

116TH CONGRESS
2D SESSION

S. 4711

To provide for judicial security and privacy.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 24, 2020

Mr. MENENDEZ (for himself, Mr. BOOKER, and Mr. GRAHAM) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To provide for judicial security and privacy.

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 “Daniel Anderl Judicial
5 Security and Privacy Act of 2020”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

8 (1) Members of the Federal judiciary perform
9 the important function of interpreting our Constitu-
10 tion and administering justice in a fair and impartial
11 manner.

1 (2) Federal judges must be able to act without
2 fear of personal reprisal from individuals affected by
3 the decisions they make in the course of carrying out
4 their public duties.

5 (3) In recent years, partially as a result of the
6 rise in the use of social media and online access to
7 information, members of the Federal judiciary have
8 been exposed to an increased number of personal
9 threats in connection to their role.

10 (4) Between 2015 and 2019, threats and other
11 inappropriate communications against Federal
12 judges and other judiciary personnel increased from
13 926 in 2015 to approximately 4,449 in 2019.

14 (5) Over the past decade, several members of
15 the Federal judiciary have experienced acts of vio-
16 lence against themselves or a family member in con-
17 nection to their Federal judiciary role, including the
18 murder of the family of United States District
19 Judge for the Northern District of Illinois Joan
20 Lefkow in 2005.

21 (6) On Sunday July 19, 2020, an assailant
22 went to the home of Esther Salas, a judge for the
23 United States District Court for the District of New
24 Jersey, impersonating a package delivery driver,
25 opening fire upon arrival, and killing Daniel Anderl,

1 the 20-year-old son of Judge Salas, and seriously
2 wounding Mark Anderl, her husband.

3 (7) In the aftermath of the recent tragedy that
4 occurred to Judge Salas and in response to the con-
5 tinuous rise of threats against members of the Fed-
6 eral judiciary, there is an immediate need for en-
7 hanced security procedures and increased availability
8 of tools to protect Federal judges and their families.

9 **SEC. 3. DEFINITIONS.**

10 In this Act:

11 (1) AT-RISK INDIVIDUAL.—The term “at-risk
12 individual” means—

13 (A) a Federal judge; or

14 (B) a senior, recalled, or retired Federal
15 judge

16 (2) DATA BROKER.—The term “data broker”
17 means a commercial entity that collects, assembles,
18 or maintains personal information concerning an in-
19 dividual who is not a customer or an employee of
20 that entity in order to sell the information or provide
21 third party access to the information.

22 (3) DIRECTIONS.—The term “directions”
23 means directions for navigation of surface streets
24 that will lead to the specific covered address, even if
25 the address is not published.

1 (4) FEDERAL JUDGE.—The term “Federal
2 judge” means—

3 (A) a justice or judge of the United States,
4 as those terms are defined in section 451 of
5 title 28, United States Code;

6 (B) a bankruptcy judge appointed under
7 section 152 of title 28, United States Code;

8 (C) a United States magistrate judge ap-
9 pointed under section 631 of title 28, United
10 States Code;

11 (D) a judge confirmed by the United
12 States Senate and empowered by statute in any
13 commonwealth, territory, or possession to per-
14 form the duties of a Federal judge; and

15 (E) a judge of the United States Court of
16 Federal Claims appointed under section 171 of
17 title 28, United States Code.

18 (5) GOVERNMENT AGENCY.—The term “Gov-
19 ernment agency” means any department enumerated
20 in section 1 of title 5 of the United States Code,
21 independent establishment, commission, administra-
22 tion, authority, board or bureau of the United States
23 or any corporation in which the United States has
24 a proprietary interest. The term includes all such in-
25 stitutions, offices, and any other bodies politic and

1 corporate of the United States Government created
2 by the constitution or statute, whether in the execu-
3 tive, judicial, or legislative branch; all units and cor-
4 porate outgrowths created by Executive order of the
5 President or any constitutional officer, by the Su-
6 preme Court of the United States, or by resolution
7 of the United States Congress.

8 (6) IMMEDIATE FAMILY.—The term “immediate
9 family” means a spouse, child, parent, or any other
10 blood relative of an at-risk individual who lives in
11 the same residence as the at-risk individual.

