

SECTION 1. SHORT TITLE.

Sets the short title of the bill to the “Government Surveillance Transparency Act of 2022”

SEC. 2. CRIMINAL SURVEILLANCE ORDERS.

(a) Limitation on Sealing

For the types of criminal surveillance order listed below, requires that these orders, the applications for the orders, and other related materials, be made public after the court-approved surveillance ends, unless the government seeks an order to seal the documents. The kinds of orders covered are:

Interception of content (wiretaps), interception of metadata (pen registers), mobile tracking devices, stored communications (content and non-content), delay of notice and non-disclosure (gag orders), search warrants, covert entry searches / sneak and peek orders, All Writs Act orders, third party surveillance assistance orders, including under the Communications Assistance for Law Enforcement (CALEA) Act.

Permits the government to seek an order sealing these documents from the public for a maximum of 180 days, which the court must grant if the government certifies that there is reason to believe that failure to seal will have an adverse result, which is defined as:

- endangering the life or physical safety of an individual;
- flight from prosecution;
- destruction of or tampering with evidence; intimidation of potential witnesses; or
- otherwise seriously jeopardizing the investigation to which the criminal surveillance order relates or unduly delaying a trial resulting from the investigation.

The court has the discretion to require the government to provide the factual basis for the certification and to review that factual basis for sufficiency.

There is a heightened standard of judicial review:

- if the government cannot certify that the target of the surveillance order does not know about the investigation and does not know that they are a target or person of interest in the investigation;
- when renewing seals of surveillance orders older than one year
- if the sealing is subsequently challenged by a provider or any other third party.

Under the heightened standard of judicial review, the court may grant the sealing order, if the government:

- demonstrates through particularized facts that failure to extend the sealing period will have an adverse result which would not be avoided by redaction of specified words, phrases, or passages in the criminal surveillance order, application, or inventory.

- Submits to the court information about, the nature of the investigation, the suspected crimes, the name of the target, and specific facts that substantiate the need for the extension.

Allows any person to challenge a surveillance sealing order. If they win, the government must pay their costs.

(b) Docketing and Publication of Criminal Surveillance Orders, Applications, Inventories, and Associated Docket Records

Requires that, regardless of whether a criminal surveillance order is sealed, courts shall maintain public dockets containing basic information about each order. This information shall include, the date and time of applications and orders, the type of order, the type of crime under investigation; the investigating agency; the duration of the requested surveillance if any; whether sealing and deferred notice were requested, if so for how long; and whether an order demanding third party assistance was requested and approved.

Requires that surveillance applications and orders for each person, phone number, device, or account targeted be issued a unique case number and generic description following rules promulgated by the Judicial Conference of the United States or the highest court of the State or Indian Tribe.

Requires that that dockets and supporting documents published online be in an accessible form consistent with section 508 of the Rehabilitation Act of 1973.

Requires the Supreme Court to update existing privacy and security rules for information published online to address personal information included in criminal surveillance orders and applications that are made available to the public.

Gives courts two years to implement the requirements of this section. Allows state and tribal courts to delay the implementation of the new requirements for sealing and docketing for up to four years if they need more time.

Requires courts to move to secure electronic filing for surveillance applications and court orders, so that officers do not have to file these documents in person. Allows this requirement to be delayed for one year per renewal, if the Administrative Office of the United States Courts or the chief judge of the highest court of the State or Tribe certifies that their existing document submission system is not secure enough.

SEC. 3. NOTICE TO COURTS OF UNLAWFUL SURVEILLANCE.

Requires that after conducting surveillance using a search warrant, an order for stored communications, or an order for intercepting metadata, that the government shall notify the court that issued the order if:

1. A provider disclosed to the government any electronic data not authorized by the court and, if so, provide the court with detailed information regarding the disclosure; and
2. the government searched persons or property, including accounts or electronic devices, or obtained metadata not authorized by the court or in a manner that exceeded the authorization granted by the court and, if so, submit to the court detailed information about what happened.

SEC. 4. NOTICE TO SUBJECTS OF LAW ENFORCEMENT SURVEILLANCE.

