Study of the Administrative Office of the U.S. Courts' Wiretap Report

Conducted at the Request of the Judiciary Data and Analysis Office of the Administrative Office of the U.S. Courts

David Rauma
James Eaglin
Carly Giffin
Marvin Astrada

FJC
Federal Judicial Center

November 2021

Federal Judicial Center
Thurgood Marshall Federal Judiciary Building
One Columbus Circle NE
Washington, DC 20002
fjc.dcn • fjc.gov

Contents

Introduction

At the request of the Administrative Office of the U.S. Courts' (AO) Judiciary Data and Analysis Office (JDAO), the Federal Judicial Center (Center) conducted a study of the Wiretap Report. The Wiretap Report is published annually by JDAO based on information provided to the AO by federal and state judges and prosecutors. Title 18 U.S.C. § 2519 requires federal and state judges to annually report information about wiretaps that expired or were terminated during the previous year.[1] The statute also requires federal and state prosecutors to annually report information on wiretap applications made during the previous year, whether those applications were approved or denied. The JDAO assembles this information each year to produce the Wiretap Report.

In an effort to improve both the Wiretap Report and the reporting process that feeds into it, the AO requested that the Center help them gather opinions and suggestions from judiciary and nonjudiciary stakeholders. Judiciary stakeholders provided opinions and suggestions concerning how the reporting process could be modernized and streamlined, and nonjudiciary stakeholders provided insight into how the Wiretap Report could be made clearer and more beneficial for users. The Center gathered this information in a three-stage study encompassing two sets of focus groups and an online survey.

The first stage of the study consisted of focus groups conducted with judges, prosecutors, and representatives from the Department of Justice (DOJ). The full report for this stage of the study can be found on page 5 of this report, and its executive summary is on page 6. The second stage was a survey sent to academics, senate staffers, journalists, and attorneys working for civil society groups and telecommunication companies. The complete results of the survey can be found on page 34 of this report, and its executive summary can be found on page 35. The final stage of the study was a set of focus groups conducted with a subset of the survey's respondents, and its full report can be found on page 49, with its executive summary on page 50.

Despite their different focuses, some of the findings from each stage of the study complement one another. These complementary findings are briefly highlighted in this Introduction. They do not represent the full range of issues discussed, or suggestions provided, in the full report of each stage.

1. While judges are required to submit reports, as we discuss below, prosecutors are the primary actors filling out the reporting forms. The judiciary stakeholder focus groups revealed that prosecutors often fill out the forms for the judges to review and submit. Thus, prosecutors were the judiciary stakeholders who had the most suggestions for updating the reporting forms.

Updating and Maintaining the Wiretap Reporting Forms and Data Collection Process

The need to modernize the wiretap reporting forms and data collection process was one of the main themes that emerged from the judiciary stakeholders focus groups. Prosecutors said that while they wanted to fulfill their reporting duties, the forms themselves made it more difficult. They said that the technologies listed on the forms were not up to date, complicating their ability to fill them out accurately. Nonjudiciary stakeholders in both the survey and the focus groups agreed that the technologies tracked in the Wiretap Report were out of date. The nonjudiciary stakeholders also requested that the data be tracked and presented with more nuance. For example, these respondents noted that the Wiretap Report does not make clear whether a wiretap application for a cell phone covers just the telephone capabilities of the device, or whether it also includes messaging applications and other data. This nuanced information could be helpful to people who use the Wiretap Report for academic, journalistic, business, and oversight purposes, and breaking the larger reporting categories apart may also make the form easier for prosecutors to complete accurately.

Suggestions for what technologies to track, as well as how to keep the form up to date moving forward, were provided in all stages of the study and are detailed in the sections below.

Updating the forms may also help to address the main theme to emerge from the nonjudiciary stakeholders: frustration that the information in the Wiretap Report is incomplete. The nonjudiciary stakeholders expressed concern about the amount of missing data[2] and late reporting by prosecutors, which cause the Wiretap Report to be incomplete and, therefore, inaccurate. This was a main theme of both the survey and focus groups with nonjudiciary stakeholders. As noted by the prosecutors themselves, modernizing the forms could make them easier for prosecutors to fill out in a timely, accurate manner. In addition to the updates already mentioned, prosecutors are frustrated by the WT-3 form used to report events (including arrests, trials, convictions, and costs) that occur in the current reporting year but refer to applications reported in a prior year. Submitting this form requires prosecutors to find and include a reference number issued by the AO so that the WT-3 can be linked to the prior report. Finding this number can be time consuming. Some prosecutors reported delaying the submission of their original reports to obviate the need to submit a WT-3, leading to their reports being submitted potentially years late. Streamlining the WT-3 process could lead to fewer late reports and better updating of previously reported information. This would go some way toward addressing the incompleteness and inaccuracy concerns raised by the nonjudiciary stakeholders.

2. Nonjudiciary stakeholders were primarily concerned with jurisdictions (i.e., states) that did not submit a report. However, AO staff explained that sometimes submitters may be alerted to errors in their submissions which they do not correct. This uncorrected information is not included in the tables of the Wiretap Report and may be another source of "missing" data.

While updating the forms will help address many of the stakeholders' concerns, clearer instructions for filling out the current forms would also be beneficial. Prosecutors in the focus groups reported confusion about how the forms were to be filled out, and how certain terms were defined. Nonjudiciary stakeholders were also confused as to how certain terms were defined and therefore should be interpreted. Further, the prosecutors noted that it was not clear to them why some of the information on the form was being requested. They suggested that providing references to the statute would clarify that the information is statutorily required. Providing clearer instructions and definitions to prosecutors would aid them in filling out the form accurately, and these same definitions and instructions could be made available to nonjudiciary stakeholders to help them interpret the data. Including the statutory references either in the instructions or on the form itself could encourage fuller reporting.

The DOJ's Electronic Surveillance Unit (ESU) reviews all federal wiretap applications prior to submission and has expressed their willingness to work with the AO to update the forms and instructions that accompany them.[3]

Improving the Wiretap Report

Another set of suggestions aims to improve the Wiretap Report itself, rather than the reporting process. Participants in the nonjudiciary stakeholders focus groups requested that clear explanations of what data are represented in the Wiretap Report accompany all relevant tables. Several of the nonjudiciary stakeholders noted that it was difficult to interpret the Wiretap Report because it was not clear how much data was represented. These stakeholders said that an explanation prominently displayed with each table stating 1) what data were included (i.e., the number of states), and 2) whether the report had been, or would be, updated with information received after the yearly deadline would help them to accurately interpret the data. While it is impossible for the JDAO to be aware of every local jurisdiction that may have approved or denied a wiretap application, an explanation of what is included in the Wiretap Report could be provided. Such an explanation might also serve to publicly reiterate the reporting mandate to judges and prosecutors, further encouraging reporting.

Nonjudiciary stakeholders in the survey were also eager to be able to filter the data in the Wiretap Report in as many ways as possible (i.e., geographic location, type of surveillance). The ability to filter would provide more nuance and clarity to the Wiretap Report, two attributes that the nonjudiciary stakeholders in the focus groups called for as well. A third suggestion to improve the Wiretap Report was to increase nonjudiciary stakeholders' access to the data in the least edited form available. These stakeholders

3. See the full report of the wiretap reporting forms focus groups, *infra* page 5, for more detail on the ESU's participation in the study and willingness to be part of modernizing the reporting forms.

appreciated the ability to download some of the data contained in the Wiretap Report and hoped that access would be continued and expanded.

The opinions and suggestions reviewed in this introduction provide only a brief snapshot of the detailed and thoughtful responses we received from the people who participated in this study. Nonjudiciary stakeholders' requests for more comprehensive, nuanced, and accessible data were driven by their reliance on this data in their teaching, reporting, oversight, and business endeavors. Many respondents expressed their gratitude to the AO for collecting and reporting this data and emphasized that their suggestions were aimed at improving what they considered to be a vital resource. Prosecutors, similarly, realize that their reporting requirement is important, and they would like to make it easier to fulfill in a timely, accurate manner. All of their responses make clear that the AO's effort to improve the Wiretap Report and the process that feeds into it is worthwhile and will benefit not only users of the data, but the providers of that data as well.

Wiretap Reporting Forms
Focus Groups

David Rauma
James B. Eaglin
Marvin Astrada

Executive Summary: Wiretap Reporting Forms Focus Groups

Title 18 U.S.C. § 2519 requires that, in January of each year, any federal or state judge who issued an order for a wiretap under 18 U.S.C. § 2518 that expired or terminated during the previous year, or denied approval of a wiretap application, report certain information about each order or application to the AO. Similarly, each federal and state prosecutor who sought an order for a wiretap, whether approved or denied, during the previous year must make a similar report to the AO in March of each year. The judge and prosecutor reports are combined onto one reporting form (WT-2A for federal reports and WT-2B for state reports). In addition to a report for each expired/ terminated wiretap order, prosecutors submit a form (WT-1) summarizing the past two years of wiretap reports and can submit supplemental forms updating information on wiretap reports from previous years (WT-3). In June of each year, the AO is required to submit to Congress a report that contains an analysis of the information reported by the judges and prosecutors in the preceding months. The JDAO has the responsibility of compiling information submitted by the judges and prosecutors and preparing the AO's annual report.

At the request of JDAO, in order to collect information about the wiretap reporting process, the Center conducted focus groups in 2019 in San Antonio, Philadelphia, and Los Angeles. Invited participants included federal and state court judges, federal and state prosecutors, representatives from the DOJ, and representatives from state-level departments of justice. During day-long sessions, the participants recounted their experiences with wiretap reporting, discussed potential changes to the reporting forms and the reporting process, and offered their own suggestions for improvements to both.

Those three days of discussions, with judges and prosecutors from different parts of the country, produced some consistent themes. One theme is important to stress at the outset: all participants involved with the submission of the wiretap reporting forms expressed a strong interest in satisfying their reporting requirements. Other themes can be summarized as follows.

Wiretap Reporting Requirements and Definitions

- There is a general absence of a consistent understanding of basic aspects of the reporting process, such as what constitutes a new wiretap order and what constitutes an extension of an existing wiretap order.
- There is confusion in both state and federal jurisdictions about what a WT-2 form represents. Is it for each wiretap application, regardless of the number of phones included in the application (and any extensions)? Or is it for each phone?
- Potentially, every county prosecutor who is required to submit a WT-2B form has

a unique interpretation of what must be reported on the form, how it must be reported, and when it must be reported.

- Further, a single investigation may require multiple orders over time, with multiple phones added or dropped in wiretap orders after the first. Some prosecutors are unsure if these orders require multiple WT-2 forms or a single form.
- All participants agreed that the statute (18 U.S.C. § 2519) is out of date with respect to modern communications technology, and that an update would resolve at least some of the confusion about what is to be reported and how.
- Some participants expressed confusion over why some information was requested on the forms. One participant suggested, and the others present agreed, that cites to the statute directly on the forms would reinforce the idea that the information was statutorily required.
- Some federal jurisdictions are not aware of the WT-1 and WT-3 forms and the requirements to submit these forms.
- Some state and federal jurisdictions intentionally do not submit WT-3 forms, instead waiting until investigations are complete and wiretap applications and their extensions have expired to submit WT-2 forms. These WT-2 forms may not be submitted until a year or more past the annual deadline.

Wiretap Forms and Instructions

- The forms do not capture all types of communication technology available today (e.g., VOIP, or encrypted apps such as "WhatsApp"). The statute itself is out of date in this regard.
- The WT-2 and WT-3 forms are too time-consuming to complete. For example, the WT-2 forms require identifying information (judge, prosecutor, and agency reference numbers). The WT-3 form requires an AO-generated report number from a prior year that must be searched for on the AO's website. The requirement for the original AO report number was the most frequently cited issue with the WT-3 form.
- Some portions of the WT-2 are completed with boilerplate language (e.g., Form WT-2, Part 2, Box 13: Comment and Assessment).
- Some portions of the WT-2 are completed with guesses or estimates of varying quality, such as costs of the wiretap (e.g., Form WT-2, Part 2, Boxes 11 & 12: Cost). For example, if an investigation involves multiple wiretap applications, total costs must be apportioned between applications, and that apportionment may be largely guesswork.

Overall, a clarification of the instructions for the current reporting forms is needed as soon as possible.

