

118TH CONGRESS
1ST SESSION

H. R. 3045

To affirm user ownership of their data, prohibit entities from requiring the transfer or monetization of private data in exchange for services, prohibit the collection of third-party contact information without written consent, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 2, 2023

Mr. CLOUD introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To affirm user ownership of their data, prohibit entities from requiring the transfer or monetization of private data in exchange for services, prohibit the collection of third-party contact information without written consent, 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 “You Own the Data
5 Act” or “YODA”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) Governments exist to protect individual
2 rights to life, liberty, and property.

3 (2) The protection of civil liberties, including
4 the rights to private property and privacy from un-
5 warranted searches and seizures, is one of the hall-
6 marks of a free society.

7 (3) It is appropriate for Congress to enact laws
8 to protect individuals from data collection by third
9 parties.

10 (4) Data is the property of the user, as the user
11 creates the data.

12 (5) A user maintains ownership of the data of
13 such user, even when such data is sold or leased
14 with the consent of such user.

15 (6) Technology should empower the individual
16 and the productivity of the individual.

17 (7) Individuals should have reasonable access to
18 and use of popularly available consumer technologies
19 without abdicating the rights of such individuals to
20 privacy and anonymity.

21 **SEC. 3. PROHIBITION ON SHARING USER CONTACTS WITH-**
22 **OUT WRITTEN CONSENT AND CLARIFYING**
23 **USER ACCESS TO DATA.**

24 (a) PROHIBITION ON ACCESS TO USER CONTACTS.—
25 It shall be unlawful for a covered entity to ask a user to

1 share the contacts or information about the contacts of
2 the user unless the user and the contacts of the user con-
3 sent to such use in writing.

4 (b) ACCESS TO, AND CORRECTION, DELETION, AND
5 PORTABILITY OF, COVERED DATA.—

6 (1) IN GENERAL.—Subject to paragraphs (2)
7 and (3), a covered entity shall provide a user, imme-
8 diately or as quickly as possible and in no case later
9 than 90 days after receiving a verified request from
10 the user, with the ability to reasonably—

11 (A) access—

12 (i) if applicable, a list of each third
13 party and service provider to whom the
14 covered entity has transferred or shared
15 the covered data of the user;

16 (ii) the covered data of the user, or an
17 accurate representation of the covered data
18 of the user, including data aggregation
19 that is a readable summary, that is held or
20 has been processed by the covered entity or
21 any service provider of the covered entity;
22 and

23 (iii) if a covered entity transfers cov-
24 ered data, a description of the covered data

1 that was transferred and the purpose for
2 which the third party requested the data;

3 (B) request that the covered entity—

4 (i) correct material inaccuracies or
5 materially incomplete information with re-
6 spect to the covered data of the user that
7 is maintained by the covered entity;

8 (ii) delete or de-identify covered data
9 of the user that is or has been maintained
10 by the covered entity;

11 (iii) notify any service provider or
12 third party to which the covered entity
13 transferred such covered data of the cor-
14 rected information; and

15 (iv) provide contact information to the
16 user of any service provider or third party
17 that the covered data of the user was
18 transferred to so that the user may make
19 requests described in this subparagraph;
20 and

21 (C) to the extent that is technically fea-
22 sible, provide covered data of the user that is or
23 has been generated and submitted to the cov-
24 ered entity by the user and maintained by the
25 covered entity in a portable, structured, and

1 machine-readable format that is not subject to
2 licensing restrictions.

3 (2) FREQUENCY AND COST OF ACCESS.—A cov-
4 ered entity shall—

5 (A) provide a user with the opportunity to
6 exercise the rights described in paragraph (1)
7 not less than twice in any 12-month period; and

8 (B) fulfill the responsibilities described in
9 paragraph (1) free of charge.

10 (3) PROHIBITION ON RETALIATION.—A covered
11 entity shall provide the same quality of goods or
12 services, at the same price or rate, regardless of
13 whether a user took an action described under para-
14 graph (1).

15 (4) RETENTION OF DATA.—A covered entity
16 that collects data on a user’s browsing history or bi-
17 ometric data and information shall delete the data
18 within 60 days after the date on which the data was
19 collected.

20 (c) DATA MINIMIZATION AND CONTEXTUALITY.—

21 (1) COLLECTION AND USE OF INFORMATION.—

22 A commercial data operator shall limit the collection
23 and sharing of information by the operator with
24 third parties to what is reasonably necessary to pro-
25 vide a service or conduct an activity that a consumer

1 has requested or is reasonably necessary for fraud
2 prevention.

3 (2) RETENTION OF INFORMATION.—A commer-
4 cial data operator that collects the personal informa-
5 tion of a consumer shall limit the use and retention
6 of that information to what is reasonably necessary
7 to provide a service or conduct an activity that a
8 consumer has requested or a related operational pur-
9 pose. Any data collected or retained by a commercial
10 data operator solely for security or fraud prevention
11 may not be used for operational purposes.