12 (7) JUDGES’ PERSONALLY IDENTIFIABLE IN-
13 FORMATION.—The term “judges’ personally identifi-
14 able information” means—

15 (A) a home address, including primary res-
16 idence or vacation home address, of an at-risk
17 individual;

18 (B) home, personal mobile, or the direct
19 telephone line to the private chambers of an at-
20 risk individual;

21 (C) the personal email address of an at-
22 risk individual;

23 (D) the social security number, driver’s li-
24 cense number, or voter registration information

1 that includes a home address of an at-risk indi-
2 vidual;

3 (E) a bank account or credit or debit card
4 information of an at-risk individual;

5 (F) property tax records or any property
6 ownership records of an at-risk individual, in-
7 cluding a secondary residence and any invest-
8 ment property of at which an at-risk individual
9 resides for part of a year;

10 (G) birth and marriage records of an at-
11 risk individual;

12 (H) vehicle registration information of an
13 at-risk individual;

14 (I) identification of children of an at-risk
15 individual under the age of 18;

16 (J) date of birth of an at-risk individual;

17 (K) directions to a home of an at-risk indi-
18 vidual or immediate family of an at-risk indi-
19 vidual;

20 (L) a photograph of any vehicle including
21 license plate or home including address of an
22 at-risk individual or immediate family of an at-
23 risk individual;

24 (M) the name and location of a school or
25 day care facility attended by a child of an at-

1 risk individual or immediate family of an at-risk
 2 individual; or

3 (N) the name and location of an employer
 4 of an immediate family member of an at-risk
 5 individual.

6 (8) SOCIAL MEDIA.—The term “social media”
 7 means any online electronic medium, a live-chat sys-
 8 tem, or an electronic dating service—

9 (A) that primarily serves as a medium for
 10 users to interact with content generated by
 11 other third-party users of the medium;

12 (B) that enables users to create accounts
 13 or profiles specific to the medium or to import
 14 profiles from another medium; and

15 (C) that enables one or more users to gen-
 16 erate content that can be viewed by other third-
 17 party users of the medium.

18 **SEC. 4. PROTECTING JUDGES’ PERSONALLY IDENTIFIABLE**

19 **INFORMATION IN PUBLIC RECORDS.**

20 (a) GOVERNMENT AGENCIES.—

21 (1) IN GENERAL.—Each at-risk individual
 22 may—

23 (A) file written notice of the status of the
 24 individual as an at-risk individual, for them-

selves and immediate family of an at-risk individual, to each Government agency; and

(B) ask each Government agency described in subparagraph (A) to mark as confidential judges' personally identifiable information.

(2) Government agencies shall not publicly post or display publicly available content that includes judges' personally identifiable information. Government agencies, upon receipt of a written request in accordance with subsection a(1)(A) of this section, shall remove the judges' personally identifiable information from publicly available content within 72 hours.

(b) STATE AND LOCAL GOVERNMENTS.—

(1) GRANT PROGRAM TO PREVENT DISCLOSURE OF PERSONAL INFORMATION OF JUDICIAL OFFICERS.—

(A) AUTHORIZATION.—The Attorney General shall make grants to prevent the release of personally identifiable information of at-risk individuals to the detriment of such individuals or their families to—

(i)(I) a State or unit of local government (as such terms are defined in section 901 of the Omnibus Crime Control and

Safe Streets Act of 1968 (34 U.S.C. 10251); or

(II) an agency of a State or unit of local government;

(ii) that operates a State or local database or registry that contains personally identifying information.

(B) APPLICATION.—An eligible entity seeking a grant under this section shall submit to the Attorney General an application at such time, in such manner, and containing such information as the Attorney General may reasonably require.

(2) AUTHORIZATION OF APPROPRIATIONS.—

There is authorized to be appropriated such sums as may be necessary to provide grants to entities described in paragraph (1) to create or expand programs designed to protect judges' personally identifiable information, including through—

(A) the creation of programs to redact or remove judges' personally identifiable information, upon the request of an at-risk individual, from public records in state agencies; these efforts may include but are not limited to hiring a third party to redact or remove judges' per-

1 sonally identifiable information from public
2 records;

3 (B) the expansion of existing programs
4 that the State may have enacted in an effort to
5 protect judges' personally identifiable informa-
6 tion;

7 (C) the development or improvement of
8 protocols, procedures, and policies to prevent
9 the release of judges' personally identifiable in-
10 formation;

11 (D) the defrayment of costs of modifying
12 or improving existing databases and registries
13 to ensure that judges' personally identifiable in-
14 formation is protected from release; and

15 (E) the development of confidential opt out
16 systems that will enable at-risk individuals to
17 make a single request to keep judges' personally
18 identifiable information out of multiple data-
19 bases or registries.

