



HONORABLE ROSLYNN R. MAUSKOPF
Director

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

JAMES R. BAUGHER
Associate Director
Department of Administrative Services

LEE ANN BENNETT
Deputy Director


WASHINGTON, D.C. 20544

PAUL C. GAMBLE
Acting Chief
Facilities and Security Office

April 20, 2023

MEMORANDUM

To: All United States Judges

From: Paul C. Gamble 

RE: IMPLEMENTATION OF THE DANIEL ANDERL JUDICIAL SECURITY AND PRIVACY ACT
AND UPDATE ON THE HOME INTRUSION DETECTION SYSTEMS PROGRAM
(IMPORTANT INFORMATION)

This memorandum contains important information on the implementation of the Daniel Anderl Judicial Security and Privacy Act which was included in the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Pub. L. No. 117-263 § 5931, et. seq.) and the services offered by the Administrative Office (AO) to assist judges with the statutory protections contained therein. It also includes information on recent developments concerning the Home Intrusion Detection Systems (HIDS) reimbursement program, including an increase in the annual allowance for monitoring and maintenance fees.

Implementation of the Daniel Anderl Judicial Security and Privacy Act

The recently [passed](#) Daniel Anderl Judicial Security and Privacy Act (Daniel Anderl Act) enacts a Judicial Conference policy adopted in 2020 and provides protection for judges' and certain family members' (at-risk individuals) covered information, including multiple forms of common personally identifiable information (PII), that is posted on the internet by private entities and the federal government. Among other provisions, the Daniel Anderl Act specifically:

- Protects at-risk individuals' covered information in federal government public records by allowing judges to request that information be marked as private and not be publicly posted or displayed;
- Prohibits data brokers from selling at-risk individuals' covered information;
- Allows at-risk individuals to request that other persons, businesses, and associations not publicly post or display on the internet covered information except where the information was voluntarily published by the judge (or other covered individual) on the internet, was

lawfully received from a federal government source, or is relevant to and displayed as part of a news story, commentary, editorial, or other speech on a matter of public concern to justify publication of such information;

- Authorizes the Director of the AO to seek removal of posted covered information on behalf of an at-risk individual, upon written request from the judge; and
- Authorizes the AO (through the Department of Justice) to seek injunctive or declaratory relief when an at-risk individual's covered information has not been removed from the internet within 72 hours of a written request.

Except for the prohibition on posting by the federal government, the provisions of this bill go into effect 120 days after enactment or April 21, 2023.

PII Removal and Redaction Services Offered by the AO

Prior to the passage of the Daniel Anderl Act, the AO, as part of the Vulnerability Management Program, began offering PII reduction and redaction services to judges. Specifically, the Threat Management Branch (TMB) of the Judiciary Security Division monitors the internet for covered information; works to assist judges with the removal of covered information under the Daniel Anderl Act; reports judicial threat-related information found to the U.S. Marshals Service (USMS); and coordinates other threat management activities with the appropriate law enforcement agencies. To do this, the TMB uses a number of different services. This includes DeleteMe, a third-party data broker monitoring and removal service to remove judges' PII from known data broker websites. In addition, the TMB provides assessments of current online exposures and recommendations for reduction and removal of covered information on the internet. These reports not only provide additional information to judges regarding their online vulnerability but are also used to inform DeleteMe of additional third-party data broker websites to be addressed.

This suite of services is the primary AO resource for judges to not only reduce their online footprint, but to limit the publication and distribution of covered information as permitted under the Daniel Anderl Act. **Enrollment for judges in these services has already begun through a phased-in approach and is now open nationwide to all judges. Judges interested in enrolling should contact their circuit administrators (see Attachment 1) or email the AO at TMB@ao.uscourts.gov.**

As noted, the Daniel Anderl Act also allows judges and covered family members to compel the removal of covered information from the internet by authorizing the AO Director to seek injunctive or declaratory relief. Fillable forms to authorize the AO to act on a judge's behalf are being developed and will ultimately be accessible through a portal being developed to enroll in the services described above. Notice will be provided when this portal is made live.

