

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

December 15, 2017

The Honorable James C. Duff
Secretary
The Judicial Conference of the United States
One Columbus Circle NE
Washington, DC 20544

Dear Secretary Duff:

I am writing to urge that you eliminate the unnecessary secrecy around electronic surveillance orders authorized by federal courts and provide Congress with data necessary to perform effective oversight over law enforcement surveillance.

Federal judges regularly approve the use of invasive military-grade surveillance technologies to spy on Americans' telephone calls, emails, and location data. Congress authorized law enforcement to intercept telephone calls and place covert audio "bugs" in Americans' homes with the Omnibus Crime Control and Safe Streets Act of 1968. Recognizing the long history of surveillance tools being abused by the state, Congress strictly regulated the use of these tools and required that courts publish detailed statistics on the use of wiretaps, believing that such reporting would "assure the community that the system of court-ordered electronic surveillance . . . is properly administered and [would] provide a basis for evaluating its operation."

Five decades after Congress first comprehensively regulated the use of wiretaps, law enforcement agencies rely even more on invasive spying tools. In today's investigations, law enforcement agencies regularly obtain both historical and real-time location data from wireless phone companies, use military-grade surveillance technology to impersonate cell-phone networks, and, in the process, send probing electronic signals into every home within a targeted neighborhood. Beyond this, law enforcement agencies also now hack into smartphones and computers, recording target's conversations or movements through personal devices. Appallingly, the government did not seek new authorization from Congress before deploying these intrusive surveillance technologies. Instead, law enforcement circumvented the legislative process by asking courts to permit surveillance using traditional search warrants—authority Congress never intended to permit.

While intrusive surveillance is now a standard law enforcement practice, disturbingly little is known about the scale of such surveillance. Indeed, as one magistrate judge has noted, though federal courts approve and seal tens of thousands of electronic surveillance orders annually, little is known about the court's criminal electronic surveillance docket, which he has described as "the most secret docket in America."

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

The courts must embrace serious transparency reforms so that Congress and the American people have the appropriate information in order to conduct effective oversight of surveillance programs and understand the scale of government surveillance. Although increased disclosure may result in minor additional clerical burdens for court staff, that burden is both necessary to effectively authorize complex government surveillance programs and pales in comparison to the vast benefit incurred from effective Congressional oversight and public awareness.

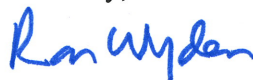
To be sure, courts around the country have demonstrated that the burden from publishing basic non-sensitive information and unsealing older cases is minimal. In the Eastern District of Virginia, electronic surveillance orders are kept in separate electronic dockets; non-sensitive information about those cases is available to the public by request. In the Southern District of Texas, Magistrate Judge Stephen Wm. Smith has stopped automatically sealing orders indefinitely, instead sealing them for 180 days at a time and permitting the government to request extensions. Judge Smith also collects basic information on requested surveillance through a “criminal cover sheet,” based on the civil cover sheet already used in federal courts across the country. Finally, Chief Judge Beryl A. Howell of the U.S. District Court for the District of Columbia recently began systematically unsealing all of the electronic surveillance orders issued in her court from 2011 through 2016. Though these courts have taken different approaches, they all address the same problem: excessive secrecy surrounding the electronic surveillance docket.

Regardless of how the federal judiciary ultimately embraces reform, the courts must address this serious deficiency. The current status quo—in which the federal judiciary simply has no idea how many location tracking, cell site simulator, and hacking orders courts issue each year—must change. To that end, I ask that you institute the following common-sense reforms:

1. Require federal courts to collect basic data on the different types of surveillance technologies they are authorizing law enforcement agencies to use and make aggregate information publicly available to Congress and the American people.
2. Require federal courts to docket the electronic surveillance orders they approve, so that each surveillance order approved is issued a unique case and document number.
3. Require federal courts to make public basic information about all electronic surveillance orders they approve, even those that are sealed. At the very least, courts should meet the standard established by the Eastern District of Virginia, which includes a public list of case numbers, surveillance order types, and the dates the docket number was issued.
4. Require federal courts to reform the current practice of indefinitely sealing electronic surveillance orders and instead seal them, if necessary, for no more than 180 days at a time.
5. Update the methodology used to collect and analyze the data presented in the annual wiretap report to reflect the variety and pervasiveness of modern surveillance technologies currently in use.

If you have any questions about this request, please contact Chris Soghoian on my staff.

Sincerely,



Ron Wyden
United States Senator