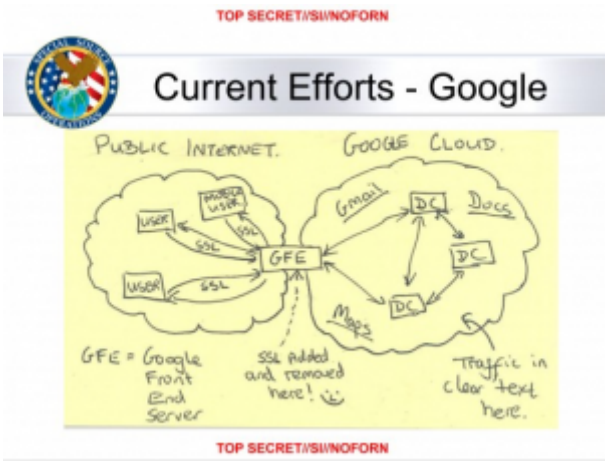
WHY SWIM UPSTREAM OVERSEAS?



In 2011, when John Bates declared the existing upstream collection illegal, he didn't stop the practice. Instead, he imposed new minimization procedures on part of the collection (just that part that included transactions including communications that were completely unrelated to the search terms used). He required that collection be segregated. And he wrung assurances from NSA they wouldn't do things — like search on data collected via upstream collection — that they could do with data collected under PRISM.

In short, it was actually a pretty permissive ruling, allowing the NSA to continue to collecting upstream data, at least for the terms and purposes they had claimed they were using it for.

So why go to the trouble of stealing data from Google and Yahoo links overseas instead of through PRISM — a question The Switch asks here — and upstream collection here?

Obviously, one of the problem is encryption. The graphic above makes it very clear NSA/GCHQ are trying to avoid Google's default and Yahoo's available SSL protection. Which mean they can't do the same kind of upstream collection on encrypted content.

Now it's clear from the aftermath of the 2011 ruling — in the way Google and Yahoo had to

invest a lot to keep responding to new orders — that PRISM collection in the US is tied in some way to that upstream collection. Julian Sanchez suggests Google and Yahoo may now be unwilling to do keyword (actually key-selector, since some of these would be code) searches. And that may be the case (though it's hard to see how they could refuse an order requiring that, given that the telecoms were responding to similar orders).

There are a few other possibilities, though.

First, remember that NSA wanted to continue its collection practice as it existed, with no changes. It considered appealing Bates' decision. And it resisted his demands they clean up existing illegally collected data.

So it may be they simply continued doing what they were doing by stealing this data overseas. But that would only make sense if MUSCULAR dates to 2012, when Bates imposed new restrictions.

It's also possible some of the restrictions he imposed wouldn't allow NSA to accomplish what it wanted to. Two possibilities are his requirement that NSA segregate this collection. Another is his refusal to let NSA search "incidentally" collected data.

A third possibility is that other FISC restrictions — such as limits on how many contact chains one could do on Internet metadata (WaPo makes it clear this collection includes metadata) — provided reason to evade FISC as well.

Finally, I wonder whether the types of targets they're pursuing have anything to do with this. For a variety of reasons, I've come to suspect NSA only uses Section 702 for three kinds of targets.

> - *Terrorists*
> - *Arms proliferators*
> - *Hackers and other cyber-attackers*

According to the plain letter of Section 702 there shouldn't be this limitation; Section 702 should be available for any foreign intelligence purpose. But it's possible that some of the FISC rulings — perhaps even the 2007-8 one pertaining to Yahoo (which the government is in the process of declassifying as we speak) — rely on a special needs exception to the Fourth Amendment tied to these three types of threats (with the assumption being that other foreign intelligence targets don't infiltrate the US like these do).

Which would make this passage one of the most revealing of the WaPo piece.

> One weekly report on MUSCULAR says the British operators of the site allow the NSA to contribute 100,000 "selectors," or search terms. That is more than twice the number in use in the PRISM program, but even 100,000 cannot easily account for the millions of records that are said to be sent back to Fort Meade each day.

Given that NSA is using twice as many selectors, it is likely the NSA is searching on content outside whatever parameters that FISC sets for it, perhaps on completely unrelated topics altogether. This may well be foreign intelligence, but it may not be content the FISC has deemed worthy of this kind of intrusive search.

That's just a wildarsedguess. But I do think it possible FISC has already told the NSA — whether it be in the 2011 opinion, opinions tied to the Internet dragnet problems (which themselves may have imposed limits on just this kind of behavior), or on the original PAA/FAA opinions themselves — that this collection violated the Fourth Amendment.

In which case the prediction Russ Feingold made back in 2007 — "So in other words, if they don't like what we [or the FISA Court] come up with, they can just go back to Article II" — would

prove, as so many Feingold comments have, prescient.