Important Exceptions to the Daniel Anderl Act

Judges should be aware of a notable exception to the Daniel Anderl Act pertaining to information contained on financial disclosure forms. Because the Daniel Anderl Act does not

protect information received from a federal government source, including information in financial disclosure reports, judges should consider requesting appropriate redactions at the time any report is filed. The Committee on Financial Disclosure may authorize the redaction of information in a financial disclosure report “where the release of the information could endanger a filer or a filer’s family member.” [Guide to Judiciary Policy, Vol. 2D, Ch. 5, § 550.30.](#)

Additionally, the Daniel Anderl Act does not cover removal or redaction of information from state and county public records agencies. Several states, however, have enacted similar legislation. The [JNet](#) contains a collection of resources to assist with state-level legislative efforts to protect their PII. As authorized by the Daniel Anderl Act, the Department of Justice is in the early stages of developing a grant program to incentivize states to establish or expand programs to protect judges’ PII. The AO will update information on the JNet about this program as it becomes available.

Attachment 2 contains further information on the protections included in the legislation and the services offered by the AO. For additional information, please contact Kyle Yoder, Chief, Threat Management Branch, at Kyle_Yoder@ao.uscourts.gov or 202-502-3177.

Home Intrusion Detection Systems Program

As you know, USMS transitioned the HIDS program from a national service provider to a reimbursement program beginning in February 2022. Under this program, judges are eligible for reimbursement up to \$2,500 for the installation of new equipment (or the alteration of existing equipment) at their primary residence. In addition, judges are eligible to receive reimbursement for annual monitoring and maintenance fees. **The USMS has increased the annual allowance for monitoring and maintenance fees to \$800 (up from \$600). This action applies to all reimbursement submissions beginning in fiscal year (FY) 2023. The USMS is in the process of reviewing all FY 2023 submissions and will increase what was reimbursed to any judge who is eligible to receive more.**

The HIDS webpage on the [JNet](#) is a comprehensive resource for all of the relevant reimbursement information including clarified guidance on the reimbursement form and an informational video featuring judges speaking to the updated technology available under the program as well as the ease of the reimbursement process. Judges who have not yet enrolled in the program are encouraged to contact their district U.S. Marshal, their local USMS Judicial Security Inspector, or the HIDS Program Office at 1-833-978-4350 or HIDS.USMS@doj.gov.

If you have any questions about the information above or any other judicial security matter, please do not hesitate to contact me at (202) 502-1200 or Paul_Gamble@ao.uscourts.gov.

Attachments

cc: Circuit Executives
District Court Executives
Clerks, United States Courts
Circuit Librarians

Circuit Administrators for AO PII Removal Program

First Circuit

Kelsey Kissane, Administrative Specialist
Kelsey_kissane@ca1.uscourts.gov

Second Circuit

Autumn Porter, Information Resources Manager
Autumn_Porter@nysb.uscourts.gov

Third Circuit

Michael Hayes, Manager of Research Services
Michael_Hayes@ca3.uscourts.gov

Fourth Circuit

Jamie Helms, IT Security Officer
Jamie_Helms@ca4.uscourts.gov

Fifth Circuit

Sue Creech, Circuit Librarian
Sue_Creech@ca5.uscourts.gov

Sixth Circuit

Owen Smith, Circuit Librarian
Owen_Smith@ca6.uscourts.gov

Seventh Circuit

Erin Schlicht, Associate Circuit Librarian
Erin_Schlicht@ca7.uscourts.gov

Eighth Circuit

Eric Brust, Circuit Librarian
Eric_Brust@ca8.uscourts.gov

Circuit Administrators for AO PII Removal Program (cont.)

