Campaign Act's expenditure limitations, finding that they ''impose direct and substantial restraints on the quantity of political speech.'' Allowing individuals to control the use of their own personal information in the context of an election does not limit the any person's quantity of political speech.

SEC. 3. SENSE OF CONGRESS.

It is the sense of Congress that—

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

(2) the Voter Privacy Act of 2019 is the most narrowly tailored approach to protecting voters from psychological manipulation online, however the Federal Government's interest would justify additional prohibitions if this Act is insufficient.

SEC. 4. VOTER DATA PRIVACY.

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

"Subtitle B—Privacy of Voter's Personal Information

"SEC. 351. DEFINITIONS.

''In this subtitle:

''(1) COVERED ENTITY.—The term 'covered entity' means—

''(A) any candidate, political committee, national committee, connected organization, or political party (as those terms are defined in section 301);

''(B) any political organization under section 527 of the Internal Revenue Code of 1986;

''(C) any person that obtains an individual's personal information for the purpose of conducting—

''(i) a public communication as defined in section 301(22), except for purposes of this subtitle such term includes a communication by means of any paid internet or paid digital communication;

''(ii) an electioneering communication as defined in section 304(f)(3); or

"(iii) any communication that would be an electioneering communication as defined in such section if such section were applied—

"(I) by taking into account communications made over the internet;

"(II) without regard to subparagraph (A)(i)(III) of such section with respect to communications described in subclause (I) of this clause; and

"(III) by treating the facilities of any online or digital newspaper, magazine, blog, publication, or periodical in the same manner as the facilities of a broadcasting station for purposes of subparagraph (B)(i) of such section;

"(iv) an independent expenditure as defined in section 301(17); or

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

"(2) TARGETING SERVICE.—The term 'targeting service' means any interactive computer service, as defined in section 230(f)(2) of the Communications Act of 1934 (42 U.S.C. 230(f)(2)), that allows a third party to target communications to an

individual based on that individual's personal information.

"(3) INDIVIDUAL.—The term 'individual' means a natural person, however identified, including by any unique identifier.

"(4) PERSONAL INFORMATION.—

"(A) IN GENERAL.—Subject to subparagraph (B), the term 'personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household that includes—

"(i) identifiers such as internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

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

"(iii) commercial information, including records of personal property, products or services purchased, obtained, or consid-

ered, or other purchasing or consuming histories or tendencies;

''(iv) biometric information;

''(v) Internet or other electronic network activity information, including browsing history, search history, and information regarding consumer's interaction with an internet website, application, or advertisement;

''(vi) geolocation data;

''(vii) health insurance information;

''(viii) audio, electronic, visual, thermal, olfactory, or similar information;

''(ix) professional or employment-related information;

''(x) education information; and

''(xi) inferences drawn from any of the information identified in this subparagraph to create a profile regarding an individual reflecting the individual's preferences, characteristics, psychological traits, psychographic modeling, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

''(B) EXCLUSIONS.—

"(i) IN GENERAL.—The term 'personal information' does not include the following:

"(I) Publicly available information.

"(II) Deidentified information.

"(III) Aggregate polling information.

"(ii) DEFINITIONS.—For purposes of clause (i):

"(I) PUBLICLY AVAILABLE INFORMATION.—The term 'publicly available information' means information obtained from a Federal, State, or local voter registration database that is lawfully made available to the public.

"(II) DEIDENTIFIED INFORMATION.—The term 'deidentified information' means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual.

"(III) AGGREGATE POLLING INFORMATION.—The term 'aggregate polling information' means information that relates to a group or category of individuals, from which individual identities have been removed, that is not linked or reasonably linkable to any known individual, including via a device or other unique identifier.

"(5) BIOMETRIC INFORMATION.—The term 'biometric information' means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

''(6) HEALTH INSURANCE INFORMATION.—The term 'health insurance information' means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify a person, or any information in the individual's application and claims history.

''(7) CATEGORIES OF PERSONAL INFORMATION.—The term 'categories of personal information' means the enumerated categories of information described in clauses (i) through (xi) of paragraph (4)(A), except as modified pursuant to regulations or guidance of the Commission pursuant to section 359(b).

''(8) VERIFIABLE REQUEST.—The term 'verifiable request' means a request made by an individual that a covered entity can reasonably verify, pursuant to regulations adopted by the Commission pursuant to section 359, to be the individual about whom the covered entity has collected information.