Form Preparation and Submission Process

- Neither federal nor state judges complete their portion of the WT-2. Prosecutors, investigators, and court staff complete that portion of the form for the judge's signature. As a result, some participants argued that judges should not or need not be a part of the reporting process. The participating judges agreed that their role in the reporting process should be rethought.[4]
- The AO's annual report includes a report of denials of wiretap applications, but denials are almost nonexistent. Participants described how an application for a wiretap is fully vetted by prosecutors and, if necessary, reworked so that a judge can approve it.
- Some jurisdictions do not know about the fillable PDFs for the WT forms. Instead, they xerox the forms, complete the xeroxed versions, convert the xerox versions to PDFs, and submit these PDF versions. The JDAO staff must then reenter the submitted information on fillable PDFs.
- Some jurisdictions edit the fillable PDFs before submission. Here, too, JDAO staff must reenter the information.
- There is no feedback from the Administrative Office concerning errors or omissions on the submitted forms. Without feedback, there is no accountability, and the errors and omissions are likely to persist.[5]
- Participants discussed several alternatives for collating or submitting wiretap reports that could improve reporting by improved coordination within jurisdictions or improved coordination between JDAO and reporting jurisdictions. One well-received suggestion was the creation of an online portal, through which jurisdictions could receive forms, complete and submit their annual reports, track past submissions in order to submit WT-3 forms, and receive feedback about errors or omissions.

Participants' Recommendations

The focus group participants made a number of suggestions and recommendations for change, with varying degrees of specificity. We will try to summarize those suggestions, and, where necessary, try to sharpen their focus based on the experiences described by

4. By statute, judges are required to submit annual reports. They cannot be eliminated from the reporting process without a change in statute.

5. After the focus groups were conducted, we learned that, starting with the 2019 Wiretap reporting year, submitters will receive automated notification reports summarizing reporting errors with instructions on how to correct the error and resubmit the data to the AO. The notification reports will list warnings and errors about data quality issues and instructions to 1) review warnings, and 2) correct errors and resubmit the form.

those participants. Some of these recommendations can be addressed directly by JDAO; other recommendations may require legislative action to implement.

- The forms are complex and, at times, confusing. Participants urged strongly that the forms be simplified and that JDAO provide better instructions for their completion.
- The forms are outdated with respect to modern communications technology. Participants wanted the forms, and the reporting process, modernized to reflect new technologies.
- Eliminate confusion over what is being reported. The statute establishes the wiretap application as the reporting unit, but investigations can be complex, involving numerous phones and internet-based applications. Keeping track of the phones can be a difficult and confusing task, and some jurisdictions have simplified the process by submitting a separate wiretap reporting form for each phone on a wiretap application.
- When JDAO finds errors or omissions in the submitted forms, there should be feedback from JDAO.
- The involvement of federal and state judges in the reporting process should be reconsidered.
- JDAO should consider developing recommendations or "best practices" for federal districts, and perhaps state jurisdictions, about how to organize the annual production of the wiretap reporting forms.
- Training and better communication from JDAO could increase consistency across jurisdictions about what should be reported and how.

Discussion

The federal wiretap statute dates to 1968. In that precellular phone and pre-Internet era, Congress seemingly wanted annual reports with counts of landline phones for which wiretap applications were made. In recent years, observers have expressed concerns about these annual reports and the data contained therein.[6] For example, some observers have pointed to differences between the number of wiretaps reported annually by the AO and the number of wiretaps reported by the major phone carriers such as Verizon and AT&T. In particular, the carriers have typically reported higher numbers of wiretaps than the AO's reports, and critics have cited this as evidence of underreporting by the AO. Others have

6. See, for example, http://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent, or https://www.forbes.com/sites/andygreenberg/2012/07/02/as-reports-of-wiretaps-drop-the-governments-real-surveillance-goes-unaccounted.

criticized the AO for not going beyond its statutory obligation and reporting on other types of phone intercepts such as "pen registers" and "trap and trace,"[7] or expanding reporting to new technologies such as internet-based communications.

In order to better understand the reporting process and uncover potential sources of errors or inaccuracies in that process, JDAO asked the Center to conduct a series of focus groups with those required by statute to report wiretap applications—federal and state judges and federal and state prosecutors. The goal of the focus groups would be to gather information about the AO's reporting forms and reporting process, and potentially uncover issues that might cause inaccurate reporting of wiretap applications. Our task in the focus groups and in this report is not to address any criticisms directly. We organized and conducted the focus groups to gather information, sometimes about specific issues, that JDAO may use to improve wiretap reporting.

Focus Group Participants

The Center organized three focus groups, held in San Antonio, Philadelphia, and Los Angeles. With a limit of 15–20 participants per focus group, we identified prospective participants from among those federal court districts and state jurisdictions with the highest numbers of reported wiretap applications in the AO's 2017 wiretap data. Reporting state jurisdictions are typically counties or court districts within states, although a small number of state attorneys general and state supreme courts report wiretap applications to the AO. As we discovered, many state and federal jurisdictions designate one or several judges to process wiretap applications and, consequently, these judges were easily identified by the number of reports associated with them. Similarly, county prosecutors' offices typically designate one or more prosecutors or staff to process and submit wiretap reports to the AO. The larger number of federal prosecutors with wiretap reporting experience made it difficult to identify the most experienced prosecutors from a single year or even two years of reports. We turned to the Executive Office of U.S. Attorneys (EOUSA) for assistance. With our list of federal districts showing the largest numbers of wiretap applications in 2017, the EOUSA contacted those districts and requested that they designate a representative experienced with wiretap reports.

We divided the list of prospective participants into three geographic regions and extended invitations to each person on the list. The AO sent invitation letters to the state and federal judges; we contacted state prosecutors by phone and sent emails to federal prosecutors designated by the EOUSA. Our contact with the EOUSA led to an expression of interest in attending the focus groups by the DOJ's Electronic Surveillance Unit (ESU). The ESU is responsible for reviewing all federal wiretap applications before their sub-

7. Pen registers record the phone numbers of a telephone's outgoing calls. Trap and trace devices record the phone number of incoming phone calls. Pen register is sometimes used as a generic term for both types of devices.

mission to a judge and has had prior discussions with JDAO staff about the wiretap reporting process. We invited ESU to participate and a different member of their staff attended each focus group. After some judges and prosecutors declined an invitation to participate, we averaged nine participants, not counting JDAO and Center staff, per focus group.

Appendix A is a complete list of focus group participants.

Focus Group Agenda

Appendix B is the agenda used for all three focus groups. Each focus group began at 9:00 a.m. and lasted until approximately 1:30 p.m. The agenda covers the different reporting forms, in turn and separately for judges and prosecutors, and the reporting process itself. We kept the agenda simple because we did not know what we would learn from the participants, and, hence, we wanted to foster a discussion that took its natural course rather than be forced into narrow, predetermined categories. We had topics we wanted to cover; if they were not raised by the participants, we asked about them. A good example of such a topic is denials of wiretap applications. The AO's 2018 wiretap report states[8] that that year only two wiretap applications were reported as denied. This topic did not come up naturally, but we asked about denials in the course of the group discussion. As it turned out, participants were eager to discuss their experiences with wiretap reporting and the issues they identified with the forms and the submission process.

Wiretap Reporting Forms

JDAO uses three separate types of forms for reporting wiretap applications. Each form is available as a fillable PDF, with a separate set of instructions for completing the forms. Appendix C contains copies of these forms.[9]

WT-1 (Annual Prosecutor Summary of Wiretap Reports) is a summary form to be completed by prosecutors, one for each reporting jurisdiction. Due in March of each year, it summarizes information for each of the previous two calendar years about the total number of wiretap reports submitted for terminated wiretaps, the number of wiretap applications denied, and, among approved applications, the number in which encryption was encountered.

WT-2A and WT-2B (Report of Application and/or Order Authorizing Interception of Communications) are separate but largely identical forms for reporting federal and state wiretap applications, respectively. According to the accompanying instructions, the form is to be completed for each wiretap application denied and for each approved wiretap application—wiretap order—that expired during the previous calendar year. The forms

8. https://www.uscourts.gov/statistics-reports/wiretap-report-2018.

9. The instructions are sometimes lengthy and can be downloaded at https://www.uscourts.gov/forms/other-forms.

have two parts. The first part is completed by the judge approving the application and subsequent extensions, with input from the prosecutor submitting the application. The second part is completed by the prosecutor. In the following pages, we will use WT-2 as a generic reference to both WT-2A and WT-2B forms and WT-2A or WT-2B to refer to that specific version of the form.

WT-3 (Supplementary Report for Wiretaps Reported in Previous Calendar Years) is a form for prosecutors to report events subsequent to an application reported on a WT-2A or WT-2B form. The events include arrests, trials, convictions, and costs that occurred in the current reporting year but refer to applications reported in a prior year.

General Observations

The focus participants had a lot to say about wiretap reporting and were not hesitant to discuss issues they had with the reporting forms and the process of submitting those forms. At the beginning of each group, we told them that we wanted to hear their views and the only rule was that we would not contest whatever they had to say. The result was a lengthy and often lively discussion in each of the three focus groups.

All focus group participants required to submit wiretap reporting forms acknowledged and affirmed their statutory obligation to report wiretap applications. They expressed no doubts about this obligation. Participants were, at the same time, open about how they have struggled to meet that obligation in the crush of other work obligations, lack of clarity about what the reporting forms represent, and misinformation or even lack of information about the scope of their reporting obligations. Consequently, these issues have likely resulted in underreporting of wiretap applications. We will detail in the following sections how, according to the focus group participants, this underreporting may come about.

Wiretap Reporting Requirements and Definitions

The focus group participants could not agree about what should be reported on the WT-2A and WT-2B forms. While the forms' instructions refer to a wiretap application as the triggering event for submission of a form, both state and federal prosecutors pointed out that, as part of a wide-ranging investigation, an application might reference dozens of phones, and that phones might be added or dropped in subsequent extensions of the original wiretap order. Alternatively, a single investigation might require multiple wiretap applications, each with extensions of the original order. Each focus group struggled to define whether a WT-2 form represents a wiretap application or a phone on a wiretap application. Regardless, trying to make sense of these many permutations and fit them on one or more WT-2 forms is seen as a daunting task, for which some jurisdictions have devised their own solutions. One state jurisdiction has adopted a procedure whereby each phone referenced on a wiretap application receives a separate WT-2B form. This procedure eliminates any confusion about what should be reported on each WT-2 form but, it could

be argued, is not consistent with the instructions. One federal prosecutor argued during the focus group discussion that the original intent of Congress was that each wiretap application represented a single phone and, consequently, each phone should receive a separate WT-2 form.

One thing upon which all focus group participants agreed is that the statute requiring wiretap reports—18 U.S.C. § 2519—is out of date with respect to current technology. When the statute was originally enacted, there were no cell phones and no internet communications (e.g., Voice Over Internet Protocol and WhatsApp), and "telephone" referred to a landline. Prosecutors in the focus groups were unanimous in stating that their wiretap applications refer almost exclusively to cell phones; landline telephones represent a largely outdated technology. An updated statute, with references to modern communications, could resolve some of the current confusion over what is to be reported.

While the state jurisdictions represented at the focus groups are aware of the WT-1 forms, the same cannot be said of the federal jurisdictions. Some of the focus group participants had never seen a WT-1 form and, consequently, did not know it was a required submission. As for the WT-3 forms, the responses were mixed. Some jurisdictions do not submit WT-3 forms, or submit them occasionally. Several federal prosecutors said that these forms, for wiretap applications reported in earlier years, are difficult to complete. One federal prosecutor described the process of finding the AO report number for the original report on the AO's website as difficult and too time-consuming. The AO report number assigned to the original WT-2 report is necessary to link the WT-3 form to that report. One prosecutor observed that this report number is difficult to find and that he would spend no more than ten minutes searching for it; that is the amount of time he could and would devote to the search. Further, since federal prosecutors are often reassigned and their cases taken up by new prosecutors, the knowledge of previous wiretap reports and the obligation of submitting supplementary information is sometimes lost. Several state prosecutors described how they waited until investigations and subsequent court cases were terminated before submitting a WT-2B form. As a result, they did not need to submit a WT-3 form as a supplementary report, but their WT-2B forms might be submitted years late. JDAO does not update annual reports from past years if WT-2 forms are sent after the deadline.

Consistency among prosecutors, or lack thereof, was a theme in the discussions in all three focus groups. This was particularly true when the discussion involved the state prosecutors. Each of the prosecutors representing state jurisdictions described a unique process for preparing forms. We described above how some state prosecutors submit WT-2B forms only after a case is concluded and each defendant has been adjudicated. This simplifies their calculation of costs and their enumeration of trials, motions, and convictions and obviates the need to submit a supplementary WT-3 form. It also means that, for some number of cases, the WT-2B form is submitted well after the annual deadline. We also described how at least one state jurisdiction submits a separate WT-2B form for

each phone listed in each wiretap application, thereby inflating the number of apparent wiretap applications approved.

Underreporting, or misreporting, may thus have different sources: confusion over what WT-2 forms represent, in part due to technological changes over time; ignorance of what forms are required; and work-arounds to avoid the difficulty of reporting supplementary information for earlier reports.

