

THE GOOGLE/YAHOO PROBLEM: FRUIT OF THE POISON MCT?

OK, this will be my last post (at least today) to attempt to understand why some Internet providers incurred so many costs associated with the response to the FISA Court's October 3, 2011 decision that the government had improperly collected US person data as part of Multiple Communication Transactions.

For the moment, I'm going to bracket the question of whether Google and Yahoo are included in upstream providers (though I think it more likely for Google than Yahoo). Footnote 3 in the October 3 opinion seems to distinguish upstream collection from collection from Internet service providers. Though note the entirely redacted sentence in that footnote that may modify that easy distinction.

But let's consider how the violative data might be used. We know from the conference call the I Cons had the other day (you can listen along here) that this is primarily about getting email inboxes.

An intelligence official who would not be identified publicly described the problem to reporters during a conference call on Wednesday.

"If you have a webmail email account, like Gmail or Hotmail, you know that if you open up your email program, you will get a screenshot of some number of emails that are sitting in your inbox, the official said.

"Those are all transmitted across the internet as one communication. For technological reasons, the NSA was not capable of breaking those down, and still is not capable, of breaking those down into their individual [email]

components.”

If one of those emails contained a reference to a foreign person believed to be outside the US – in the subject line, the sender or the recipient, for instance – then the NSA would collect the entire screenshot “that’s popping up on your screen at the time,” the official continued.

Now, whether or not this collection comes from the telecoms or the Internet companies themselves, it effectively serves as an index of Internet communications deemed interesting based on the participants or because the email talks about an approved selector.

But it may be that this upstream collection serves primarily to identify which content the government wants to collect.

In his November 30, 2011 opinion, Bates emphasized (see page 10) the limits on what analysts could do with properly segregated upstream MCTs in the future.

An analyst seeking to use (e.g., in a FISA application, in an intelligence report, or in a Section 702 targeting decision) a discrete communication within an Internet transaction that contains multiple discrete communications must document each of the determinations. [my emphasis]

Then, the September 25, 2012 opinion describes how, using threats that he would declare the previous collection a crime under 1809(a)(2), which prohibits the “disclosure” of any information collected illegally, Judge John Bates got the government purge that previous collection and any reports generated from it.

The government informed the Court in October 2011 that although the amended NSA procedures do not by their terms

apply to information acquired before October 31, NSA would apply portions of the procedures to the past upstream collection, including certain limitations on the use or disclosure of such information.

That effort, according to Bates, did not begin until “late in 2011.”

But here’s the thing: the government would have “disclosed” this information to email providers if it had used any of the violative MCTs to target emails in their custody – the Section 702 targeting decisions Bates was explicitly concerned about.

So presumably, once Bates made it clear he considered 1809 violations real problems in November 2011, the government would have had to modify any certifications authorizing collection on email addresses identified through the violative upstream collection (regardless of source).

I don’t yet understand why, in adjusting to a series of modified certifications, the providers would incur millions of dollars of costs. But I think expunging poison fruit targeting orders from the certifications would have taken some time and multiple changed certifications.

Update: Footnote 24 in the October 3, 2011 opinion provides more clarity on whether PRISM collection includes MCTs; it doesn’t.

In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [redacted] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its “PRISM collection.” Aug. 30 Submission at 11. The Court understands that NSA does not acquire Internet transactions” through its PRISM collection. See Aug Submission at 1.