''(9) COLLECT OR COLLECTED.—The terms 'collect' or 'collected' mean, with respect to an individual, any personal information that is gathered directly from that individual.

''(10) RECEIVED.—The term 'received' means any individual's personal information that is not collected by a covered entity directly from that individual, including any personal information that is bought, rented, licensed, acquired, or accessed, by a covered entity from any third party.

''(11) OBTAINED.—The term 'obtained' means any personal information that is either collected or received.

''(12) PROCESSING.—The term 'processing' means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

''(13) THIRD PARTY.—The term 'third party' means a person who is not—

''(A) the person that collects an individual's personal information directly from that individual; or

''(B) a person to whom a covered entity discloses an individual's personal information for processing pursuant to a written contract, provided that the contract prohibits the person receiving the personal information from—

''(i) selling or transferring the personal information to a third party; or

''(ii) retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the written contract.

''SEC. 352. VOTER'S RIGHT OF ACCESS.

''(a) IN GENERAL.—An individual shall have the right to direct a covered entity that obtains an individual's personal information to disclose to that individual the categories of personal information and specific pieces of personal information the covered entity has obtained with respect to the individual.

''(b) REQUIREMENT.—A covered entity that receives a verifiable request from an individual to access that individual's personal information pursuant to subsection (a), shall provide the requested information in accordance with subsection (e).

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

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

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

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

''(1) The categories of personal information obtained regarding that individual.

''(2) The specific sources from which the personal information was obtained.

''(3) The specific third party or third parties to whom the personal information has been transferred or disclosed.

''(4) The period for which the personal information will be stored by the covered entity.

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

''(6) The existence of the right of an individual to request erasure of that individual's personal information under section 353.

''(7) The existence of the right to request prohibition of the transfer of personal information to any third party under section 354.

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

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

''(f) SPECIFIC PIECES OF PERSONAL INFORMATION.—In addition to the information provided under subsection (e), upon specific, verifiable request an individual shall have the right to access all of that individual's specific pieces of personal information obtained by a covered entity.

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

''(h) COST.—A covered entity that receives a verifiable request from an individual shall provide information required under this section free of charge.

''(i) LIMITATION.—A covered entity shall not be required to provide an individual's personal information to the individual pursuant to this section more than two times in a 12–month period.

''(j) PROHIBITION ON THIRD PARTY REQUESTS.—No third party shall submit a verifiable request to a covered entity on behalf of another individual. No individual

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

"SEC. 353. VOTER'S RIGHT OF ERASURE.

"(a) IN GENERAL.—An individual shall have the right to direct a covered entity to delete any of that individual's personal information obtained by a covered entity.

"(b) REQUIREMENT.—A covered entity that receives a verifiable request to delete an individual's personal information pursuant to subsection (a)—

"(1) shall immediately cease processing such personal information, and as soon as practicable, permanently delete such information, except as provided under subsections (c), (d), and (e); and

"(2) shall not, unless the covered entity receives written authorization from the individual, re-collect or otherwise obtain any of the individual's personal information, except as provided under such subsections.

"(c) LIMITATION.—The requirement to delete personal information in subsection (b) does not apply to publicly available information as defined in this subtitle.

"(d) RECORDS.—Notwithstanding subsections (a) and (b), a covered entity shall maintain such personal information as is necessary to maintain adequate records of a request to delete information under subsection (a) or

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

''(e) CONFIRMATION.—A covered entity shall provide confirmation to the individual requesting deletion of personal information under section (a) not later than 5 days following the deletion of the information.

''SEC. 354. VOTER'S RIGHT TO PROHIBIT TRANSFER.

''(a) IN GENERAL.—An individual shall have the right to direct a covered entity not to sell or otherwise transfer any of that individual's personal information obtained by a covered entity to any third party.

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

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

''(d) RECORDS.—Notwithstanding section 353, a covered entity shall retain sufficient records, including any necessary personal information, to determine whether an

individual has directed the covered entity not to transfer that individual's data to a third party. Any personal information retained pursuant to this section shall not be used for any other purpose, and shall be reviewable by the Commission.

''(e) PROHIBITION ON TRANSFER OVERSEAS.—

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

''(2) PENALTY.—Any person who violates paragraph (1) shall be fined under title 18, United States Code, imprisoned not more than 3 years, or both.

''SEC. 355. NOTICE OF RECEIPT OF VOTER'S PERSONAL INFORMATION.