20 (3) REPORT.—

21 (A) IN GENERAL.—Not later than 1 year
22 after the date of enactment of this Act, and bi-
23 ennially thereafter, the Comptroller General of
24 the United States, shall submit to the Com-
25 mittee on the Judiciary of the Senate and the

1 Committee on the Judiciary of the House of
2 Representatives an annual report that in-
3 cludes—

4 (i) a detailed amount spent by States
5 and local governments on protection of
6 judges' personally identifiable information;
7 and

8 (ii) where the judges' personally iden-
9 tifiable information was found.

10 (B) STATES AND LOCAL GOVERNMENTS.—

11 States and local governments that receive funds
12 under this section shall submit to the Comp-
13 troller General a report on data described in
14 clauses (i) and (ii) of subparagraph (A) to be
15 included in the report required under that sub-
16 paragraph.

17 (c) DATA BROKERS AND OTHER BUSINESSES.—

18 (1) PROHIBITION.—

19 (A) DATA BROKERS.—It shall be unlawful
20 for a data broker to sell, license, trade, pur-
21 chase, or otherwise provide or make available
22 for consideration judges' personally identifiable
23 information.

24 (B) OTHER BUSINESSES.—No person,
25 business, or association shall publicly post or

1 publicly display on the internet judges' person-
2 ally identifiable information if the at-risk indi-
3 vidual has, either directly or through an agent,
4 made a written request of that person, business,
5 or association to not disclose the judges' per-
6 sonally identifiable information of the at-risk in-
7 dividual or that of the at-risk individual's im-
8 mediate family.

9 (C) LIST.—The Administrative Office of
10 the United States Courts may, upon request,
11 act as an agent and provide data brokers with
12 a current list of Federal judges and their imme-
13 diate family for the purpose of maintaining
14 compliance with this section.

15 (2) REQUIRED CONDUCT.—

16 (A) IN GENERAL.—After a person, busi-
17 ness, or association has received a written re-
18 quest from an at-risk individual to protect the
19 judges' personally identifiable information, that
20 person, business, or association shall have 72
21 hours to remove the judges' personally identifi-
22 able information from the internet.

23 (B) INFORMATION PROTECTED.—After a
24 person, business, or association has received a
25 written request from an at-risk individual, that

1 person, business, or association shall ensure
2 that the at-risk individual's judges' personally
3 identifiable information is not made available
4 on any website or subsidiary website controlled
5 by that person, business, or association.

6 (C) TRANSFER.—After receiving an at-risk
7 individual's written request, no person, busi-
8 ness, or association shall transfer the judges'
9 personally identifiable information to any other
10 person, business, or association through any
11 medium.

12 (d) REDRESS AND PENALTIES.—

13 (1) IN GENERAL.—An at-risk individual whose
14 judges' personally identifiable information is made
15 public as a result of a violation of this Act may
16 bring an action seeking injunctive or declaratory re-
17 lief in any court of competent jurisdiction. If the
18 court grants injunctive or declaratory relief, the per-
19 son, business, or association responsible for the vio-
20 lation shall be required to pay the at-risk individ-
21 ual's costs and reasonable attorney's fees.

22 (2) PRIVATE RIGHT OF ACTION.—

23 (A) IN GENERAL.—An at-risk individual or
24 immediate family member who is aggrieved by
25 a violation of subsection (c) of this section may

1 bring an action in any court of competent juris-
2 diction.

3 (B) DAMAGES.—A prevailing plaintiff in
4 an action described in subparagraph (A) shall
5 be awarded damages in an amount—

6 (i) not greater than 3 times the actual
7 damages to the plaintiff; and

8 (ii) not less than \$10,000.

9 **SEC. 5. HOME INTRUSION DETECTION SYSTEM PROGRAM.**

10 There is authorized to be appropriated such sums as
11 may be necessary to provide security monitoring services
12 for active, senior, recalled, or retired Federal judges, in-
13 cluding any method or methods designed to provide secu-
14 rity through a system of interworking components and de-
15 vices such as integrated electronic devices working to-
16 gether with a central control panel, including doorbell
17 cameras, outdoor cameras, and motion detection devices.

18 **SEC. 6. TRAINING AND EDUCATION.**

19 There is authorized to be appropriated to the Federal
20 judiciary such sums as may be necessary for biannual judi-
21 cial security training for active, senior, or recalled Federal
22 judges and their immediate family, including—

23 (1) best practices for using social media and
24 other forms of online engagement and for maintain-
25 ing online privacy;

1 (2) home security program and maintenance;

2 (3) understanding removal programs and re-
3 quirements for judges' personally identifiable infor-
4 mation;

5 (4) any other judicial security training that the
6 United States Marshals Services and the Adminis-
7 trative Office of the United States Courts deter-
8 mines is relevant.

