

DID FBI FIRST REQUEST JAMES RISEN'S PHONE RECORDS USING THE CAU PROGRAM?

In Josh Gerstein's report on DOJ's collection of James Risen's phone and business records, he quotes University of Minnesota law professor Jane Kirtley saying that the government doesn't give reporters notice when it collects telephone or business records on them.

Kirtley also said journalists often aren't notified when the government asks telecom companies, banks or other service providers for their records.

DOJ must inform reporters if their call records have been subpoenaed

That may be the case in practice. But DOJ policy actually requires that journalists receive notice if their phone records are subpoenaed.

(g) In requesting the Attorney General's authorization for a subpoena for the telephone toll records of members of the news media, the following principles will apply: (1) There should be reasonable ground to believe that a crime has been committed and that the information sought is essential to the successful investigation of that crime. The subpoena should be as narrowly drawn as possible; it should be directed at relevant information regarding a limited subject matter and should cover a reasonably limited time period. In addition, prior to seeking the Attorney General's authorization, the government should have pursued all reasonable alternative investigation steps as required by paragraph (b) of this section.

(2) When there have been negotiations with a member of the news media whose telephone toll records are to be subpoenaed, the member shall be given reasonable and timely notice of the determination of the Attorney General to authorize the subpoena and that the government intends to issue it.

(3) When the telephone toll records of a member of the news media have been subpoenaed without the notice provided for in paragraph (e)(2) of this section, notification of the subpoena shall be given the member of the news media as soon thereafter as it is determined that such notification will no longer pose a clear and substantial threat to the integrity of the investigation. In any event, such notification shall occur within 45 days of any return made pursuant to the subpoena, except that the responsible Assistant Attorney General may authorize delay of notification for no more than an additional 45 days.

(4) Any information obtained as a result of a subpoena issued for telephone toll records shall be closely held so as to prevent disclosure of the information to unauthorized persons or for improper purposes.

From that we should assume that DOJ got the phone records by subpoenaing Sterling's records, not Risen's. But if that's the case, you'd think the government would have just told Risen that when his lawyer asked whether his records had been subpoenaed back in 2008.

Risen said the government never notified him that they were seeking his phone records. But he said he got an inkling in 2008 that investigators had collected some information about his calls.

"We heard from several people who had been forced to testify to the grand jury that prosecutors had shown them phone records between me and those people—not the content of calls but the records of calls," he said. "As a result of what they told us, my lawyers filed a motion with the court as asking how the Justice Department got these phone records and whether or not they had gotten my phone records."

"We wanted the court to help us decide whether they had abided by the attorney general's guidelines," Risen said. "We never got an answer from the court or the government."

In other words, there may be no cause for suspicion, except for the suspicious funkiness on the government's part.

DOJ has refused to inform at least one reporter his or her records were subpoenaed

Now, there **is** one case we know of where DOJ collected information on a reporter's phone records and did not inform him or her. The DOJ Inspector General Report on Exigent Letters describes three cases in which reporters' phone records were collected through the telecom's onsite Communications Analysis Unit. Two of these were collected using exigent letters; in both, the editors (for stories published in both the NYT and WaPo) and the journalist (for an Ellen Nakashima story) were informed the reporters' records had been collected.

In the third case, the records were collected with a grand jury subpoena. Here's what we know about the collection:

- The investigative team included two federal prosecutors who appear to belong to a

counterintelligence group at DOJ, an AUSA from the jurisdiction in which the grand jury was seated who was rubberstamping records for the investigation, the FBI case agent, and intelligence analysts.

- The FBI case agent asked the CAU agent about how to do a phone records subpoena for the leak investigation, and the CAU agent referred the case agent to the telecom analysts at CAU for help with the subpoena. Following a meeting with (I think) an AT&T analyst, the case agent asked that analyst for boilerplate language to make sure the subpoena was "as encompassing as possible." It appears from the report (though this information is highly redacted) that the resultant subpoena may have asked for the community of interest of the suspected leaker's numbers. That is, it appears the subpoena asked for a network analysis of all the people who had directly contacted the target.
- One of the two prosecutors used that boilerplate language to write up

attachments to the subpoena; the rubberstamp AUSA never saw the attachments. This was the first subpoena the rubberstamp AUSA signed in the case.

- The prosecutor that generated the subpoena claims—with an undated document to back up that claim—that the case agent told him the subpoena would not collect phone records for the reporter that—they both knew at the time—had been in phone contact with the suspected leaker. The case agent, however, did not recall such a discussion and claims it was “very unlikely” such a conversation occurred. The implication of this seems to be that the case agent knew full well he’d be getting the reporter’s call data.
- In talking to a counterintelligence Special Agent, the prosecutor who generated the subpoena learned that such a subpoena **could** produce the records of reporters; he also learned there was a way to write the subpoena to avoid that from happening. Once he realized that, he had conversations

with other DOJ lawyers and supervisors about what to do; they all agreed to seal the records. Though they sealed the records of the case agent and deleted them from his computer, they didn't ask what CAU had done with the records, much less ask the CAU analyst to delete the records.

- When the IG learned about all this, they finally checked whether this information got loaded into the investigative database. The target's records were entered into the FBI database; the IG did not find any reporters' information uploaded, though much of the report's discussion on this topic is redacted.
- DOJ's Criminal Division informed the Court overseeing the grand jury of the subpoenas and the "corrective actions" taken.