Ninth Circuit

Reggie Galjour, IT Security Officer
rgaljour@ce9.uscourts.gov

Tenth Circuit

Helane Davis, Circuit Librarian
Helane_Davis@ca10.uscourts.gov

Eleventh Circuit

Michael Shubeck, Circuit Librarian
Michael_Shubeck@ca11.uscourts.gov

DC Circuit

Lauren Brown, Judicial Security Officer
Lauren_Brown@ao.uscourts.gov

Federal Circuit/Court of Federal Claims

Jessica Perovich, Circuit Librarian
perovicj@cafc.uscourts.gov

Daniel Anderl Judiciary Privacy and Security Act of 2022

Fact Sheet

The Daniel Anderl Judicial Security and Privacy Act of 2022 ([Pub. L. No. 117-263](#)) restricts the dissemination and posting of certain personally identifiable information of judges' (and certain other individuals') on the internet.

Who is covered?

- Active, senior, recalled, retired federal judges and Justices;
- Their spouses, parents, siblings, or children;
- Anyone for whom the judge stands *in loco parentis*; and
- Any other individual living in the household of the judge.

What information is covered?

- Home address, including primary and secondary residences;
- Home and personal mobile telephone number;
- Personal email addresses;
- Social security numbers and driver's license number;
- Bank accounts and credit/debit card information;
- License plate numbers and other unique identifiers of vehicles owned, leased, or regularly used by an at-risk individual;
- Identifying information of children of an at-risk individual under the age of 18;
- Full date of birth;
- Information regarding current and future school and day care attendance, including the name and address of the school/day care provider, schedules of attendance, and routes taken to or from the school or day care by an at-risk individual; or
- Information regarding the non-governmental employment location of an at-risk individual, including the name and address of the employer, employment schedules, and routes taken to or from the employer by an at-risk individual.

Who is restricted from disseminating covered information?

- Federal Government agency: Executive agency, as defined in section 105 of title 5, United States Code; and any agency in the judicial branch or legislative branch;
- Data brokers: entities that collect and sell or license to third parties the personal information of an individual with whom the entity does not have a direct relationship, except as excluded; and
- Other persons, businesses, and associations.

When do restrictions for disseminating covered information not apply?

- *When the information being provided by a commercial entity is an excluded activity* (i.e., the information is relevant to and displayed as part of a news story, commentary, editorial, or other speech on a matter of public concern; 411 directory assistance or directory information services; alert and emergency notification service; consumer reporting agency subject to the Fair Credit Reporting Act; financial institutions under

Daniel Anderl Judiciary Privacy and Security Act of 2022 Fact Sheet

Gramm Leach Bliley Act; HIPAA covered entities; and collection and sale or licensing of covered information incidental to conducting the above activities).

- ***When the covered information publicly posted or displayed by a person or business is:***
 - Relevant to and displayed as part of a news story, commentary, editorial, or other speech on a matter of public concern;
 - Voluntarily published on the internet by the at-risk individual after the date of enactment of this Act; and
 - Lawfully received from a Federal Government source (or from an employee or agent of the Federal Government). This includes a judge's financial disclosure report.

How can I remove or restrict dissemination of my covered information? Except for PII that has been voluntarily provided or part of an excluded activity defined above, at-risk individuals and immediate family members can either ***act individually*** or ***request that the Director of the AO or their designee*** act to:

- ***With a federal government agency***, file written notice requesting that each agency mark their covered information "private," which triggers the requirement for agencies to remove the covered information from publicly available content within 72 hours of receiving the request; and
- ***With other persons, businesses, and/or associations*** request removal of publicly posted or publicly displayed covered information, whereupon the recipient person or business shall (unless exceptions apply) remove covered information within 72 hours after receipt of the request and ensure that the information is not made available on any website or subsidiary website under their control.

What if my information is not removed? If the request for removal is not honored and the information is not removed within the 72-hour timeframe, at-risk individuals can request that the Director of the Administrative Office of the United States Courts, may file an action seeking injunctive or declaratory relief in any court of competent jurisdiction through the Department of Justice.

