

“IN THE FIRST HALF OF 2016” SIGNAL RECEIVED AN (OVERBROAD) SUBPOENA

This morning, the ACLU released a set of information associated with a subpoena served on Open Whisper Systems, the maker of Signal), for information associated with two phone numbers. As ACLU explained, OWS originally received the subpoena with a broad gag order. OWS was only able to turn over the account creation and last connection date for one of the phone numbers; the other account had no Signal account associated with it.

<u>Account</u>	<u>Information</u>
██████████	N/A
██████████	Last connection date: ██████████ Unix millis Account created: ██████████ Unix millis

But OWS also got ACLU to go challenge the gag associated with it, which led to the release of today’s information. All the specific data associated with the request is redacted (as reflected above), though ACLU was able to say the request was served on OWS in the first half of the year.

There are two interesting details of this. First, as OWS/ACLU noted in their response to the government, the government asked for far more information than they can obtain with a subpoena, including:

- subscriber name
- subscriber address
- subscriber telephone numbers
- subscriber email addresses
- subscriber method of payment
- subscriber IP registration

- IP history logs and addresses
- subscriber account history
- subscriber toll records
- upstream and downstream providers
- any associated accounts acquired through cookie data
- any other contact information from inception to the present

As OWS/ACLU noted,

OWS notes that not all of those types of information can be appropriately requested with a subpoena. Under ECPA, the government can use a subpoena to compel disclosure of information from an electronic communications service provider only if that information falls within the categories listed at 18 U.S.C. § 2703(c)(2). For other types of information, the government must obtain a court order or search warrant. OWS objects to use of the grand-jury subpoena to request information beyond what is authorized in Section 2703(c)(2).

I've got an email in with ACLU, but I believe ECPA would not permit the government to obtain the IP, cookie, and upstream/downstream information. Effectively, the government tried to do here what they have done with NSLs, obtain information beyond the subscriber and toll record information permitted by statute.

ACLU says this is "the only one ever received by OWS," presumably meaning it is the only subpoena the company has obtained, but it notes the government has other ways of gagging compliance, including with NSLs (it doesn't mention Section 215 orders, but that would be included as well).

I do wonder whether in the latter case – with a request for daily compliance under Section 215 – Signal might be able to turn over more information, given that they would know prospectively the government was seeking the information. That's particularly worth asking given that the District that issued this subpoena – Eastern District of Virginia – is the one that specializes in hacking and other spying cases (and is managing the prosecution of Edward Snowden, who happens to use Signal), which means they'd have the ability to use NSLs or individualized 215 orders for many of their cases.

Update: Here's a Chris Soghoian post from 2013 that deals with some, but not all, of the scope issues pertaining to text messaging.