''(a) NOTICE.—A covered entity that receives any individual's personal information from a third party shall inform such individual as to the scope and purpose of receiving such personal information.

''(b) TIMING.—A covered entity shall provide notice required in subsection (a) to an individual within a reasonable period after receiving that individual's personal information, but not later than—

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

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

''(3) if the personal information is to be transferred or sold to a third party, 14 days prior to that transfer or sale.

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

''(1) The identity and the contact information of the covered entity.

''(2) The categories of personal information received.

''(3) The purposes for which the personal information was received.

''(4) The period for which the personal information will be retained.

''(5) The existence of the right to request from the covered entity access to all specific pieces of personal information under section 352(f).

''(6) The existence of the right of an individual to request erasure of all that individual's personal information obtained by a covered entity under section 353.

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

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

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

''(e) COST.—Notice required under subsection (a) shall be provided at no cost to any individual with respect to whom a covered entity has received personal information.

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

"SEC. 356. VOTER'S RIGHT TO PROHIBIT TARGETING BASED ON PERSONAL INFORMATION.

"(a) IN GENERAL.—An individual shall have the right to prohibit a targeting service from using that individual's personal information to deliver targeted communications to that individual—

"(1) on behalf of a covered entity; and

"(2) on behalf of all covered entities.

"(b) REQUIREMENT.—A targeting service that receives a verifiable request pursuant to subsection paragraph (1) or (2) of subsection (a)—

"(1) shall immediately cease providing access, use, or processing of that individual's personal information to any or all covered entities with respect to which such request is made, including for use in delivering targeted communications to that individual based on that individual's personal information; and

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

"(c) NOTICE.—

"(1) IN GENERAL.—

''(A) NOTICE BY COVERED ENTITY.—A covered entity shall provide notice to a targeting service of the covered entity's status as a covered entity under this subtitle, prior to accessing, using, or processing any individual's personal information provided by the targeting service.

''(B) NOTICE BY TARGETING SERVICE.—A targeting service shall provide notice to any individual whose personal information is accessed, used, or processed, including for use in delivering a targeted communication based on that individual's personal information, by a covered entity.

''(2) CONTENTS.—Notice required under paragraph (1)(B) shall include—

''(A) the identity and the contact information for the targeting service;

''(B) the identity and the contact information of the covered entity;

''(C) the categories of personal information accessed, used, or otherwise made available to a covered entity, including any personal information used to target an advertisement or other

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

"(D) information on the right of an individual to prohibit a covered entity or all covered entities from using a targeting service to deliver advertisements or other information to that individual based on that individual's personal information under this section.

"(3) TIMING.—Notice required under paragraph (1)(B) shall be provided by a targeting service at the time of each targeted communication with an individual by the targeting service on behalf of a covered entity that is based on the individual's personal information.

"(4) FORMAT.—Notice required under paragraph (1)(B) shall be provided in a concise and easily accessible form, using clear and plain language.

"(d) CONFIRMATION.—A targeting service shall provide confirmation of an individual's verifiable request to prohibit targeted communications from a covered entity or all covered entities based on that individual's personal information not later than 3 days following receipt of a verifiable request from that individual pursuant to subsection (a).

"(e) RECORDS.—

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

''(2) COVERED ENTITY.—A covered entity shall maintain records of all notices provided to a targeting service as required under subsection (c)(1)(A).

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

''(f) RULE OF CONSTRUCTION.—Nothing in this section shall be interpreted—

''(1) to prohibit a covered entity from using a targeting service to deliver information to an individual that is not based on that individual's personal information; or

''(2) to prohibit a targeting service from using an individual's personal information to deliver targeted communications to that individual on behalf of a third party that is not a covered entity.

"SEC. 357. RIGHT TO LODGE A COMPLAINT.

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

"SEC. 358. ENFORCEMENT.

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

"SEC. 359. COMMISSION RULEMAKING.

''(a) IN GENERAL.—Not later than 180 days after the date of enactment of this subtitle, the Commission shall conduct a rulemaking to implement the requirements of this subtitle, including to provide guidance on the definition of a 'verifiable request,' which will ensure individuals can exercise their rights under this subtitle in a secure manner.

''(b) UPDATING AS NEEDED.—The Commission shall produce and update as needed guidance and regulations relating to adding categories of personal information for purposes of this subtitle in addition to those described in section 351(4)(A), in order to address changes in technology, data practices of covered entities, and privacy concerns.''.

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

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

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