Wiretap Forms and Instructions

As noted in the previous section, focus group participants agreed that the statute requiring annual reporting is outdated with respect to modern communications technology. In turn, the WT-2 forms do not capture well the technological changes that have occurred since the statute was enacted in 1968, especially with respect to the fields capturing type of intercept and location specified in an intercept order. The ESU has offered to work with AO staff to identify possible updates to the reporting forms that reflect current communication technology. For example, focus group participants described how a single wiretap application/order may encompass multiple cell phones, with phones added or dropped in subsequent extensions of the order. The WT-2 form records only the types of communication devices listed in the order and the dates and duration of extensions of the original order. If the logic behind the statute was that a wiretap application targeted a single landline telephone and that annual reports would show the number of telephones intercepted, the WT-2 forms do not capture this information.

In addition to the types of devices, judges and prosecutors are required to include on the WT-2 form information identifying the official making the wiretap application, the prosecutor authorizing the application, the law enforcement agency conducting the wiretap, the judge authorizing or denying the application, the offense, locations of the wiretap, a general description of the intercepts (e.g., number of days in use, number of communications intercepted, number of individuals whose communications were intercepted, whether encryption was encountered), the cost of the wiretap, the results of the wiretap (e.g., arrests, trials, motions to suppress, convictions), the importance of the wiretap, and the name and identifying information of the person who prepared the report. Some of this information is required by statute, but participants in the focus groups were not aware of what was required and questioned why it had to be included. One participant suggested, and others in that session agreed, that a reference to the statute be included on those portions of the form required by statute, as an incentive for prosecutors to record it in as detailed and accurate a fashion as possible. As we discovered, and several of the judges discovered,[10] the WT-2 form is completed largely by prosecutors, often with input

10. Several judges described how their portion of the WT-2 report was completed by their courtroom deputy; the judges signed the form when it was completed. However, after hearing the prosecutors describe

from investigators.[11] That includes the part of the form that is to be completed by the judge. Some of the information is straightforward if time consuming to assemble. Other information is more difficult to obtain. Costs and results are difficult to obtain, particularly for multiyear, multidefendant investigations of which the wiretap is only one part or not even the only wiretap. The prosecutors explained how they obtained cost estimates for large investigations and assigned a share to the wiretap, but several prosecutors admitted that the apportionment of costs was largely guesswork. Because of trials and appeals, convictions are also problematic to report. Conviction information represents a snapshot in time. As for the importance of the wiretap, some of the prosecutors described how they use boilerplate language rather than write a new description for each report.

Part of each focus group discussion centered around whether clearer instructions or training would help resolve some of the confusion and uncertainty about what forms are to be completed and how. Most agreed that clearer instructions would help, but there was no consensus about training, especially about who would deliver the training and when. Federal prosecutors receive training at the National Advocacy Center in South Carolina, and that could be an opportunity for training on wiretap reporting. There is no centralized training for state prosecutors.

Form Preparation and Submission Process

As we noted above, the judges in the focus groups told how the WT-2 forms were completed for them, for their signature. This was true of both federal and state judges. Further, the judges expressed no dissatisfaction with their largely hands-off role in the process. It was clear from the discussion with the judges that their role in completing the form could be rethought and possibly eliminated.

Denials of wiretap applications are almost nonexistent. We asked specifically why that is the case, and the response was that applications are reworked until they will be approved. That reworking may take place after review by the ESU or after an initial denial by a judge.

JDAO provides fillable PDF versions of the wiretap reporting forms for use by reporting jurisdictions.[12] These fillable PDF forms have embedded XML[13] codes to make the forms machine-readable. Some jurisdictions are not aware of the importance of using the forms

---

the process of completing the form, they checked with their chambers and found that their portion of the form was completed by prosecutors and given to their courtroom deputies.

11. Several prosecutors described their reliance on forms created by investigators at the Drug Enforcement Agency (DEA). These forms contained information needed to complete the WT-2 form.

12. JDAO is introducing a new system for wiretap reporting, using Excel rather than fillable PDFs. Only one jurisdiction represented in the focus groups acknowledged using the new system; thus, we have no information about its general reception nor any issues it presents to users.

13. eXtensible Markup Language is used to create documents that are both machine- and human-readable.

as provided and distribute xerox copies to prosecutors instead. When submitted to JDAO, the xeroxed forms must be entered by hand, introducing an additional source of potential error. Some jurisdictions have edited the forms to present information in a format they choose. This too creates issues when the altered forms are processed by JDAO. This discussion prompted some focus group participants to point to a larger problem: they receive no feedback from JDAO when there are errors or omissions in their reports. As a result, jurisdictions have not been held accountable for submitting incorrect or altered forms or incomplete information; however, starting with 2019 reporting period, JDAO sends to data submitters automated notification reports with instructions on how to correct errors and resubmit the data. These notifications list warnings and errors about data quality issues; they include instructions to review the warnings, correct errors, and resubmit the data.

Toward the end of each focus group, we asked about how, from the user perspective, the submission process could be improved. One suggestion was that the federal courts' Case Management/Electronic Case Files (CM/ECF) system could be used to organize and track wiretap orders for reporting purposes. One focus group participant, a representative from a federal district's clerk's office, described how that district uses a portion of the CM/ECF system to do just that, generating reports that federal judges and prosecutors in that district can use to track and check their reports. This could work for federal districts, and federal prosecutors showed some receptivity to the idea, but state prosecutors were noncommittal about the idea of using the federal CM/ECF system for that purpose. As a practical matter, a solution involving CM/ECF gives the responsibility of coordinating with the district courts to the state jurisdictions. For the AO's 2017 wiretap report, 130 counties plus a small number of other jurisdictions submitted reports. Approximately one-third of these jurisdictions submitted ten or more reports and only four jurisdictions submitted one hundred or more reports. These four jurisdictions had representatives at the focus groups and they showed little or no interest in using CM/ECF for tracking wiretap reports. If the high-volume jurisdictions did not want to coordinate CM/ECF use with a district court, why would jurisdictions generating far fewer reports?

A suggestion that received a positive response was that JDAO create a secure web portal, perhaps modeled after patient portals in healthcare, that could be used by every jurisdiction to interact with JDAO directly. Such a site could allow jurisdictions to log in securely, track wiretap orders, submit wiretap reports and supplementary reports such as the WT-3, and receive feedback from JDAO about receipt of such reports and errors or omissions. As a single, centralized approach, a portal could be attractive to large and small jurisdictions because it would require no effort on their part to implement and could simplify the creation and submission of wiretap reports.

Finally, we want to reemphasize that, among all the focus group participants, there was a strong recognition of, and determination to follow, the statutory reporting obligations imposed by 18 U.S.C. § 2519. At the same time, there was a recognition that, apart from the

statutory obligation, there is little incentive to submit the forms in a timely fashion, if at all. In jurisdictions with large numbers of wiretaps, the task of completing the wiretap forms is time-consuming and can require a large degree of coordination between and within the courts and prosecutors. A concerted effort to improve both the forms and the submission process, especially with assistance from the ESU, would be welcomed by all participants in this annual process.

Appendix A: Focus Group Participants[14]

Judges

Hon. Cynthia A. Bashant	S. District of California
Hon. John D. Galluzzo	18th Judicial Circuit, Florida
Hon. John A. Gibney	E. District of Virginia
Hon. David J. Hale	W. District of Kentucky
Hon. George C. Hanks, Jr.	S. District of Texas
Hon. Timothy S. Hillman	District of Massachusetts
Hon. John Molloy	Superior Court of Riverside County, Riverside, California
Hon. Judith Ference Olson	Superior Court of Pennsylvania

Prosecutors

Michael BenAry	Assistant U.S. Attorney, E. District of Virginia
Annemarie Braun	Senior Assistant, Colorado Office of the Attorney General
Mark Burnley	Deputy District Attorney, District Attorney's Office, Los Angeles County, California
Matt Chen	Deputy Attorney General, California Department of Justice
Eun Young Choi	Assistant U.S. Attorney, S. District of New York
Miranda Crawford	Legal Executive Assistant, DA's Office, Clark County, Nevada
Peter Crusco	Executive Assistant DA, District Attorney's Office, Queens County, New York
Thomas H. Edmonds	Assistant U.S. Attorney, District of Oregon
Mary Sue Feldmeier	Assistant U.S. Attorney, District of Arizona
Christopher Hotaling	Assistant U.S. Attorney, N. District of Illinois
Jodie Kane	Chief, Rackets Bureau, DA's Office, New York County, New York
Richard J. Magness	Deputy Criminal Chief, U.S. Attorney's Office, S. District of Texas

14. Participants' job titles are shown as of the time of the focus groups, with the exception of AO personnel, whose positions are current as of August 2020.

Diana Pauli	Assistant U.S. Attorney, C. District of California
Linda Ricci	Assistant U.S. Attorney, District of Massachusetts
Joseph S. Smith, Jr.	Chief, OCDETF Section, U.S. Attorney's Office, S. District of California
Ronnell Wilson	Assistant U.S. Attorney, District of New Jersey

Department of Justice

Seth J. Applebaum	Deputy Chief, Office of Enforcement Operations, Electronic Surveillance Unit, Criminal Division
Sarah Kauke	Deputy Chief, Electronic Surveillance Unit, Criminal Division
Jeffrey Pollak	Deputy Chief for Policy, Electronic Surveillance Unit, Criminal Division

Other

Robert F. Flaig	Operations Support Supervisor, District Clerk's Office, W. District of Texas

Federal Judicial Center Staff

Marvin Astrada	Senior Research Associate
James B. Eaglin	Director, Research Division
David Rauma	Senior Research Associate

Administrative Office Staff

Sheila Barnes-Jones	Acting Chief, Data Quality and Production Branch
Fay Cheung	Deputy Chief, Systems Development and Support Office
Danita Chiles	Social Science Analyst
Erin Short	Chief, Data Governance Division
Lisa Seghetti	Chief, Production and Analysis Division

Appendix B: Focus Group Agenda

9:00 a.m.	**Introductions of Participants & Goals of Focus Group**
9:15 a.m.	**Wiretap Reports–Overview by JDAO Staff**
9:35 a.m.	**Individual Forms and Instructions–Reporting Challenges**
9:45 a.m.	**Judge's Report** Federal Form WT-2A and State Form WT-2B
10:50 a.m.	**Break**
11:00 a.m.	**Prosecutor's Reports** Federal Form WT-2A and State Form WT-2B Annual Prosecutor Summary: Form WT-1 Supplementary Report: Form WT-3 AO Guidance on completing WT-2 forms
12:00 p.m.	**Break**
12:10 p.m.	**Suggestions for Change** Quality and Quantity of Information Submission Process
1:15 p.m.	**Wrap up and Follow-up Expectations**
1:30 p.m.	**Adjourn**

Appendix C: Wiretap Reporting Forms

WT-1

WT-2A Federal

WT-2B State

WT-3

WT-1
(Rev. 03/19)

ANNUAL PROSECUTOR SUMMARY OF WIRETAP REPORTS
Submitted Pursuant to 18 U.S.C. § 2519

THIS SUMMARY (AS WELL AS THE INDIVIDUAL WIRETAP REPORTS FOR CALENDAR YEAR 2018 AND SUPPLEMENTAL REPORTS FOR PRIOR YEARS) MUST BE RECEIVED BY THE ADMINISTRATIVE OFFICE NO LATER THAN MARCH 31, 2019.

Completed copies of the form as well as questions concerning this form may be sent via e-mail to sd-wiretap@ao.uscourts.gov.

____ Total Number of Reports Submitted for Wiretaps Terminated in Calendar Year 2018
(Total = Denied + Granted)

- ____ Number of Wiretap Applications Denied
- ____ Number of Wiretap Applications Granted
  - ____ Of Those Granted, Number Where Encryption Was Encountered
    - ____ Of Those with Encryption, Number Where Encryption Prevented Law Enforcement from Obtaining the Plain Text of Communications Intercepted

____ Total Number of Reports Submitted for Wiretaps Terminated in Calendar Year 2017 or Earlier
(Total = Denied + Granted)

- ____ Number of Wiretap Applications Denied
- ____ Number of Wiretap Applications Granted
  - ____ Of Those Granted, Number Where Encryption Was Encountered
    - ____ Of Those with Encryption, Number Where Encryption Prevented Law Enforcement from Obtaining the Plain Text of Communications Intercepted

DATE: _____

Jurisdiction (Federal Prosecutors only): _____
(Judicial District, e.g., Maryland, Florida - S)

Jurisdiction (State Prosecutors only): _____ State: _____
(e.g., State Attorney General, Winston County, Jud. Dist. of Denton (Yates Co.))