12 (3) MONETIZATION.—Monetization of personal
13 information shall not be considered reasonably nec-
14 essary to provide a service or conduct an activity
15 that a consumer has requested or reasonably nec-
16 essary for security or fraud prevention.

17 (d) CONSUMER CHOICE AND CONTROL.—

18 (1) COMMERCIAL DATA OPERATOR.—A com-
19 mercial data operator shall provide a prominently
20 and conspicuously displayed icon a user may click to
21 opt out of data collection on every unique website,
22 mobile application, or computer application.

23 (2) COVERED ENTITIES.—Within 2 years after
24 the date of the enactment of this Act, a covered enti-
25 ty shall take reasonable steps, taking account of

1 available technology, to provide users the ability to
2 directly delete the covered data collected by the cov-
3 ered entity.

4 (e) DEFAULT SETTINGS.—A covered entity may re-
5 quire, through terms of service or otherwise, that a user
6 must consent to the transfer of covered data in order to
7 use the service of the covered entity.

8 (f) POLICIES REGARDING DATA FROM MINORS.—A
9 covered entity may not collect, retain, or transfer the cov-
10 ered data of a user to a third party without affirmative
11 consent from the parent or guardian of the user if the
12 user is below the age of 18 years old, where technically
13 feasible.

14 (g) PROHIBITION ON TRACKING COOKIES WITHOUT
15 USER CONSENT.—A commercial data operator—

16 (1) unless authorized by the user, may not
17 track cookies, including on mobile applications; and

18 (2) shall provide the same services to users who
19 do not authorize tracking cookies.

20 (h) TRANSPARENCY.—

21 (1) PRIVACY NOTICE.—A covered entity shall
22 provide users with a clear, comprehensible, accurate,
23 and continuously available privacy notice that—

24 (A) describes in detail the information col-
25 lected by the operator, how that information

1 would be used, and whether the information
2 would be sold or shared with any third party;
3 and

4 (B) is 1,000 words or less.

5 (2) REPORT ON USE OF INFORMATION RE-
6 QUIRED.—If a user allows a commercial data oper-
7 ator to sell the covered data of the user, the com-
8 mercial data operator shall provide the user with an
9 annual report regarding the types of third parties
10 with whom data has been shared. The report shall
11 include a description of what information has been
12 shared, for what purpose information is shared, and
13 a list of each third party that receives data.

14 (i) DATA SECURITY AND BREACH NOTIFICATION.—
15 A covered entity shall notify each user in a timely manner
16 of any data breach with respect to the information of the
17 user and provide any remedy to compensate the user for
18 the breach of their information, including a credit protec-
19 tion service, fraud alert, and credit monitoring through
20 credit reporting agencies.

21 (j) ENFORCEMENT.—

22 (1) ENFORCEMENT BY THE FEDERAL TRADE
23 COMMISSION.—

24 (A) UNFAIR OR DECEPTIVE ACTS OR PRAC-
25 TICES.—A violation of this section shall be

1 treated as a violation of a regulation under sec-
2 tion 18(a)(1)(B) of the Federal Trade Commis-
3 sion Act (15 U.S.C. 57a(a)(1)(B)) regarding
4 unfair or deceptive acts or practices.

5 (B) POWERS OF COMMISSION.—The Com-
6 mission shall enforce this section in the same
7 manner, by the same means, and with the same
8 jurisdiction, powers, and duties as though all
9 applicable terms and provisions of the Federal
10 Trade Commission Act (15 U.S.C. 41 et seq.)
11 were incorporated into and made a part of this
12 Act. Any person who violates this section shall
13 be subject to the penalties and entitled to the
14 privileges and immunities provided in the Fed-
15 eral Trade Commission Act.

16 (2) EFFECT ON OTHER LAWS.—Nothing in this
17 section shall be construed in any way to limit the
18 authority of the Commission under any other provi-
19 sion of law or to limit the application of any Federal
20 or State law.

21 (3) ENFORCEMENT BY STATE ATTORNEYS GEN-
22 ERAL.—

23 (A) IN GENERAL.—If the chief law en-
24 forcement officer of a State, or an official or
25 agency designated by a State, has reason to be-

1 believe that any person has violated or is violating
2 this section, the attorney general, official, or
3 agency of the State, in addition to any author-
4 ity it may have to bring an action in State
5 court under its consumer protection law, may
6 bring a civil action in any appropriate United
7 States district court or in any other court of
8 competent jurisdiction, including a State court,
9 to—

10 (i) enjoin further such violation by
11 such person;

12 (ii) enforce compliance with this sec-
13 tion;

14 (iii) obtain civil penalties; and

15 (iv) obtain damages, restitution, or
16 other compensation on behalf of residents
17 of the State.

