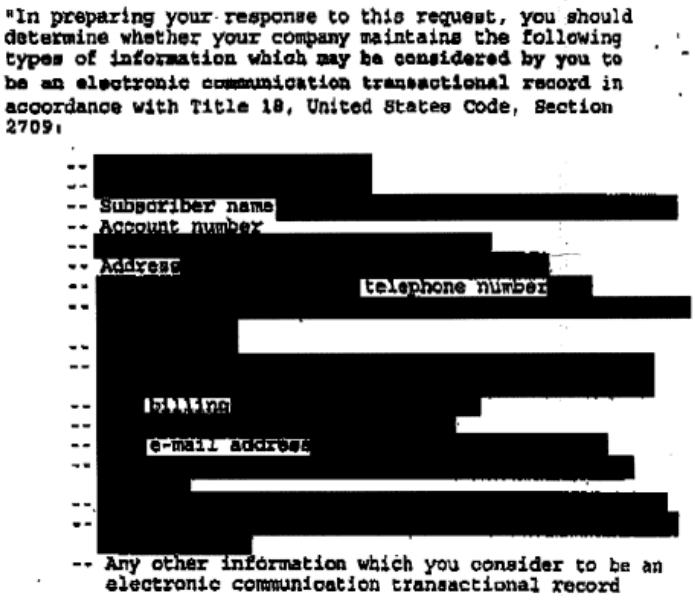
FBI DOESN'T WANT YOU TO KNOW IT USES NSLS TO "CORRELATE" ALL THE IDENTITIES YOU USE ONLINE

Back in March, I parsed the declaration Nicholas Merrill submitted in his bid to reveal the contents of what he was asked to turn over via an NSL back in 2004. As a reminder, here's what FBI permitted Merrill to reveal at the beginning of this suit.


"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

-- [redacted]
-- Subscriber name [redacted]
-- Account number [redacted]
-- Address [redacted]
-- [redacted] telephone number [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- e-mail address [redacted]
-- [redacted]
-- [redacted]
-- Any other information which you consider to be an electronic communication transactional record

And here's Merrill's description of what kind of records his ISP, Calyx, might have had on customers.

> Calyx Internet Access, like most ISPs, collected a wide array of information about its clients. For a given client, we may have collected their [1] name, [2] address and [3] telephone number; [4] other addresses associated with the account; [5] email addresses associated with the account; [6] IP addresses associated with the account; [7] Uniform Resource Locator (URL) addresses assigned to the account; [8] activity

> logs for the account; [9] logs tracking visitors to the client's website; [10] the content of a client's electronic communications; [11] data files residing on Calyx's server; [12] the client's customer list; [13] the client's bank account and [14] credit card numbers; [15] records relating to merchandise bought and sold; and the [16] date the account was opened or closed. [numbers 1 through 16 added]

FBI has submitted a counter-declaration (posted by Cryptome) that — even in its excessively redacted form — includes a number of interesting details.

FBI's limited new admission

The FBI now concedes that it had publicly confirmed some aspects of what it asked for from Merrill. It specifically admits that "screen names or other online names associated with the account" and "all email addresses associated with the account" may be disclosed, as well as that the request involved an "account number" from an "Internet service provider" (though in the sections that must describe these requests, those phrases remain redacted).

In addition, this paragraph appears without redaction:

> The NSA issued to [Merrill's ISP] Calyx requested "the names, addresses, lengths of service and electronic communication transaction records, to include existing transaction/activity logs and all e-mail header information (not to include message content and/or subject fields)" for the email account haroon@mojo.calyx.net.

FBI disses Merrill for

interacting with his ISP client

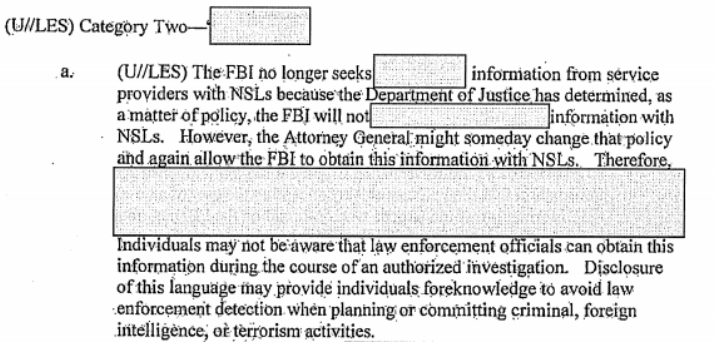
Part of — potentially a big part of — the declaration seems to insinuate that Merrill's lawsuit should be distrusted because he had a personal relationship with the target of the NSL. It describes,

> Merrill stated that he previously "engaged in ongoing communications with [redacted] on a variety of issues," including "topics related to politics and current events."