Contact Name: _____

Title: _____

Telephone: _____

Print | Save As... | Submit

WT-2A Federal
(Rev. 08/2015)

Administrative Office of the United States Courts

Part 1 (Judge's Report - Federal)
Report of Application and/or Order Authorizing Interception of Communications

(To be reported by January 31 for denied applications and for approved applications for orders that expired during the preceding year, pursuant to 18 U.S.C. § 2519(1))

1. Judge Authorizing or Denying the Application

Judge's First Name:	Middle Initial:	Last Name:	Suffix:

Court Jurisdiction: Select:	Court Reference No.:

2. Source - Official Making Application

Official's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Title: *(i.e., DA, etc.)* Select or enter a title:	Official's Jurisdiction/Agency:

3. Deputy Assistant Attorney General (DAAG)

Deputy Assistant Attorney General's Name Select:	Other Deputy Assistant Attorney General's Name

3A. Prosecution Official Authorizing Application

Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Prosecutor's Jurisdiction: Select:	Prosecutor Reference No.:

3B. Law Enforcement Agency Conducting the Wiretap

Agency Name *(FBI, DEA, etc.)* Select or enter an Agency Name:	Agency Reference No.:

Contact Person's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.: Extension:

4. Offense *(Most Serious)*	**5. Type of Order *(Select One)***
Most Serious Offense: Select:	☐ Ordinary Specification Order *(including most cell phone wiretaps)*
Title/Section of Offense:	☐ Roving - Relaxed Specification Order Granted under 18 U.S.C. 2518(11)

6. Duration of Intercept

Order or Extension	No. of Days	Date of Application	*Check One* Denied	Granted	Date Order Denied or Granted	Date that a Granted Order/Extension was Modified or Amended, if applicable.
Original Request			☐	☐		Date Modified /Amended
1st Extension			☐	☐		Date Modified /Amended
2nd Extension			☐	☐		Date Modified /Amended
3rd Extension			☐	☐		Date Modified /Amended
4th Extension			☐	☐		Date Modified /Amended
5th Extension			☐	☐		Date Modified /Amended
6th Extension			☐	☐		Date Modified /Amended
Use the last page of the form for additional extensions.	**Total Number of Extensions:** 0				**Total Days Authorized:** 0	

WT-2A Federal
(Rev. 08/2015)

7. Type of Intercept ***(Check all that apply to this order/authorization)***

Phone - check device(s)	**Oral -** check device(s)	**Electronic -** check device(s)
☐ Cellular or Mobile Telephone	☐ Microphone / Eavesdrop	☐ Computer *(including email)*
☐ Standard Telephone *(land line)*	☐ Other *(specify)*	☐ Digital Pager
☐ Other *(specify)*	_____	☐ Fax Machine
_____		☐ Text Messaging
		☐ App
		☐ Other *(specify)*
		_____

8. Location Shown in Intercept Order ***(Check all that apply to this order/authorization)***

☐ Portable Device - Carried by/on Individual *(e.g., cell phone, pager)*
☐ Personal Residence *(e.g., single family house, apartment, mobile home, rooming house, dormitory)*
☐ Business *(e.g., store, office, restaurant, gym, hospital, school)*
☐ Public Area *(e.g., pay telephone, park, station, airport, library, street, cemetery)*
☐ Other Location *(e.g., motel, prison, jail, vehicle, another specified location not listed)*
Specify
☐ No Location Specified in Order *(either "roving" as shown in item 5, or other circumstances)*
Describe

8A. Judge's Signature ***(Use /s/ or Check Endorsement Box)***

	☐ Judge's Endorsement	Date:	Telephone No.:

8B. Report Prepared By

Report Preparer's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.: Extension:

Title:	Date:

Instructions

When Part 1 (Judge's Report) is completed, do the following:

(1) Click the "Validate Part 1" button to identify any data quality issues with Part 1.
(2) Save a PDF copy of the completed form by clicking the "Save As" button below and assigning a unique file name.
(3) Click the "Submit by Email" button below to submit this form or attach one or more saved PDF forms to an email and send to SD-WIRETAP@AO.USCOURTS.GOV.
(4) Provide an electronic copy of the completed Part 1 to the official making the application.
(5) Retain a copy of the completed Part 1 for the judge's files.

Additional Instruction

Judges stop here. Prosecutors and Law Enforcement Agencies continue to Part 2 of the WT-2 Form.

Validate Part 1 **Save As** **Submit by Email**

WT-2A Federal
(Rev. 08/2015)

Administrative Office of the United States Courts

Part 2 (Prosecutor's Report - Federal)
Report of Application and/or Order Authorizing Interception of Communications

(To be reported by March 31 for terminated investigations, pursuant to 18 U.S.C. § 2519(2))

Judge Authorizing or Denying the Application

Judge's First Name:	Middle Initial:	Last Name:	Suffix:

Court Jurisdiction:	Court Reference No.:

Prosecution Official Authorizing Application

Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Prosecutor Reference No.:	Agency Reference No.:	Application Date (Original Request):

NOTE: Items listed above should match information entered in Part 1 of Form WT-2.

9. Installation

☐ Never Installed ☐ Installed but Not Used ☐ Installed and Used

10. Description of Intercepts

10A. Termination Date of Interception	10B. No. of Days in Actual Use	10C. No. of Communications Intercepted ☐ Unknown	10D. No. of Persons Whose Comm. Were Intercepted ☐ Unknown	10E. No. of Incriminating Comm. Intercepted ☐ Unknown

10F. Was Encryption Encountered in this Wiretap? ☐ Yes ☐ No	10G. If Yes, Did Encryption Prevent Law Enforcement from Obtaining the Plain Text of Communications Intercepted? ☐ Yes ☐ No

11. Cost (Rounded to Nearest Dollar)

Check the option that applies:

☐ Costs for this wiretap are reported below.

☐ Costs for this wiretap are included on another wiretap form with the following reference number.

Reference Number Type: Reference Number:

☐ Costs for this wiretap are unknown at this time.

11A. Nature and Quantity of Personnel Used to Install, Monitor, and Prepare Transcripts

11B. Personnel Cost		11C. Resource Cost (installation fees, supplies, equipment, etc.)		11D. Total Cost = Personnel Cost + Resource Cost
$	+	$	=	$

12. Results

Check the option that applies:

☐ Results for this wiretap are reported below.

☐ Results for this wiretap are included on another wiretap form with the following reference number.

Reference Number Type: Reference Number:

☐ Results for this wiretap are not known at this time. *(Future results should be reported on the WT-3 Supplementary Report)*

12A1. No. of Persons Arrested	12A2. Arrest Offense (Most Serious):	12B. No. of Motions to Suppress Granted	Denied	Pending

12C. No. of Persons Convicted	12D. No. of Trials Completed	12E. Conviction Offense (Most Serious):	12F. Title/Section of Conviction Offense:

13. Comments and Assessment
Describe importance of the interceptions, drugs and money seizure amounts, impact on community, etc. **DO NOT** include target's name, address, phone numbers, name of gangs, or other sensitive information.

13A. Report Prepared By				
Prosecutor Responsible for Part 2	Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:
Report Preparer	☐ Check if Prosecutor and Report Preparer are the same person.			
	Report Preparer's First Name:	Middle Initial:	Last Name:	Suffix:
	Title:		Telephone No.: Extension:	Date:

Instructions

When Part 2 (Prosecutor's Report) is completed, do the following:

(1) Click the "Validate Part 2" button to identify any data quality issues with Part 2.

(2) Save a PDF copy of the completed form by clicking the "Save As" button below and assigning a unique file name.

(3) Attach one or more saved PDF forms to an email and send to the Federal Law Enforcement Agency Contact who will review and submit the PDF forms to the DOJ's Office of Enforcement Operations.

(4) Retain a copy of the completed form for your files.

Validate Part 2 Only **Validate Parts 1 & 2** **Save As**

6. Duration of Intercept ***(Additional Extensions)***						
Order or Extension	No. of Days	Date of Application	*Check One* Denied	Granted	Date Order Denied or Granted	Date that a Granted Order/Extension was Modified or Amended, if applicable.
7th Extension			☐	☐		Date Modified /Amended
8th Extension			☐	☐		Date Modified /Amended
9th Extension			☐	☐		Date Modified /Amended
10th Extension			☐	☐		Date Modified /Amended
11th Extension			☐	☐		Date Modified /Amended
12th Extension			☐	☐		Date Modified /Amended
13th Extension			☐	☐		Date Modified /Amended
14th Extension			☐	☐		Date Modified /Amended
15th Extension			☐	☐		Date Modified /Amended
16th Extension			☐	☐		Date Modified /Amended
17th Extension			☐	☐		Date Modified /Amended
18th Extension			☐	☐		Date Modified /Amended
19th Extension			☐	☐		Date Modified /Amended
20th Extension			☐	☐		Date Modified /Amended
21st Extension			☐	☐		Date Modified /Amended
22nd Extension			☐	☐		Date Modified /Amended
23rd Extension			☐	☐		Date Modified /Amended
24th Extension			☐	☐		Date Modified /Amended
25th Extension			☐	☐		Date Modified /Amended
26th Extension			☐	☐		Date Modified /Amended
27th Extension			☐	☐		Date Modified /Amended
28th Extension			☐	☐		Date Modified /Amended
29th Extension			☐	☐		Date Modified /Amended
30th Extension			☐	☐		Date Modified /Amended
31st Extension			☐	☐		Date Modified /Amended
32nd Extension			☐	☐		Date Modified /Amended
33rd Extension			☐	☐		Date Modified /Amended
34th Extension			☐	☐		Date Modified /Amended
35th Extension			☐	☐		Date Modified /Amended
36th Extension			☐	☐		Date Modified /Amended

WT-2B State
(Rev. 10/2015)

Administrative Office of the United States Courts

Part 1 (Judge's Report - State / County / Local)
Report of Application and/or Order Authorizing Interception of Communications

(To be reported by January 31 for denied applications and for approved applications for orders that expired during the preceding year, pursuant to 18 U.S.C. § 2519(1))

1. Judge Authorizing or Denying the Application

Judge's First Name:	Middle Initial:	Last Name:	Suffix:

State: Select:	Court Jurisdiction:	Other Court Jurisdiction:

Court Reference No.:

2. Source - Official Making Application

Official's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Title: *(i.e., DA, etc.)* Select or enter a title:	Official's Jurisdiction/Agency:

3A. Prosecution Official Authorizing Application

Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Prosecutor's Jurisdiction:	Other Prosecutor's Jurisdiction:

Prosecutor Reference No.:

3B. Law Enforcement Agency Conducting the Wiretap

Agency Name *(FBI, DEA, Sheriff, etc.)*	Agency Reference No.:

Contact Person's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.: Extension:

4. Offense *(Most Serious)*

Most Serious Offense:
Select:

Title/Section of Offense:

5. Type of Order *(Select One)*

☐ Ordinary Specification Order *(including most cell phone wiretaps)*

☐ Roving - Relaxed Specification Order Granted under 18 U.S.C. 2518(11)

6. Duration of Intercept

Order or Extension	No. of Days	Date of Application	*Check One* Denied	Granted	Date Order Denied or Granted	Date that a Granted Order/Extension was Modified or Amended, if applicable.
Original Request			☐	☐		Date Modified /Amended
1st Extension			☐	☐		Date Modified /Amended
2nd Extension			☐	☐		Date Modified /Amended
3rd Extension			☐	☐		Date Modified /Amended
4th Extension			☐	☐		Date Modified /Amended
5th Extension			☐	☐		Date Modified /Amended
6th Extension			☐	☐		Date Modified /Amended
Use the last page of the form for additional extensions.	**Total Number of Extensions:** 0				**Total Days Authorized:** 0	

WT-2B State
(Rev. 10/2015)

7. Type of Intercept ***(Check all that apply to this order/authorization)***

Phone - check device(s)	**Oral -** check device(s)	**Electronic -** check device(s)
☐ Cellular or Mobile Telephone	☐ Microphone / Eavesdrop	☐ Computer *(including email)*
☐ Standard Telephone *(land line)*	☐ Other *(specify)*	☐ Digital Pager
☐ Other *(specify)*	_____	☐ Fax Machine
_____		☐ Text Messaging
		☐ App
		☐ Other *(specify)*
		_____

8. Location Shown in Intercept Order ***(Check all that apply to this order/authorization)***

☐ Portable Device - Carried by/on Individual *(e.g., cell phone, pager)*
☐ Personal Residence *(e.g., single family house, apartment, mobile home, rooming house, dormitory)*
☐ Business *(e.g., store, office, restaurant, gym, hospital, school)*
☐ Public Area *(e.g., pay telephone, park, station, airport, library, street, cemetery)*
☐ Other Location *(e.g., motel, prison, jail, vehicle, another specified location not listed)*
Specify
☐ No Location Specified in Order *(either "roving" as shown in item 5, or other circumstances)*
Describe

8A. Judge's Signature ***(Use /s/ or Check Endorsement Box)***

	☐ Judge's Endorsement	Date:	Telephone No.:

8B. Report Prepared By

Report Preparer's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.: Extension:

Title:	Date:

Instructions

When Part 1 (Judge's Report) is completed, do the following:

(1) Click the "Validate Part 1" button to identify any data quality issues with Part 1.
(2) Save a PDF copy of the completed form by clicking the "Save As" button below and assigning a unique file name.
(3) Click the "Submit by Email" button below to submit this form or attach one or more saved PDF forms to an email and send to SD-WIRETAP@AO.USCOURTS.GOV.
(4) Provide an electronic copy of the completed Part 1 to the official making the application.
(5) Retain a copy of the completed Part 1 for the judge's files.