9 **SEC. 7. NEW THREAT MANAGEMENT CAPABILITY.**

10 (a) AUTHORIZATION OF APPROPRIATIONS.—

11 (1) NEW THREAT MANAGEMENT CAPABILITY.—

12 There is authorized to be appropriated to the Ad-
13 ministrative Office of the United States Courts such
14 sums as may be necessary to establish, in coordina-
15 tion with the U.S. Marshals Service and other rel-
16 evant Federal law enforcement and security agen-
17 cies, a new threat management capability for moni-
18 toring all-source information which may:

19 (A) provide a threat monitoring and anal-
20 ysis capability for the protection of at-risk indi-
21 viduals and judiciary assets;

22 (B) coordinate social media monitoring
23 and threat assessments;

24 (C) proactively manage the monitoring of
25 data broker websites for judges' personally

1 identifiable information and report violations to
2 the United States Marshals Service, and other
3 appropriate Federal and local law enforcement
4 authorities;

5 (D) maintain files of escalating behaviors
6 and work in conjunction with the United States
7 Marshals Service, and appropriate Federal and
8 local law enforcement to counteract overt acts
9 of aggression;

10 (E) maintain a database of each active,
11 senior, recalled, or retired Federal judge to
12 catalogue complaints, including the name and
13 other relevant personal information of the indi-
14 vidual or group of individuals engaging in direct
15 or indirect threatening behavior; and

16 (F) coordinate complaints by active, senior,
17 recalled, or retired Federal judges of all sources
18 and other online threats, whether direct or indi-
19 rect, with law enforcement partners.

20 (b) EXPANSION OF CAPABILITIES OF OFFICE OF
21 PROTECTIVE INTELLIGENCE.—There is authorized to be
22 appropriated such sums as may be necessary to the United
23 States Marshals Service to expand the current capabilities
24 of the Office of Protective Intelligence of the Judicial Se-
25 curity Division to—

1 (1) increase the workforce of the Office of Pro-
2 tective Intelligence to include additional intelligence
3 analysts, United States deputy marshals, and any
4 other relevant personnel to ensure that the Office of
5 Protective Intelligence is ready and able to antici-
6 pate and deter threats to the judiciary;

7 (2) provide a number of intelligence analysts of
8 the United States Marshals Service to assist the Ad-
9 ministrative Office of the U.S. Courts in establishing
10 the threat monitoring capability described in sub-
11 section (a); and

12 (3) develop a monitoring, collection, and analyt-
13 ical capability to share relevant information lever-
14 aged from the Administrative Office of the United
15 States Courts and partnered law enforcement and
16 security agencies to protect judiciary personnel and
17 assets.

18 (c) REPORT.—

19 (1) IN GENERAL.—Not later than one year
20 after the date of enactment of this Act, the Depart-
21 ment of Justice, in consultation with the Adminis-
22 trative Office of the United States Courts, shall sub-
23 mit to the Committee on the Judiciary of the Senate
24 and the Committee on the Judiciary of the House of
25 Representatives a report on the security of Federal

1 judges arising from the Federal prosecutions and
2 civil litigation.

3 (2) DESCRIPTION.—The report required under
4 paragraph (1) shall describe—

5 (A) the number and nature of threats and
6 assaults against at-risk individuals handling
7 prosecutions and other matters described in
8 paragraph (1) and the reporting requirements
9 and methods;

10 (B) the security measures that are in place
11 to protect the at-risk individuals handling pros-
12 ecutions described in paragraph (1), including
13 threat assessments, response procedures, avail-
14 ability of security systems and other devices,
15 firearms licensing such as deputations, and
16 other measures designed to protect the at-risk
17 individuals and immediate family of an at-risk
18 individual; and

19 (C) for each requirement, measure, or pol-
20 icy described in subparagraphs (A) and (B),
21 when the requirement, measure, or policy was
22 developed and who was responsible for devel-
23 oping and implementing the requirement, meas-
24 ure, or policy.

1 **SEC. 8. SEVERABILITY.**

2 If any provision of this Act or the application of such
3 provision to any person or circumstance is held to be un-
4 constitutional, the remainder of this Act and the applica-
5 tion of such provision to any person or circumstance shall
6 not be affected thereby.

7 **SEC. 9. EFFECTIVE DATE.**

8 This Act shall take effect on the date that is 120 days
9 after the date of enactment of this Act.

○