

The Government Surveillance Transparency Act

Law enforcement agencies obtain hundreds of thousands of secret surveillance orders and subpoenas in criminal cases each year, routinely demanding private information from phone and internet companies. The government has no obligation to ever notify most of the people surveilled. In addition, the government routinely obtains gag orders preventing providers from telling their customers. Even the scale of surveillance is hidden from the American people, because many surveillance orders are sealed indefinitely and the government publishes no statistical data on the most common types of surveillance.

Americans should eventually learn they were spied on, once it will no longer disrupt a case.

Although people targeted by wiretaps and bank subpoenas must eventually be notified that they were the subject of surveillance, there is no similar requirement when the government obtains Americans' emails and texts, location data, photos stored in the cloud, and records of phone calls. People who are prosecuted may eventually learn through discovery, but those who are never charged with a crime will never be told.

Over the past decade, many technology companies have adopted a policy of voluntarily notifying their customers when the firms receive surveillance orders and subpoenas for their data. In response, the government now routinely obtains gag orders to accompany their surveillance orders and subpoenas, which federal law permits to be issued indefinitely, prohibiting the firms from notifying their customers.

The Government Surveillance Transparency Act adopts transparency best practices from other areas of surveillance law and reforms pioneered by several federal courts around the country. The bill mandates the use of these best practices by federal, state, and tribal courts nationwide, while ensuring that active investigations aren't disrupted. This bill:

- Requires law enforcement to eventually notify targets about subpoenas and court ordered surveillance of their electronic data, similar to existing rules for wiretaps and bank subpoenas.
- Reforms indefinite "gag" orders to providers. Shifts to non-disclosure orders for court ordered surveillance and subpoenas that last 180 days, which can be renewed if necessary.
- Explicitly permit providers and other interested parties to challenge sealing and gag orders, and require the government to pay the challenger's costs and legal fees if the government loses.
- Requires that surveillance applications and orders eventually be unsealed and docketed so they are available to the public and press, once it will no longer disrupt an investigation or put individuals at risk of harm. Permits courts to redact sensitive information from these documents.
- Requires courts to publish online basic data about every surveillance order they authorize. This will not reveal the target's name or other information that could disrupt an active investigation.
- Requires that law enforcement notify courts if they search the wrong person, house or device pursuant to an order issued by the court or if a provider discloses data not authorized by the court.
- Require the Administrative Office of the Courts to expand the annual wiretap reports to include data on the surveillance of stored communications, interception of metadata, and gag orders.
- Provide grants to State and Tribal courts to implement the requirements of the Act.