Additional Instruction

Judges stop here. Prosecutors and Law Enforcement Agencies continue to Part 2 of the WT-2 Form.

Validate Part 1 **Save As** **Submit by Email**

WT-2B State
(Rev. 10/2015)

Administrative Office of the United States Courts

Part 2 (Prosecutor's Report - State / County / Local)
Report of Application and/or Order Authorizing Interception of Communications

(To be reported by March 31 for terminated investigations, pursuant to 18 U.S.C. § 2519(2))

Judge Authorizing or Denying the Application

Judge's First Name:	Middle Initial:	Last Name:	Suffix:

State:	Court Jurisdiction:	Court Reference No.:

Prosecution Official Authorizing Application

Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Prosecutor Reference No.:	Agency Reference No.:	Application Date (Original Request):

NOTE: Items listed above should match information entered in Part 1 of Form WT-2.

9. Installation

☐ Never Installed ☐ Installed but Not Used ☐ Installed and Used

10. Description of Intercepts

10A. Termination Date of Interception	10B. No. of Days in Actual Use	10C. No. of Communications Intercepted ☐ Unknown	10D. No. of Persons Whose Comm. Were Intercepted ☐ Unknown	10E. No. of Incriminating Comm. Intercepted ☐ Unknown

10F. Was Encryption Encountered in this Wiretap? ☐ Yes ☐ No	10G. If Yes, Did Encryption Prevent Law Enforcement from Obtaining the Plain Text of Communications Intercepted? ☐ Yes ☐ No

11. Cost (Rounded to Nearest Dollar)

Check the option that applies:

☐ Costs for this wiretap are reported below.

☐ Costs for this wiretap are included on another wiretap form with the following reference number.

Reference Number Type: Reference Number:

☐ Costs for this wiretap are unknown at this time.

11A. Nature and Quantity of Personnel Used to Install, Monitor, and Prepare Transcripts

11B. Personnel Cost		11C. Resource Cost (installation fees, supplies, equipment, etc.)		11D. Total Cost = Personnel Cost + Resource Cost
$	+	$	=	$

12. Results

Check the option that applies:

☐ Results for this wiretap are reported below.

☐ Results for this wiretap are included on another wiretap form with the following reference number.

Reference Number Type: Reference Number:

☐ Results for this wiretap are not known at this time. *(Future results should be reported on the WT-3 Supplementary Report)*

12A1. No. of Persons Arrested	12A2. Arrest Offense (Most Serious):	12B. No. of Motions to Suppress Granted	Denied	Pending

12C. No. of Persons Convicted	12D. No. of Trials Completed	12E. Conviction Offense (Most Serious):	12F. Title/Section of Conviction Offense:

13. Comments and Assessment
Describe importance of the interceptions, drugs and money seizure amounts, impact on community, etc. **DO NOT** include target's name, address, phone numbers, name of gangs, or other sensitive information.

13A. Report Prepared By				
Prosecutor Responsible for Part 2	Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:
Report Preparer	☐ Check if Prosecutor and Report Preparer are the same person.			
	Report Preparer's First Name:	Middle Initial:	Last Name:	Suffix:
	Title:		Telephone No.: Extension:	Date:

Instructions

When Part 2 (Prosecutor's Report) is completed, do the following:

(1) Click the "Validate Part 2" button to identify any data quality issues with Part 2.
(2) Save a PDF copy of the completed form by clicking the "Save As" button below and assigning a unique file name.
(3) Click the "Submit by Email" button below to submit this form or attach one or more saved PDF forms to an email and send to SD-WIRETAP@AO.USCOURTS.GOV.
(4) Retain a copy of the completed form for your files.

Validate Part 2 Only **Validate Parts 1 & 2** **Save As** **Submit by Email**

6. Duration of Intercept ***(Additional Extensions)***						
Order or Extension	No. of Days	Date of Application	*Check One* Denied	Granted	Date Order Denied or Granted	Date that a Granted Order/Extension was Modified or Amended, if applicable.
7th Extension			☐	☐		Date Modified /Amended
8th Extension			☐	☐		Date Modified /Amended
9th Extension			☐	☐		Date Modified /Amended
10th Extension			☐	☐		Date Modified /Amended
11th Extension			☐	☐		Date Modified /Amended
12th Extension			☐	☐		Date Modified /Amended
13th Extension			☐	☐		Date Modified /Amended
14th Extension			☐	☐		Date Modified /Amended
15th Extension			☐	☐		Date Modified /Amended
16th Extension			☐	☐		Date Modified /Amended
17th Extension			☐	☐		Date Modified /Amended
18th Extension			☐	☐		Date Modified /Amended
19th Extension			☐	☐		Date Modified /Amended
20th Extension			☐	☐		Date Modified /Amended
21st Extension			☐	☐		Date Modified /Amended
22nd Extension			☐	☐		Date Modified /Amended
23rd Extension			☐	☐		Date Modified /Amended
24th Extension			☐	☐		Date Modified /Amended
25th Extension			☐	☐		Date Modified /Amended
26th Extension			☐	☐		Date Modified /Amended
27th Extension			☐	☐		Date Modified /Amended
28th Extension			☐	☐		Date Modified /Amended
29th Extension			☐	☐		Date Modified /Amended
30th Extension			☐	☐		Date Modified /Amended
31st Extension			☐	☐		Date Modified /Amended
32nd Extension			☐	☐		Date Modified /Amended
33rd Extension			☐	☐		Date Modified /Amended
34th Extension			☐	☐		Date Modified /Amended
35th Extension			☐	☐		Date Modified /Amended
36th Extension			☐	☐		Date Modified /Amended

Reset

WT-3
(Rev. 10/15)

SUPPLEMENTARY REPORT FOR WIRETAPS REPORTED IN PREVIOUS CALENDAR YEARS

THIS REPORT IS MADE IN ACCORDANCE WITH TITLE 18, UNITED STATES CODE, SECTION 2519. DO NOT REPORT ANY COSTS, ARRESTS, TRIALS, MOTIONS OR CONVICTIONS THAT HAVE BEEN PREVIOUSLY REPORTED ON EITHER THE ORIGINAL FORM 2 OR ON A SUPPLEMENTARY REPORT FORM 3. IF YOU HAVE NO ADDITIONAL ACTIVITY TO REPORT, NO REPORT IS REQUIRED. PLEASE COMPLETE ALL COLUMNS FOR EACH ENTRY. An example is provided below.

Completed copies of the form as well as any questions concerning this form may be sent via e-mail to sd-wiretap@ao.uscourts.gov.

(1) Report Year	(2) A.O. Report Number	(3) Date of Application	ADDITIONAL ACTIVITY DURING CALENDAR YEAR								
			(4) Cost $	(5) Persons Arrested		(6) Trials Completed	(7) Motions to Suppress			(8) Persons Convicted	
				Number	Offense(s)		Granted	Denied	Pending	Number	Offense(s)
Example											
2001	6	06-28-2001	-	3	Gambling, narcotics, conspiracy	2	1	1	-	1	Gambling

Name of the person responsible for completion of this form	Jurisdiction	State Attorney General ❒ Yes	Area Code and Phone Number
Street Address	City and State	Zip Code	Date

Print Save As... Submit

Survey of Nonjudiciary Stakeholders

Carly Giffin
Marvin Astrada

Executive Summary: Survey of Nonjudiciary Stakeholders

In collaboration with the AO, the research division of the Center administered a survey to gather nonjudiciary stakeholders' opinions about the AO's Wiretap Report. While the previous focus groups provided feedback about the reporting process, the survey assessed how the report, including visualizations or dashboards, could be modernized and adjusted to be most useful to nonjudiciary stakeholders.

The survey was sent to 100 individuals representing seven groups: academics, civil society groups (e.g., Brennan Center for Justice, ACLU), international organizations (e.g., U.K's Investigatory Powers Commissioner's Office), journalists, legislative staffers, practitioners, and telecommunication companies (e.g., AT&T). All individuals invited to participate were identified by Center staff or a legislative staffer as being interested in issues surrounding technology and privacy. We received responses from 25 individuals, for a response rate of 25%.

Overall, the responses received were detailed and reflected the interest and expertise that many of our respondents have in this area. A few key themes emerged. The first theme is that, while respondents believe that any visualization of available wiretap data would be at least slightly useful, they are most interested in being able to download or otherwise get access to the data in the least edited form available. Several commentators mentioned this as being more important to them than any specific visualizations offered by the AO.

The second theme is that respondents are interested in having the ability to filter the data in as many ways as possible. The third, related, theme is that respondents would like to see the AO present wiretap information by type of surveillance (e.g., cell phone, messaging application) whenever possible. Several respondents further expressed interest in getting more nuanced information about type of surveillance. For example, when a wiretap is approved for a cell phone, does that cover just the phone calls or all digital information transmitted over that cell phone?

The fourth and final theme was a frustration with prosecutors filing many wiretap reports "late"—that is, outside of their yearly window. While respondents seemed to realize that good reason(s) for such exceptions did exist, they worried that these exceptions were being made too often and could lead to the data being misleading or even inaccurate if it were not carefully updated.

Respondent Demographics

This survey was designed to solicit opinions from nonjudiciary stakeholders about the AO's Wiretap Report. The questions were developed by staff from the Center's research division after discussions with the AO's JDAO, Office of Legislative Affairs (OLA), and Office of

General Counsel (OGC). The survey was initially sent on April 12, 2021, and, after an extension to encourage greater participation, closed for most recipients on April 29, 2021.[15]

The initial survey invitation and several reminders were sent to 100 people, and 25 people responded for a response rate of 25%.[16] The 100 individuals were identified by a legislative staffer and Center staff as having an interest in issues concerning privacy and technology policy. We received nine (36%) responses from academics, six (24%) responses from legal practitioners, five (20%) responses from people who work at civil society groups, two (8%) responses each from journalists and people working with international organizations, and one (4%) response from a legislative staffer.

On the initial page of the survey, respondents were encouraged to either watch a video or download slides concerning the AO's reporting requirements and authority under the Wiretap Act (18 U.S.C. § 2519(3)). We installed a timer on this page to see if people stayed on the page long enough to watch the video or view the slides, and the mean time respondents spent on this first page was about 4.5 minutes or 270 seconds. However, this mean is artificially inflated by three respondents who each spent more than 20 minutes on this page. While it is possible that they spent this time watching the video and reviewing the slides, it is also possible that they left the survey open while they attended to other tasks. In all, including these three respondents, only seven respondents spent enough time on the initial slide to watch the entire video. An additional two respondents spent between three and four minutes on the slide, arguably long enough to read some of the key slides. Sixteen respondents spent a minute or less on this initial slide, about the time needed to read the text on the page. Notably, though, several respondents left comments that display a keen familiarity with the Wiretap Act, so perhaps not all who skipped the video were uninformed.

Results

Technologies to be Captured

Respondents were first asked which technology they would like to see captured in the AO's wiretap reporting form. Overall, most respondents thought all listed technologies should be captured, though digital pagers and fax machines received slightly less endorsement, likely because these technologies are becoming obsolete. See table 1.

15. After reviewing responses, we found that only one legislative staffer had responded. The AO's OLA reached out to a legislative staffer who had been in touch about the project, in hopes that the staffer could encourage more participation by this key stakeholder group. The survey was then sent out again to legislative staffers on May 18, 2021, and closed on May 28, 2021. No additional responses were received.

16. Not all respondents answered each question. Some chose to answer only one or two questions, perhaps based on their interests or expertise.

Table 1: Surveillance Technologies that Should be Captured in the Wiretap Report

What surveillance technologies should be captured on the AO wiretap reporting form? *Please check all that apply.*	
	f
Cellular, Mobile, and Smart Telephones	23
Standard Telephone	21
Microphone	21
Computer	23
Email	22
Digital Pager	19
Fax Machine	19
Text Messaging	22
Phone Messaging Applications (e.g., WhatsApp, WeChat, Facebook Messenger)	22
VoIP	22
Smart Speaker (e.g., Alexa)	22
Videoconferencing Platforms (e.g., Zoom, Teams)	23
Other	12

The "Other" responses represented a broad range of possible technologies, but one technology mentioned by more than one respondent was the "internet-of-things" such as cars, refrigerators, and other appliances that are connected to the internet. Full "Other" comments to this question are presented below.