Financial Disclosure Implications: Additionally, separate from the Daniel Anderl Act, within the judiciary, judges can request redaction of information in financial disclosure reports that would endanger the judge or the judge's family members when the financial disclosure report is filed. Upon receipt of a request, the Committee on Financial Disclosure can authorize redaction of required information if it finds that release of the information could endanger the filer or a family member.

Who can help me? The AO Facility and Security Office's Judiciary Security Division can provide technical assistance regarding the requests authorized by this legislation. Inquiries should be sent to TMB@ao.uscourts.gov, or call Kyle Yoder, 202-502-3177.



ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

JAMES R. BAUGHER
Associate Director
Department of Administrative Services


WASHINGTON, D.C. 20544

PAUL C. GAMBLE
Chief
Facilities and Security Office

May 7, 2024

MEMORANDUM

To: All United States Judges

From: Paul C. Gamble 
Chief

RE: UPDATES ON IMPLEMENTATION OF THE DANIEL ANDERL JUDICIAL
SECURITY AND PRIVACY ACT (**IMPORTANT INFORMATION**)

This memorandum follows up on the [April 20, 2023 memorandum](#), detailing implementation of the Daniel Anderl Judicial Security and Privacy Act (Daniel Anderl Act), which was included in the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Pub. L. No. 117-263 § 5931, et. seq.) and the services offered by the Administrative Office (AO) to assist at-risk individuals (judges and members of their family) with the statutory protections contained therein.

Personally Identifiable Information Reduction and Redaction Services

The Threat Management Branch (TMB) of the AO's Judiciary Security Division manages a suite of services to help reduce the availability of the personally identifiable information (PII) of at-risk individuals online and to limit the publication and distribution of their "covered information" as defined in the Daniel Anderl Act. This information is reflected in an [updated JNET page about PII services](#). This page also references a PII Removal Portal that gives judges and non-judiciary personnel (i.e., members of their family) access to the PII protection resources, including information on the overall PII removal process. Each at-risk individual must complete the [Request for Access to PII Removal and Privacy Program Resources Form](#) before they can enter the portal. The TMB has developed a [video with step-by-step instructions](#) for users to navigate the portal and select their desired PII services.

State Legislative PII Initiatives and Information

In addition to the services detailed above, the TMB is actively providing research and information regarding the status of PII legislation at the state level. The information includes current initiatives and potential resources available in most states and the status of proposed online privacy legislation. It further identifies state agencies making protected information available to the public and the legislative and judicial offices at the state level that may be contacted with concerns regarding available protections in a state. This information and the [toolbox](#) developed by the AO's Office of Legislative Affairs can be accessed through the [TMB PII State Legislation Dashboard](#).

PII Reduction and Redaction Program Enrollment Efforts

Currently, the PII Reduction and Redaction Program is providing coverage to 69 percent of active judges, 54 retired judges, and 185 qualifying family members. Enrolled judges receive DeleteMe, a data broker redaction service, which, as of April 24, 2024, has redacted over 4.22 million pieces of PII on enrollees from publicly accessible internet sites. The program has also provided over 600 judges personalized reporting regarding the availability of their information on the internet, recommendations on personal actions that can be taken to reduce their online footprint, and guidance on requesting redaction of their information from local online public records. To assist judges who are not enrolled, the TMB **will host twice-monthly virtual Enrollment Open Hours. During these sessions, TMB staff will be available to assist with enrollment, address any technical issues with the services, and answer questions about the program. These sessions will occur on the first and third Fridays of every month from 1:00 p.m. to 4:00 p.m. (eastern time) through July 19, 2024. Registration for these sessions can be accessed [here](#).**

For additional information on the PII Reduction and Redaction Program including support on state legislative resources, please contact Kyle Yoder, Chief, Threat Management Branch, at Kyle_Yoder@ao.uscourts.gov or (202) 502-3177. If you have any other questions regarding other judicial security matters, please do not hesitate to contact me at (202) 502-1200 or via email at Paul_Gamble@ao.uscourts.gov.

cc: Circuit Executives
District Court Executives
Clerks, United States Courts
Circuit Librarians