Interestingly, the declaration makes clear the NSL — which was almost certainly authorized as a terrorism investigation — was authorized in Pittsburgh. I raise that because Pittsburgh's FBI office was investigating a number of anti-war targets as terrorists in the 2004-timeframe. So I do wonder whether Merrill thought the investigation improper for that reason.

FBI mentions just one kind of Internet production as having moved to Section 215 orders

As I've noted, we know some production obtained until 2009 using NSLs has moved under Section 215. This paragraph seems to acknowledge that, even while saying the FBI may ignore what the Office of Legal Counsel has told it ECPA permits FBI to obtain using an NSL.



(U//LES) Category Two—[redacted]

a. (U//LES) The FBI no longer seeks [redacted] information from service providers with NSLs because the Department of Justice has determined, as a matter of policy, the FBI will not [redacted] information with NSLs. However, the Attorney General might someday change that policy and again allow the FBI to obtain this information with NSLs. Therefore, [redacted] Individuals may not be aware that law enforcement officials can obtain this information during the course of an authorized investigation. Disclosure of this language may provide individuals foreknowledge to avoid law enforcement detection when planning or committing criminal, foreign intelligence, or terrorism activities.

Curiously, this pertains *only* to the second bullet of the request (above), of 17 categories of information, suggesting just one kind of production moved to Section 215 orders.

FBI doesn't want you to know how much of your activities it can correlate by going to your ISP

The FBI has a separate paragraph addressing why it cannot reveal the other 15 categories of information it requested from Merrill 11 years ago. The paragraphs are worth reading, because they're each somewhat different. Some say not just counterterrorism and counterintelligence investigations might be affected with the release of the information, some claim greater use than others, some warn that potential criminals might avoid turning over certain kinds of information (perhaps an alternate email or phone number?) if they knew it could be obtained via an NSL.

All seem to pretend that a lot of this isn't already available from exhibits submitted in other cases.

As I noted in this post, for example, here's what the government obtains from Google subpoenaing a Google voice account and then the underlying Google account as a whole.

> [T]he two reports Google provided in response to administrative subpoenas for information on Shantia Hassanshahi, the guy caught using the DEA phone dragnet (these were subpoenas almost certainly used to parallel construct data obtained from the DEA phone dragnet and PRISM targeted at the Iranian, "Sheikhi," they found him through), included:
>
> - *a primary gmail account*
> - *two secondary gmail accounts*

> - *a second name tied to one of those gmail accounts*
> - *a backup email (Yahoo) address*
> - *a backup phone (unknown provider) account*
> - *Google phone number*
> - *Google SMS number*
> - *a primary login IP*
> - *4 other IP logins they were tracking*
> - *3 credit card accounts*
> - *Respectively 40, 5, and 11 Google services tied to the primary and two secondary Google accounts, much of which would be treated as separate, correlated identifiers*

There's surely a significant overlap between this list and the things FBI says Merrill can't reveal because if he did, it would tip off intelligence and criminal targets that the FBI can obtain them (though as Merrill made clear in his description of what Calyx had to turn over, they had more details about the websites run under an account).

Ultimately, though, the FBI seems to want to prevent anyone from realizing how much information your Internet providers have — and can be forced to turn over — that correlate all your multiple identities online.

FBI's false transparency

going forward

There's one more really funny part of this declaration. It notes that Office of Director of National Intelligence released a report in February claiming that "the FBI will now presumptively terminate National Security Letter nondisclosure orders at the earlier of three years after the opening of a fully predicated investigation or the investigations close."

But it says it won't have to comply with that policy for this NSL because "the investigation at issue here was closed prior to the implementation of the policy."

One would think that they would reveal all these categories of information going forward if they were really going to comply with ODNI's order.

Unless the FBI has already started to change the way they write NSLs (or perhaps plan on leaving more to verbal communications with Agents or some other means of communicating the list without including these descriptions) so as to get all the information without stating that they're demanding all that information.