1.	any electronic communications required under ECPA
2.	Any IoT device with sensors
3.	chat
4.	VPNs and servers
5.	Home WiFi router / cable modem, connected car, smart watch,
6.	See comment below[17]
7.	Internet-of-Things devices, Automotive communications, Internet-connected cameras and sensors
8.	Social Media, ISPs / Internet Traffic
9.	Internet of things (fridge, coffee machine, etc.) and vehicles
10.	browser search terms
11.	Cell site simulators

17. Despite this comment, this respondent left no other comment in the survey, instead answering only the multiple-choice questions.

Keeping the Wiretap Reporting Form Current

Respondents were next asked to provide any information they believed would be helpful for the AO to consider while working to maintain the currency of the wiretap reporting form. While each response provides a unique contribution, three noted that the number of later supplements (WT-3s) complicates their ability to accurately interpret the data. Respondents wanted the late supplements rolled into the initial report and questioned why so many submissions were allowed to be late. Full responses to this question are provided below.

1.	Annual reporting is generally good. The most challenging part of dealing with the AO's data is combining what's in the annual reports with what comes in the later supplements; it would be helpful if the AO could better integrate the two so that there is one place to go for a complete picture, even if that picture necessarily changes a little over time.
2.	The AO should better enforce reporting requirements such that there are fewer late reports. In 2018, the number of late reports was almost equal to the number of original reports. Late reports make it very difficult to assess the true number and scope of wiretaps each year.
3.	One a year is fine.
4.	Include space for open-ended responses regarding surveillance mechanisms, then make additions to the list of surveillance mechanisms in subsequent years based on open-ended responses.
5.	I would think the AO would want to know why such a large % of reports are late. It is not enough for the field to simply assert reporting would endanger an ongoing investigation, especially when the Wiretap Report is an annual report. Late filed reports skew the credibility and relevance of the Report, and it is unclear whether all wiretaps actually ever get reported. For the Report to be both current and relevant, tightening the reporting procedures and bases for delay (which the statute in any case does not include), would be most helpful.
6.	There is a pressing need for greater transparency around how warrants, among other legal tools, impact privacy on the internet. As these processes are applied to the internet, and data brokers (or other aggregators of information), the potential for exposing private information skyrockets. To stay current, it would be helpful to see the AO strengthen reporting around these applications and the number of people affected.
7.	Rather than just capturing data about the kind of device/account that is being wiretapped, it would be very helpful to capture data about the means by which the government conducts the wiretap. In particular, it would be extremely helpful if the wiretap report captured instances in which the government engaged in self-service surveillance (rather than going to a provider for assistance), such as when the government uses a stingray/cell site simulator or hacks into the phone/computer of a target.

	Self-service surveillance raises far greater privacy/civil liberties concerns, because providers often act as proxy for the user, and push back on improper requests. If the government can conduct surveillance all by itself, there is no one to push back.
8.	"Computer" seems overbroad: it would be better to break wiretaps of computers into at least three categories: installation on target's premises (e.g. key logger); installation at direct upstream provider (e.g. broadband provider or cell provider); or installation elsewhere in the cloud or network (e.g. upstream provider).

Usefulness of Different Types of Data Displays

Respondents were asked to rate the usefulness of different data displays. No respondent chose "not at all useful" for any display, but two types of displays were rated the most useful. Eighteen respondents (72%) said that the ability to download data records would be "extremely useful," and 13 respondents (52%) said that the ability to filter information would be "extremely useful." The one "Other" response simply said, "[p]rofessional visualization experts." See table 2.

Table 2: Usefulness of Static and Other Data Display Types

In the AO's annual wiretap reports, wiretap information is displayed as static summary data tables and graphs. Please rate the usefulness of static and other types of data displays.

	Not At All Useful	Slightly Useful	Moderately Useful	Very Useful	Extremely Useful
Static Summary Data Tables	0	0	7	9	5
Static Graphs	0	1	7	9	4
Interactive Dashboards	0	0	5	10	5
Ability to Download Data Records	0	0	1	2	18
Ability to Filter Information (e.g., by geographic location, year)	0	0	1	7	13
Other	0	0	0	1	1

Ability to Filter Data

The next question asked respondents which methods of filtering information would be most useful. Again, respondents indicated that most of these filters would be at least "moderately useful," but two kinds of filters received the greatest endorsement. Eighteen respondents (72%) said that filtering by type of surveillance would be "extremely useful," and 13 respondents (52%) said that filtering by state versus federal jurisdiction would be "extremely useful." See table 3.

Table 3: Usefulness of Data Filters

Please rate the usefulness of the following ways **to filter** the wiretap intercept data, **regardless** of whether it is presented in a static table, static graph, or interactive dashboard.

	Not At All Useful	Slightly Useful	Moderately Useful	Very Useful	Extremely Useful
Year of Intercept	0	1	1	7	12
Geographic Region	0	0	4	5	10
Criminal Offense	0	0	2	8	10
Type of Surveillance (e.g., landline, cell phone, email)	0	2	0	1	18
State versus Federal Jurisdiction	0	1	1	6	13
Whether an Arrest or Trial Results from the Wiretap	1	0	4	5	11
Other	0	0	0	0	6

The six "Other" comments were each unique; see full comments below.

1.	All fields should be filterable unless there's a compelling reason not to
2.	number of devices covered by wiretap
3.	It is unfortunate that the number of people intercepted is no longer tabulated
4.	whether arrest or data resulted from wiretap of defendant or of another party
5.	Cost
6.	Agency

Usefulness of Data Displays for Different Kinds of Data

Respondents were asked to indicate how useful a data display would be for certain kinds of data, regardless of the kind of display (static, interactive, etc.). As with the prior tables, we find that most respondents would find displays of all these data types to be "extremely useful." However, a few categories were endorsed slightly more than others. Seventeen respondents (68%) said that displays showing the number of each type of intercept would be "extremely useful," and 15 respondents (60%) each said that displays showing the number of overall intercepts per year, the number of federal intercepts per year, the number of federal denials per year, and the number of times encryption prevented law enforcement from obtaining plain text of a communication would be "extremely useful." See table 4.

Table 4: Usefulness of Data Displays for Different Kinds of Data

Please rate the usefulness of data displays for each kind of data, **regardless** of whether it is presented in a static table, chart, or interactive dashboard.

	Not At All Useful	Slightly Useful	Moderately Useful	Very Useful	Extremely Useful
Number of **Overall Intercepts** Per Year	0	0	3	3	15
Number of **Overall Denials** Per Year	0	0	1	7	13
Number of **Federal Intercepts** Per Year	0	1	1	4	15
Number of **Federal Denials** Per Year	0	1	1	4	15
Number of **State Intercepts** Per Year	0	1	1	6	13
Number of **State Denials** Per Year	0	1	1	5	14
Number of Each Type of Intercept (e.g., cell phones, computers)	0	0	2	2	17
Average Duration of Orders	0	2	1	7	11

	Not At All Useful	Slightly Useful	Moderately Useful	Very Useful	Extremely Useful
Average Duration of Orders Including Extensions	0	1	2	8	10
Number of Extensions	0	0	2	8	11
Number of Extensions by Type of Technology (e.g., cell phones, computers)	0	3	1	6	11
Expenses Related to the Surveillance	0	2	6	7	6
Number of Incriminating Communications Intercepted	0	2	2	7	10
Number of Orders in Which Encryption was Encountered	1	0	1	7	12
Number of Times Encryption Prevented Law Enforcement from Obtaining Plain Text of an Intercepted Communication	1	0	0	5	15
Number of Arrests, Trials, and Convictions Resulting from Interception	0	1	3	7	10
Other	0	0	0	0	3

Of the "Other" responses, two said they wanted to be able to see how many people were covered by a particular wiretap, and the third wanted to be able to see how many times the government was able to overcome encryption. Full responses are below.

1.	Number of individuals covered by each wiretap
2.	Average number of people intercepted per order
3.	The number of times encryption was able to be circumvented through tools or other techniques

Additional Information to Consider in Updating Displays of Wiretap Data

Respondents were asked to provide any additional information they believed might be helpful for the AO to consider during the process of updating their displays of wiretap data. Each comment presented unique ideas, though several said the most important consideration was being able to access the raw data in an easy to use format. See full comments below.

1.	In general, the AO's raw data is good and very helpful. More detail would always be better. In some instances, it might also be helpful to be able to determine where a particular case stands. For example, there are instances in which wiretaps result in no arrests or prosecutions because they weren't productive (or for other reasons), and cases in which a wiretap hasn't *yet* resulted in an arrest because it's still ongoing even if the intercept order itself has expired. That seems like an important distinction. Also, my understanding is that wiretaps are frequently used as the basis for seizures that aren't necessarily associated with an arrest. It would be informative to be able to track assets or contraband seized because of a wire.
2.	There are a number of stakeholders here, so I'd expect that they have very different demands, which would indicate a need for different survey questions. Ultimately, the data is the most important part. If it's available, then people can figure out the rest on their own. I would invest in that being as complete and accurate as possible, and let the rest of the questions around what to include and what to show fall by the wayside as much as legally possible.
3.	It would be extremely helpful if the AO also provided data on the approximate number of persons whose communications were intercepted as well as the number of motions to suppress made with respect to such interceptions, and the number granted or denied (both of which are required under 18 U.S. Code § 2519).
4.	Besides number of people intercepted per order who were not identified on the order, it would be great to know to how many people notice was given, whether minimization occurred, and what efforts were made to investigate before the order was issued. But I realize the latter 3 data on the latter three points are very difficult to collect.
5.	Moving to a completely cloud-based system would allow greater access and analysis of the data. For those of us that have mined the Reports for insights over the years, the AO has made progress in making the data more available in a useful form, and this effort seems to be in line with increasing such accessibility. There are database experts who could give the AO more guidance than end user lawyers and policy-makers, but thank you for asking for this input.
6.	The wiretap report has lots of problems, but they're not related to how the data is displayed. The problem is that courts are not capturing the right information. Fixing the wiretap reports and making them more useful to policy makers will require capturing additional data at the time that the wiretap order is approved.
7.	The most important thing is to provide the raw, underlying data in an easily data file format, such as JSON or CSV. The FJC should also publish a detailed codebook explaining each data field in depth.

8.	Number of applications granted on resubmission after denial (broken into total, federal and state).
9.	In my own research and teaching, the raw data is what's most valuable. Generating tables, figures, and interactive presentations from the data is easy.
10.	It would be very helpful to know how often previously authorized wiretap data is subsequently disclosed in court, and by whom, pursuant to the testimonial exception. Here is an analysis of the issue from my perspective (footnotes with statutory and case law citations are in the appendix of this document available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3428607): Federal law today generally prohibits the providers of wire and electronic communications services from divulging the contents of their users' communications. The statutory text expressly exempts disclosures to law enforcement under certain circumstances, but lacks any express exception specifically for disclosures to criminal defense investigators. Therefore, at first glance, the text appears to create a privacy asymmetry. However, I classify the wiretap law's service providers regulations as symmetrical because the statutory text also includes an express exemption authorizing "any person" to disclose the contents of authorized wiretap materials in courtroom testimony. That exemption could, and I submit should, be construed neutrally to permit either law enforcement or defense investigators to subpoena service providers for the contents of certain communications (specifically, communications that the providers previously intercepted incident to performing their service). The argument for a symmetrical reading proceeds as follows. The statute provides that any person testifying in court may disclose the contents of authorized intercepts. The statute also authorizes service providers to intercept communications incident to performing their service. Therefore, service providers testifying in court may disclose the contents of communications that they intercepted incident to performing their service. Either law enforcement or defense counsel should thus be able to compel such testimony from service providers using a subpoena ad testificandum. And, by extension, either law enforcement or defense counsel may also be able to compel the service providers to disclose the intercepted communications directly, pretrial, using a subpoena duces tecum. Further, my textual reading of the testimonial exception would likely entitle criminal defendants not merely to subpoena service providers for any communications that the providers had previously intercepted incident to their service, but also to subpoena wiretap materials from law enforcement. Such a reading would further strengthen my symmetry classification. Thus, while the statute's express exemptions permitting service providers to disclose contents to law enforcement might be broader than the "any person" testimonial exception, defense counsel may be able to use the testimonial exception to access anything that law enforcement has previously obtained.