18 (B) NOTICE AND INTERVENTION BY THE
19 FEDERAL TRADE COMMISSION.—The attorney
20 general of a State shall provide prior written
21 notice of any action under subparagraph (A) to
22 the Commission and provide the Commission
23 with a copy of the complaint in the action, ex-
24 cept in any case in which such prior notice is
25 not feasible, in which case the attorney general

1 shall serve such notice immediately upon insti-
2 tuting such action. The Commission shall have
3 the right—

4 (i) to intervene in the action;

5 (ii) upon so intervening, to be heard
6 on all matters arising therein; and

7 (iii) to file petitions for appeal.

8 (C) LIMITATION ON STATE ACTION WHILE
9 FEDERAL ACTION IS PENDING.—If the Commis-
10 sion has instituted a civil action for violation of
11 this section, no State attorney general, or offi-
12 cial or agency of a State, may bring an action
13 under this paragraph during the pendency of
14 that action against any defendant named in the
15 complaint of the Commission for any violation
16 of this section alleged in the complaint.

17 (4) PRIVATE RIGHT OF ACTION.—

18 (A) IN GENERAL.—Any individual alleging
19 a violation of this section or a regulation pro-
20 mulgated under this section may bring a civil
21 action in any Federal or State court of com-
22 petent jurisdiction against a covered entity that
23 has global annual gross revenues of at least
24 \$50,000,000.

1 (B) RELIEF.—In a civil action brought
2 under subparagraph (A) in which the plaintiff
3 prevails, the court may award—

4 (i) \$100 to \$750 per violation;

5 (ii) reasonable attorney’s fees and liti-
6 gation costs; and

7 (iii) any other relief, including equi-
8 table or declaratory relief, that the court
9 determines appropriate.

10 (k) DEFINITIONS.—In this section:

11 (1) COMMERCIAL DATA OPERATOR.—The term
12 “commercial data operator” means an entity acting
13 in its capacity as a consumer online services provider
14 or data broker that—

15 (A) generates a material amount of rev-
16 enue from the use, collection, processing, sale,
17 or sharing of data generated by a user; and

18 (B) has more than 100,000,000 unique
19 monthly visitors or users in the United States
20 for a majority of months during the previous 1-
21 year period.

22 (2) COMMISSION.—The term “Commission”
23 means the Federal Trade Commission.

24 (3) CONSENT.—The term “consent” means an
25 affirmative act by an individual that clearly commu-

1 nicates the informed authorization of the individual
2 for an act or practice.

3 (4) CORE FUNCTION.—The term “core func-
4 tion” does not mean targeted advertising or mar-
5 keting.

6 (5) COVERED DATA.—The term “covered data”
7 means individually, identifiable information about a
8 user collected online, including any of the following:

9 (A) Location information that would iden-
10 tify the physical address of an individual.

11 (B) Telephone number.

12 (C) Email address.

13 (D) Social security number or other
14 unique, government-issued identifiers.

15 (E) Nonpublic personal information (as de-
16 fined in section 509 of the Gramm-Leach-Bliley
17 Act (15 U.S.C. 6809)).

18 (F) Content of a personal wire communica-
19 tion, oral communication, or electronic commu-
20 nication such as email or direct messaging with
21 respect to any entity that is not the intended
22 recipient of the communication.

23 (G) Call detail records.

1 (H) Web browsing history, application
2 usage history, and the functional equivalent of
3 either that is not aggregated data.

4 (I) Biometric data and information, such
5 as facial and voice recognition data.

6 (6) COVERED ENTITY.—The term “covered en-
7 tity” means a commercial data broker or large on-
8 line operator that collects covered data from a user
9 through an online platform.

10 (7) DATA BROKER.—The term “data broker”
11 means a covered entity whose principal source of
12 revenue is derived from processing or transferring
13 the covered data of individuals with whom the entity
14 does not have a direct relationship on behalf of a
15 third party for use by the third party.

16 (8) DE-IDENTIFY.—The term “de-identify”
17 means to separate information from the user or IP
18 address the information is associated with.

19 (9) DELETE.—The term “delete” means to re-
20 move or destroy information so that the information
21 is not maintained in human or machine-readable
22 form and cannot be retrieved or used in such form
23 in the normal course of business.

24 (10) LARGE ONLINE OPERATOR.—The term
25 “large online operator” means any person that—

1 (A) provides an online service; and

2 (B) has more than 100,000,000 authenti-
3 cated users of an online service in any 30-day
4 period.

5 (11) MONETIZATION.—The term “monetiza-
6 tion” means the process of collecting, using, and
7 storing data solely for economic benefit.

8 (12) USER.—The term “user” means an indi-
9 vidual residing in the United States who uses a
10 website that collects data and information from the
11 user.

○