Requires that when the government conducts surveillance of stored communications or under the All Writs Act, it follows all of the requirements for executing and returning a warrant under Rule 41 of the Rules of Criminal Procedure (which among other things, require the government to provide a copy of the the order to the surveillance target).

Requires that the government provide prior notice to the the targets of such court-ordered surveillance, unless the government seeks and obtains an order for delayed notice under 18 U.S.C 2705.

Requires the government to provide notice to individuals whose information is turned over voluntarily to the government in emergencies, within 5 days of the disclosure, unless the government seeks and obtains an order for delayed notice under 18 U.S.C 2705.

Clarifies that for the purposes of providing notice, the government must notify the person or persons whose communications are obtained under the order. This is necessary because courts have previously interpreted the notice requirements for warrants issued under Rule 41, when applied to user data held by technology companies, to only require notice to the provider, and not to the targeted user.

SEC. 5. DELAY AND PRECLUSION OF REQUIRED NOTICE.

Replaces the existing statute, 18 U.S.C. 2705, allowing the government to obtain court orders delaying required notice to the target by the government and orders gagging a provider from notifying customers about surveillance of their data.

Permits the government to request an order delaying mandatory notice to court-ordered surveillance of stored data or intercepted metadata, but only if the surveillance order is itself sealed, and only for the duration of the sealing order.

Permits the government to request a non-disclosure order prohibiting a provider from revealing the existence of a surveillance order or subpoena. In the case of a surveillance order, only if the surveillance order is itself sealed, and only for the duration of the sealing order.

For surveillance required by a subpoena or voluntarily by a provider in an emergency, permits the government to seek an order delaying required notice to the targets. Also permits the government to seek a non-disclosure to the providers order for surveillance required by a subpoena. These delayed notice and non-disclosure orders may be issued by a court for up to 180 days, renewable:

- For the initial order and the first renewal, delaying notice, the court shall grant the order if the government certifies that there is reason to believe that failure to issue the order will have an adverse result. However, the court may require the government to provide the factual basis for the certification.
- For subsequent renewals of the non-disclosure order (after one year), if the government meets the higher judicial standard of review described in section two.

Adds to the annual wiretap report published by the Administrative Office of the United States Courts, mandated aggregate reporting for non-disclosure orders to providers.

Amends 18 U.S.C. 3103a, which allows the government to obtain warrants for covert entry searches, also known as “sneak and peek” or “black bag” searches. The statute currently allows notice for these searches to be delayed indefinitely. This new text limits the delay of notice to 180 days per order, which can be renewed.

SEC. 6. INCENTIVES FOR STATE AND TRIBAL COURTS TO IMPLEMENT REQUIREMENTS.

While the sealing and docketing rules in section two explicitly apply to state and tribal courts, this section reinforces those requirements.

Limits the use of federal statutes authorizing the surveillance of stored communications, the interception of metadata, and the interception of content, to courts that follow the sealing and docketing requirements in section two.

Limits “full-faith and credit” guarantees for the inter-state enforcement of state court orders, in 28 U.S.C 1738, to orders from courts in states that follow the sealing and docketing requirements in section two.

Gives state and tribal courts a total of six years before these additional provisions kick in.

SEC. 7. MODERNIZING CRIMINAL SURVEILLANCE REPORTS.

Adds to the annual wiretap report published by the Administrative Office of the United States Courts, mandated aggregated reporting for surveillance of stored records and communications content under the Stored Communications Act and the interception of metadata under the Pen Register Act.

SEC. 8. GRANTS.

Requires the Attorney General to issue a maximum of \$25 million in grants to State and Tribal court systems for the cost of implementing the requirements of this bill. The grant program may last five years.

SEC. 9. AUTHORIZATION OF APPROPRIATIONS.

Authorizes to be appropriated \$1 million to the Administrative Office of the United States Courts to implement the requirements of this Act.

Authorizes to be appropriated \$25 million for the grant program under section 8.

SEC. 10. SEVERABILITY.

Specifies that if any provision of this Act is held to be unconstitutional, the remaining provisions of the Act shall not be affected.