	While I have been unable to locate any case law addressing this textual argument directly, current doctrine contains some reasons to think it might succeed, and some reasons to think it might not. The federal courts have weighed in on the related issue of whether the "any person" testimonial exception permits civil litigants to subpoena law enforcement for pretrial disclosure of authorized wiretap materials. The Ninth and Fifth Circuits have construed the statute to permit civil litigants to do this, although in both cases the litigant seeking disclosure was another government entity, namely the IRS. The Eighth Circuit held explicitly that the testimonial exception is not available to nongovernmental civil litigants (without commenting on whether it might be available to criminal defendants). Meanwhile, the Second Circuit has acknowledged that a plain text reading of the testimonial exception could support permitting any litigant to subpoena law enforcement for authorized wiretap materials, but ultimately declined to construe the statute in that manner on the basis of Title III's legislative history.
11.	I worry that the number of electronic intercepts is being underreported and that where the intercept includes text messaging it may be listed as a wire.
12.	It would be good to know if the data was collected with the help of a third party pursuant to the technical assistance provision of the statute, what type of technical assistance was provided, and whether there was litigation over the appropriateness of the government demand for that assistance.

Overall Comments and Thoughts about the Collection and Dissemination of Wiretap Data

Lastly, respondents were asked to share any final thoughts about the AO's collection and dissemination of wiretap data, keeping in mind that the AO may lack the authority or capability to address every suggestion. Some comments were short and straightforward; see comments 1 and 5, for example. Most of these comments, though, were detailed and showed the respondents' interest in, and knowledge of, this issue. The only theme that came up in multiple comments was concern about the timing of reports from prosecutors. One respondent worried that the amount of time that elapses before the forms are filled out might cause some inaccuracies simply due to forgetfulness. Two others were concerned about these late reports in and of themselves, arguing that they lessen the utility of the wiretap report.

1.	Data, data, data.
2.	These are absolutely critical data, and I'm *so grateful* that you are collecting them. My primary concern would be areas where the ways in which the data are reported creates uncertainty about how to interpret them (e.g., reporting only the most serious offense) or raises concerns about accuracy (e.g., I'm never sure how much to trust the information from the prosecutor's reports, given that I think they might be filled out well after the information from the wiretap is actually used in trial, and some of the terms are not well defined - e.g., how "related to" the wiretap does an arrest have to be to be counted). I'd strongly recommend doing interviews with judges and prosecutors asking them how

	they fill out the reports in order to identify potential inconsistencies in this process, and see what could be done to make the process more accurate.
3.	Section 2519 of Title 18 requires any judge who issued, denied or extended a wiretap order during the preceding year to make a report to the AO each year. There are no exceptions in the statute for reporting the actual number of wiretaps authorized by the courts. None. Federal and state prosecutors likewise are required to report wiretap information each year. It is mandatory and there are no exceptions to reporting here either. In June of each year, the AO is required to provide Congress "a full and complete report concerning the number of applications for orders authorizing or approving wiretaps and the number of orders and extensions granted or denied during the preceding calendar year." In sum, all orders issued, denied or extended in the prior year should be reported to the AO and ultimately to Congress. No exceptions. Yet the AO regulations give prosecutors a break and allow them to not report in a timely way, and perhaps at all inasmuch as there seems to be no audit trail or penalty for nonsubmission of data. The Report therefore presents a skewed image of surveillance and may mislead Congress and the public about the scope and nature of surveillance. The loophole on reporting should be closed or extremely limited. The AO ought to take a lookback over 10 years of reporting to determine whether the delays have been legitimate or rather serial neglect by certain offices. An IG-like review would not hurt. In the interest of transparency, it would be a worthwhile endeavor. If the data in the Report becomes suspect, its reliability and usefulness goes away, and that would defeat the intent of Congress in requiring such reporting.
4.	Smartphones are computers that happen to make phone calls. However, the wiretap reports do not currently differentiate between a wiretap authorizing an interception of the "telephone" service on a target's smartphone vs. the data connection which then enables the government to intercept web browsing and "over the top" apps like Signal, WhatsApp, etc. Given the fact that the vast majority of wiretaps target cell phones, it isn't clear from the reports what in fact is being authorized - are law enforcement agencies tapping every bit of data going in and out of the phone, or are they just tapping the telephone service? The reports would be far more useful if they captured the nature of the specific services/apps on a device that the court is permitting the government to wiretap, and if the court is permitting a wiretap of all data going in and out of a device, the reports should capture this. The wiretap act includes statutory "assistance" authority, in which the government can compel the assistance of a third party, such as a landlord. In 2003, the 9th circuit held that there are limits to how far the government can go in compelling such assistance - see: The Company v. United States, 02-15635 (349 F.3d 1132; United States Court of Appeals, Ninth Circuit; Nov. 18, 2003). However, the wiretap reports do not currently capture how frequently courts issue orders compelling providers to deliver new code to customers' devices (e.g., backdoors), or engage in other forms of surveillance assistance that stray from the norm of just turning over data flowing through their networks. These are often the most controversial forms of compelled surveillance assistance, raise serious

	cybersecurity questions, put the global reputations of providers at risk, but there is no data on their frequency, making congressional oversight next to impossible. It would also be helpful for the wiretap report to capture information on how long the wiretap orders themselves remain sealed, and how many extensions of the sealing the government asks for. Every so often, the government undoubtedly obtains wiretaps on the wrong numbers, accounts, and devices. Either because of an error by the government or the provider (for example, swapping 2 digits in a phone number). The wiretap report doesn't currently capture any information about such accidental/improper wiretaps. As an illustrative example from the area of foreign intelligence, NSA apparently accidentally intercepted a large number of calls in the Washington DC area, because a "programming error confused the U.S. area code 202 for 20, the international dialing code for Egypt." See: https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html. While the wiretap report obviously won't capture NSA's mistakes, it seems reasonable to assume that law enforcement agencies also make mistakes too, and the wiretap report should capture that.
5.	Address the seeming discrepancy in the numbers reported by the AO and those reported by companies (https://cyberlaw.stanford.edu/blog/2016/11/wiretap-numbers-still-dont-add).
6.	Transparency is crucial to the work I do in this area so as much data and other information that can be revealed will be very helpful in explaining to the public what this all means and why they should care.
7.	The AO's reporting on encryption is very ambiguous and limited. First, what does it mean for a law enforcement agency to "encounter" encryption? Does that mean end-to-end encryption (e.g., Signal messaging), or does it also include transport encryption (e.g., TLS/SSL)? Types of encryption, like types of electronic communications, are not interchangeable. Each type has different privacy properties and implications for law enforcement. Second, what does it mean for encryption to "prevent" law enforcement from obtaining communications? Does that mean all attempts to obtain the communications were unsuccessful (e.g., alternative investigative methods failed, such as searching communications backups or seizing a device), or does that mean just the one method of obtaining the communications was unsuccessful (regardless of whether alternative methods were successful)? There is a significant difference between these two interpretations, because one includes only possible impediments to law enforcement investigations and the other additionally includes the routine law enforcement practice of adapting alternative methods as an investigation proceeds. Third, the reporting on encryption focuses exclusively on the execution of wiretap orders. That omits essential context: when wiretaps encounter encryption, are there still arrests, trials, and convictions? Those are much more important big-picture issues for

	encryption research and policy, in comparison to whether specific interception methods are unsuccessful or whether specific communications are unavailable. In my reading of 18 U.S.C. § 2519, the AO has authority to require reporting of this information.
8.	Late filed reports undermine the integrity and utility of these congressionally mandated reports. Chronic abusers should be publicly highlighted, like they are with the 6 month pending motion reports.

Nonjudiciary Stakeholders' Wiretap Report Focus Groups

Marvin Astrada
Carly Giffin

Executive Summary: Nonjudiciary Stakeholders' Wiretap Report Focus Groups

As part of the AO's assessment of its Wiretap Report, the Center conducted two focus groups in July of 2021. The focus groups were comprised of nonjudiciary stakeholders who had indicated in the survey a willingness to participate in a focus group.

The focus groups sought to obtain feedback and suggestions about the Wiretap Report from people who use it in their work. The goal was to provide the AO with insight into how the AO might improve the clarity, accuracy, and usefulness of the Wiretap Report. While some of the suggestions focused solely on the presentation of data in the Wiretap Report, many implicated the data collection process, and these latter suggestions complement those given by prosecutors and judges in the earlier focus groups. All participants made it clear that they valued the information provided by the Wiretap Report, and that their suggestions were aimed at improving what they considered a vital resource for their teaching, reporting, oversight, or business endeavors.

Incompleteness of the Wiretap Report

- Participants' largest concern was that the information in the Wiretap Report is incomplete to the point of being misleading. This incompleteness was attributed to poor state and federal compliance with reporting requirements. The sharp contrast between the data collected by telecommunication companies and those collected by the AO was highlighted by participants. Telecommunication companies' data have not shown any significant decline in the number of wiretap orders they are receiving, but the AO's data reflect the opposite trend. Some participants believe that this state of affairs compromises the integrity of the AO's data collection process and raises questions about the accuracy of not only the Wiretap Report, but other reports as well.
- Access to detailed, clear, updated, comprehensive, and precise wiretap data, provided in an accessible, efficient, and user-friendly format, emerged as a central theme of the focus groups. While the incompleteness of the data concerned participants, they appreciated the ability to download the data from the tables and hoped that this access was expanded.

Suggestions to Update and Maintain the Wiretap Reporting Forms and Data Collection Process

- Most participants thought the reporting forms require updating to reflect the considerable changes that have transpired in the realm of surveillance technology and privacy. Participants thought the Wiretap Report should highlight techniques that encroach on privacy when the government starts using them.

One participant disagreed that the form needed updating, noting that the major categories have not changed; rather, it is the specific telecommunication providers who have changed.

- Participants suggested that reporting might be improved by providing state and federal agencies with a more explicit, uniform, and formalized set of instructions regarding reporting requirements. It was suggested that these instructions could include definitions of key terms that could later be shared with users of the Wiretap Report.

Suggestions to Improve the Wiretap Report

- Participants supported the idea of providing an explanation with all the tables in the Wiretap Report detailing what data were represented (e.g., what states had reported) and discussing the AO's policy for updating the tables with information submitted late by prosecutors.
- Most participants queried what steps have been or will be taken to verify the accuracy of the information provided to and published by the AO going forward. Several participants wanted clarification as to why the AO accepts incomplete, late, and nonreporting.

Participant Misapprehensions

- There were general and specific misapprehensions and questions pertaining to the AO's and the courts' capacity to proactively collect, organize, and analyze wiretap data, and whether the AO could act independently of congressional mandates to compel reporting. The AO's authority and capacity to procure comprehensive and precise wiretap data was a prominent topic of discussion.

Discussion

The final stage of the Center's study of the Wiretap Report was two focus groups conducted in July of 2021. The focus groups were comprised of nonjudiciary stakeholders who had indicated in the survey that they would be willing to participate in a focus group. Most of the participants were academics, with the remainder being a journalist, a senate staffer, counsel for a telecommunication company, and an attorney working with a civil society group.

While the first set of focus groups explored the process of providing the information that becomes the Wiretap Report, these focus groups sought to solicit more feedback and suggestions about the Wiretap Report itself from people who use it in their work. Based in part on the findings of the survey, the JDAO was specifically interested in two topics: 1) which types of technology should be tracked in the Wiretap Report, and 2) how to keep the reporting forms up to date. Two groups of participants engaged in two separate (virtual) sessions. The FJC staff asked structured and unstructured questions related to these two topics as well as to solicit more general feedback and suggestions about how the Wiretap Report is used by nonjudiciary stakeholders and how it could best serve these users.[18]

We first describe participants' overarching concern with the Wiretap Report before presenting the suggestions for improvement that they provided. These suggestions are broken into two sections: suggestions for updating to the wiretap reporting forms and data collection process, and suggestions to improve the Wiretap Report. Finally, we discuss some of the misapprehensions that participants held about the AO's duties and capabilities concerning the Wiretap Report and how these misapprehensions might be corrected. Regardless of their concerns or misapprehensions, participants all agreed that the Wiretap Report was useful to their work, and they emphasized that their goal was only to have the information provided in the most accessible, efficient, comprehensive, and user-friendly format possible.

Incompleteness of the Wiretap Report

The incompleteness of the Wiretap Report was the most prominent topic of discussion. Many comments by participants revealed an underlying concern that the information reported by the AO is both incomplete and imprecise—causing it to be inaccurate. Participants were particularly concerned about the limited number of states reporting, as well as the number of late reports submitted by both state and federal prosecutors. Some participants brought up the sharp contrast between the data collected by providers and those collected by the AO. Providers' data have not shown any significant decline in the

18. Telecommunication companies are seen primarily as providers of information to courts and the public. However, our focus group revealed they also use the Wiretap Report to help them plan the resources that may be necessary to respond to wiretap orders. Thus, they are also users of the Wiretap Report for the purposes of this study.

number of wiretap orders they are receiving, but the AO's data appear to reflect the opposite trend. Further, participants said that some of the technology categories tracked are so broad (e.g., computer, cell phone) that it made interpreting the data nearly impossible.