After learning all this, the IG asked DOJ whether it should have notified the reporter in question per the policy cited above. Here's what happened:

The Criminal Division and the OIG asked the Department's Office of Legal Counsel (OLC) to opine on the question when the notification provision in the regulation

would be triggered. OLC concluded in an informal written opinion dated January 15, 2009, that the notification requirement would be triggered if, using an "objective" standard and

based on the totality of the circumstances, a reasonable Department of Justice official responsible for reviewing and approving such subpoenas would understand the language of the subpoenas to call for the production of the reporters' telephone toll numbers, the subpoenas would be subject to the notification requirement of subsection (g)(3), regardless of the subjective intent of the individuals who prepared them.

The OLC opinion also concluded that the notification requirement would be triggered even if a reporter's toll records were not in fact collected in response to such a subpoena.

Based on the OLC opinion, the Criminal Division concluded that it was not required to notify the reporters because it believed that neither the [the prosecutor who generated the subpoena] nor the case agent understood at the time the subpoenas were issued that the subpoenas called for reporters' records.

Now, ultimately the IG accepts the prosecutor and case agent's descriptions that they had no idea the subpoena, as written, would collect reporters information. That, in spite of the fact that the case officer,

- Asked for a subpoena—in an investigation where a reporter was known to have

contact with the suspected leaker—"that is as encompassing as possible."

- Explained they had to use what appears to be a community of interest request to get local calls.
- May have told the prosecutor it would not include the known journalist contact of the target.
- Denied having told the prosecutor the subpoena wouldn't collect reporter information.

Also note, the IG appears not to have asked the telecom analyst about this at all. And the IG only discovered this issue because the prosecutor was involved in the exigent letters targeted at Ellen Nakashima.

In short, it all stinks.

It all looks like the FBI used their kid-in-a-candy-store-system to collect information they knew to include a reporter's calls, and found a way to deny they did it deliberately that helped them avoid telling the journalist(s) involved. As part of that, they got a last minute OLC opinion while Stephen Bradbury still ran the office (though frankly, I think the OLC opinion would suggest they should have informed the journalists).

The timing of the subpoena and the Sterling investigation

Now, there's nothing that affirmatively suggests there's any connection between this reporter subpoena and the Sterling case. But a number of the details suggest it is **possible**.

- The subpoena would have had

to have been issued between early 2002, when DOJ first contracted to have the telecom involved onsite, and January 2008, when the telecoms moved out of CAU. If it were indeed a community of interest subpoena, then it would have had to have been issued before early 2007, when the FBI discontinued the program. While we don't know whether the Sterling investigation began after Risen first tried to report the story in April 2003 or after he published his book in January 2006, both would fall in the time frame during which CAU was active.

- The investigative team was clearly focused on one target, which would be the case in the Sterling investigation but not—for example—in the warrantless wiretap investigation. In addition, the investigative team knew of at least one reporter who had had contact with the target; given both a 2000 article Risen had written about Sterling and the unsuccessful attempt to publish in 2003 would have alerted the CIA that Risen

was in contact with Sterling.

- The report doesn't describe much about the structure of the investigative team, though it seems to be consistent with a Main DOJ-led team assisted by the rubberstamp AUSA in the grand jury district. The description of the Special Agent who told the prosecutor about the (I think) community of interest subpoena—"an FBI Special Agent assigned to another counterintelligence squad in the division"—suggests he, too, was in a counterintelligence squad in a Main DOJ Division (probably National Security). This would rule out other reporter leak investigations, like the BALCO case (though that was probably already clear). The press release announcing Sterling's arrest says this about the investigative team:

This case is being prosecuted by Senior Litigation Counsel William M. Welch II of the Criminal Division, Trial Attorney Timothy J. Kelly of the Criminal Division's Public Integrity Section and Senior Litigation Counsel James L. Trump

of the Eastern District of Virginia. The case was investigated by the FBI's Washington Field Office, with assistance in the arrest from the FBI's St. Louis Field Office.

But we know that wasn't the original team, because Welch and Kelly were investigating PIN matters until that division was disgraced during the Ted Stevens trial.

In other words, while the Sterling investigation would fit, there's utterly no proof that Risen is the journalist in question.

But I am struck by one more detail. As I mentioned, this subpoena had to have been issued no later than January 2008, when the telecoms left CAU. Footnote 129, which refers to a "leak under investigation" seems to suggest the investigation was ongoing in January 2010 when this report was written. And there was an OLC opinion about whether or not to alert the journalist issued on January 15, 2009, in one of those last minutes of cleanup DOJ did before Obama assumed the Presidency.

Now, again, we have no proof, but if it were true, the timing would explain certain details about the investigation, not least why DOJ didn't indict Sterling after their early 2008 subpoena of Risen, but did after their April 2010 subpoena of Risen. After all, until DOJ got that OLC opinion, they would be at risk of having their telecom and (possibly) email evidence challenged. Particularly if Risen had asked, but gotten no answer, about how the government got his phone records. But then after 2009, after new prosecutors took over and any taint was resolved, then the government could go ahead and indict away!

The tie to Risen is, again, all a Wildarsed Guess. But think of the irony if it were true. After all it was Risen's partner Eric Lichtblau who first reported substantively about the

community of interest program.