This incompleteness was troubling to participants because they value the information provided by the Wiretap Report. They see it as a vital source of unbiased information that they use in their work. Participants reported using the information from the Wiretap Report in a variety of ways. The information in the Wiretap Report is presented to students to give a sense of how wiretaps are used nationally. It is written about for general audiences who are interested in how the government surveils its citizens and others. It is studied by legislative bodies to provide oversight and inform legislation, and it is used by telecommunication companies to plan what resources might be needed in coming years to respond to wiretap orders. Broadly, our participants used the Wiretap Report to understand both the current level of wiretap use throughout the country and how the use of wiretaps has evolved, in prevalence and in the kinds of technologies intercepted.

All of these uses are complicated by deficient data that can result in erroneous or less-than-accurate conclusions about surveillance, privacy, and government accountability. Participants noted that they were unsure how much data were being represented by the report, and that this lack of certainty made interpreting the data difficult. Users were, quite simply, not sure what caveats or explanations they should provide or consider when presenting and using the data, and they were concerned that they sometimes gave students, clients, or the public an inaccurate impression of wiretap activity throughout the country. Further, one participant noted that the existence of documents like the Wiretap Report serves as an example of transparency for other countries, but the effect of this example is diminished if the report is not "comprehensive."

Some participants went further, expressing concern that the incompleteness of the Wiretap Report compromises its integrity, and perhaps even that of AO reports in general. These participants noted that until the providers' reports were available, they had no idea that the AO's report was so incomplete, which then lead them to question the accuracy of other reports published by the AO, and even the AO's ability to present accurate data.

To better understand the incompleteness, several participants asked for clarification as to why the AO accepts incomplete and late submissions, as well as nonreporting. Participants asked what steps, if any, have been or will be taken to verify the accuracy of the information provided to and published by the AO. Some of these questions represented misapprehensions about the scope of the AO's enforcement authority, discussed in more detail below.

Participants believe that the courts are the first line of defense for privacy, and when the government starts using a new technology that encroaches on privacy, that technique should be tracked in each relevant table of the Wiretap Report. Participants offered many suggestions to make the Wiretap Report more complete, and therefore more accurate and useful. We have arranged these suggestions into two categories: suggestions that focus on the reporting forms and data that feed into the Wiretap Report, and those that target the presentation of the Wiretap Report itself.

Suggestions to Update and Maintain the Wiretap Reporting Forms and Data Collection Process

One set of suggestions was to update the official reporting forms, an action that would require the cooperation of the DOJ and members of the judiciary. All but one participant said that the official reporting forms should be updated to include more modern and nuanced technology categories. Participants said this would be helpful for them as users, and they believed it would make reporting more accurate. Prosecutors in the earlier focus groups agreed, saying that modernization would make reporting easier, and, therefore, perhaps more robust. One nonjudiciary participant did mention that it was difficult to know which technologies to suggest be included because they could not be aware of all technologies currently being surveilled. However, participants were able to provide some specific suggestions. Technologies and other information that the nonjudiciary participants suggested should be tracked were:[19]

- Pen registers
- Trap and trace
- Geofencing
- Turning on of laptop and cell phone microphones
- Number of targets per application[20]
- Extent of the wiretap (i.e., is it monitored 24 hours a day, or is some minimization done)
- Provider or type of facility the order was issued to[21]

Participants also suggested that providing more nuanced information about some of the technologies currently tracked would make the data easier to interpret. Again, prosecutors had also indicated that this would make it easier to submit their reports. The categories nonjudiciary participants asked to be differentiated were:

Category to Differentiate	How to Differentiate the Category
Multiple Device Orders	Delineate each device covered in an application
Cell phones	Specify what data are being captured: telephone, geographic data, messaging applications, etc.
Computer	Specify what data are being captured: emails, searchers, social media accounts.
Encryption	Delineate which kind of encryption is being encountered.

19. Additional suggestions for technologies to track can be found in the survey responses, on page 37.

20. Wiretap table 4 does list the average number of people intercepted, but participants additionally wanted to know how many of those intercepted were a target on the wiretap application. Wiretap table 4 for 2020 can be found at https://www.uscourts.gov/statistics/table/wire-4/wiretap/2020/12/31.

21. This request goes beyond the statutory language, but we include it to provide the fullest representation of the focus groups discussions. It was further suggested that even if the AO did not release the provider information, it could be used to check the accuracy of their own numbers against provider reports.

In addition to these specific suggestions, several participants advocated for a way to record various kinds of surveillance that do not fit into the categories listed on the form, and this arose as the only clear suggestion for keeping the form up to date moving forward. The reporting forms could be modified to include an open-ended box on the form, and prosecutors could be instructed to list any technology not included in the current form in that box. The AO could periodically convert popular open-ended responses into set options on the form for following years.

Another set of suggestions does not address updating the forms directly but rather implicates the data collection process more broadly. First, some participants proposed that perhaps wiretap applications, at least federal applications, could be tracked through CM/ECF. This would obviate the need to follow up with federal judges and prosecutors as well as alleviate some of the data quality issues the AO currently faces (e.g., faxed forms with nearly illegible handwriting). This suggestion was also made by some of the federal prosecutors in the earlier focus groups. AO staff present in the focus group noted that this might address some of the issues they currently face, but that getting consistent implementation in all districts would still present a challenge and require the cooperation of the district personnel.

Other suggestions about the data collection process implicated the AO's communication with the reporting judges and prosecutors. One participant suggested that to better ensure compliance it would behoove the AO to have the rules and the reporting process articulated prominently and explicitly in conjunction with a more precise and formalized process of data collection. For instance, one participant noted that the statute only indicates the month in which reports are due; jurisdictions/agencies may thus be incentivized to either report late or not report all because there is not a precise timeline or window for reporting. Providing more specific dates or timelines in the rules may give the reports more priority and thereby increase reporting.

Another communication that could be improved concerns states without any applications. Participants proposed that the AO update its instructions so that states without any wiretap applications the previous year were instructed to submit a report to this effect. While the AO still does not have the ability to enforce this instruction, it is possible that some states believe that if they have no applications to report, submitting paperwork is unnecessary. An instruction from the AO stating otherwise could correct that belief. Currently, the AO does release Wiretap table 1, which lists the states that reported wiretaps. It is not possible to tell from this table, however, if the state truly had no wiretap applications or if the state simply did not submit a report to the AO.[22] Participants would like this distinction to be made clear, and instructions to submit a report even if no wiretap applications were submitted could increase the accuracy of Wiretap table 1. Several participants believed that listing which states did not report would not only be useful for data clarity, but it also might serve as an incentive for more states to report. If publicly listing the

22. See https://www.uscourts.gov/statistics/table/wire-1/wiretap/2020/12/31 for Wiretap table 1 for 2020.

nonreporting states was considered untenable, one participant suggested that the list of nonreporting states should at minimum be released in the AO report sent to Congress.

One final suggestion may help address the incompleteness of data in a more holistic way. One participant suggested that it may be worthwhile to survey some of the nonreporting jurisdictions to get a better understanding of why they are not submitting their reports. Some jurisdictions may not have any applications to report, while others may lack information about the requirements or find the reporting process too difficult. Differentiating between these possible causes could help the AO devise ways to increase reporting.

Suggestions to Improve the Wiretap Report

While the previous suggestions were directed at the wiretap reporting forms and data collection process, other suggestions were directed at the presentation of the Wiretap Report itself.

One strongly endorsed suggestion about the presentation of the Wiretap Report was for the AO to display an explanation with each table that made clear what data was represented. Specifically, participants wanted a list of the states that had reported, so that it would be immediately clear to the reader that not all states were represented. Participants would also like the explanation to note that prosecutors send in later supplements so that readers would be alerted to the fact that some federal data may also be missing from the tables. Participants felt this would greatly improve the user's ability to properly interpret and use the information provided by the Wiretap Report.

Another clarification that nonjudiciary stakeholders requested is the clear definition of terms. Participants said it would help users to analyze the data contained in the Wiretap Report if they knew the precise definitions prosecutors had in mind when reporting. Without definitions, one participant referred to the prosecutors' reports as "wildcard[s]" because it was not possible to ensure that the prosecutor understood the terms in the same way that the reader did. One example provided by a participant was encryption. There are several different kinds of encryption, and without standardized definitions and more nuanced technology categories, it is not clear what is being reported. This echoes suggestions that prosecutors provided in the earlier focus groups asking for definitions or clearer instructions to accompany the reporting forms. One set of instructions and definitions could be provided to prosecutors and then later included with each table in the Wiretap Report. This would help prosecutors reporting, and it would give users of the Report a better understanding to use in their scholarship, reporting, and preparation.

In addition to clarifying explanations and definitions, participants also suggested that related data be more clearly linked in the tables of the Wiretap Report. Specifically, participants requested that the AO work to find a clearer, more consistent way to link supplemental reports filed by prosecutors (WT-3s) with the original reports they reference. While participants came to understand that the AO lacked an enforcement mechanism to increase overall timely reporting, they argued that it is still within the AO's power to update earlier tables or devise some other method that ensures that a reader looking at a table can

easily access any supplemental data. Prosecutors' late reporting was one of the most discussed topics in these focus groups, with one participant saying that it is extremely difficult to effectively and efficiently analyze the reports in light of supplemental data reported after initial publication of the annual Wiretap Report. Better linking of the supplemental data with the data it references would go some way toward combating the incompleteness of data that concerns nonjudiciary stakeholders.

Participant Misapprehensions

Initial questions and suggestions posed by the participants in the focus groups revealed that some of them were not fully aware of the specific duties, responsibilities, and capabilities of the AO to collect, analyze, and especially compel compliance with reporting requirements. Some of the participants' questions and suggestions reflected their inaccurate assumption that the AO has the legal authority to compel states (in particular) to submit wiretap data in a consistent and timely fashion. Participants seemed largely unaware that not only did the AO lack the ability to enforce reporting requirements, but also that no penalties existed for nonreporting.

It was further assumed by some stakeholders that the AO has some degree of authority to act independently of the statutory framework governing wiretap data collection. Some participants seemed to believe that AO regulations made it easier for prosecutors to submit late reports or fail to submit any report. Other questions centered on whether the AO should be more proactive about collecting data, including whether it could collect data that it currently does not collect—data that is not covered by the authorizing statute. Some participants further inaccurately assumed or were unsure as to whether the courts have the capacity to unilaterally authorize the collection of data pertaining to wiretaps, and participants were also unsure about the courts' ability to collect information not explicitly authorized by statute.

Due to these misapprehensions, some participants were initially confrontational with JDAO staff about what they perceived to be a lack of effort by JDAO to enforce reporting requirements. However, upon learning that the JDAO did not have much of the authority they had assumed, as well as hearing of some of the other challenges the data present, participants' tone changed. One participant expressed surprise, noting that he had not previously been aware that enforcement was an issue. Another participant, at the close of the focus group, expressed that they were "embarrassed" about some previous comments they had made about the incompleteness of the Wiretap Report because they had not realized the statutory limitations and challenges the JDAO faces.

One focus group participant encouraged the AO to reach out to Congress and ask for legislative changes that would either grant them enforcement powers or impose penalties—perhaps the inability to grant or obtain any wiretaps if a jurisdiction has failed to file their report for the previous year. This participant noted that even if Congress did not alter legislation, it would be helpful for them to see the extent of nonreporting. With or without new legislation, many participants wanted the AO to do more than send reminders.

However, precise suggestions for how the AO could be more aggressive in their follow-up procedures were not forthcoming.

In the absence of enforcement mechanisms or penalties, participants suggested that providing an explanation of the collection and enforcement limitations along with the Wiretap Report would inform users about the statutory framework and dispel misapprehensions about the AO's authority. This explanation could be in conjunction with the data explanation discussed above.

The Federal Judicial Center

About the Federal Judicial Center

The Federal Judicial Center is the research and education agency of the federal judicial system. It was established by Congress in 1967 (28 U.S.C. §§ 620–629), on the recommendation of the Judicial Conference of the United States.

By statute, the Chief Justice of the United States chairs the Center's Board, which also includes the director of the Administrative Office of the U.S. Courts and seven judges elected by the Judicial Conference.

The organization of the Center reflects its primary statutory mandates. The Education Division plans and produces education and training for judges and court staff, including in-person programs, video programs, publications, curriculum packages for in-district training, and web-based programs and resources. The Research Division examines and evaluates current and alternative federal court practices and policies. This research assists Judicial Conference committees, who request most Center research, in developing policy recommendations. The Center's research also contributes substantially to its educational programs. The Federal Judicial History Office helps courts and others study and preserve federal judicial history. The International Judicial Relations Office provides information to judicial and legal officials from foreign countries and informs federal judicial personnel of developments in international law and other court systems that may affect their work. Two units of the Director's Office—the Information Technology Office and the Editorial & Information Services Office—support Center missions through technology, editorial and design assistance, and organization and dissemination of Center resources.