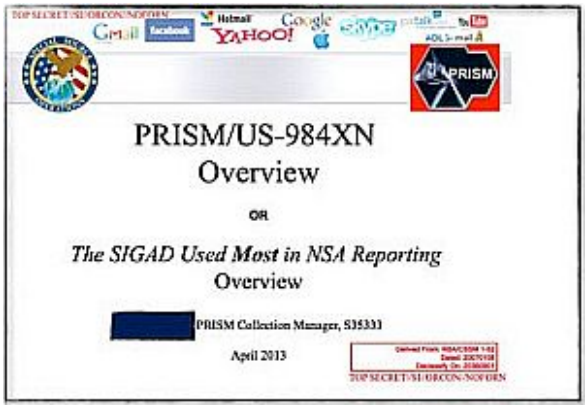
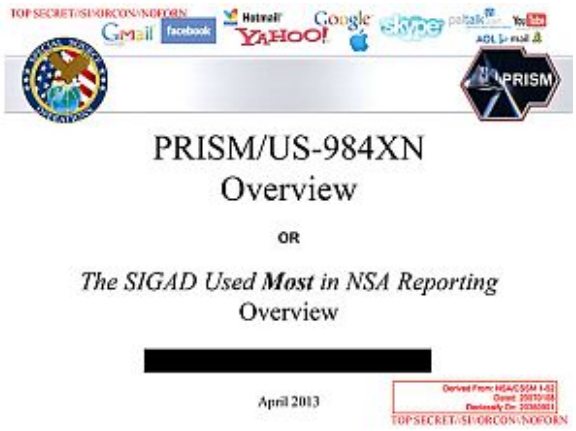
NSA PRISM SLIDES: NOTICE ANYTHING UNUSUAL OR MISSING?

We haven't seen (and likely will never see) all of the NSA slides former Booz Allen employee Edward Snowden shared with the Guardian-UK and the Washington Post. But the few that we have seen shared by these two news outlets tell us a lot – even content we might expect to see but don't tells us something.

First, let's compare what appears to be the title slide of the presentation – the Guardian's version first, followed by the WaPo's version. You'd think on the face of it they'd be the same, but they aren't.



[NSA presentation, title slide, via Guardian-UK]



[NSA presentation, title slide, via Washington Post]

Note the name of the preparer or presenter has been redacted on both versions; however, the Guardian retains the title of this person, "PRISM Collection Manager, S35333," while the WaPo completely redacts both name and title.

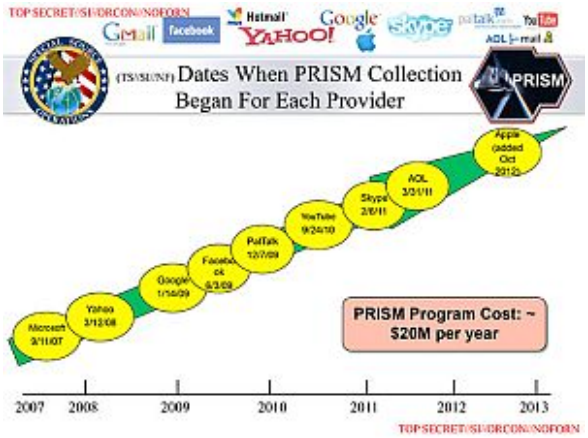
This suggests there's an entire department for this program requiring at least one manager. There are a number of folks who are plugging away at this without uttering a peep.

More importantly, they are working on *collection* – not exclusively on search.

The boldface reference to "The SIGAD Used Most in NSA Reporting" suggests there are more than the PRISM in use as SIGINT Activity Designator tools. What's not clear from this slide is whether PRISM is a subset of US-984XN or whether PRISM is one-for-one the same as US-984XN.

Regardless of whether PRISM is inside or all of US-984XN, the presentation addresses the program "used most" for reporting; can we conclude that reporting means the culled output of mass *collection*?

Here's the next slide referred to most frequently, from the WaPo's site. No redactions were made by either Guardian or WaPo to this slide:

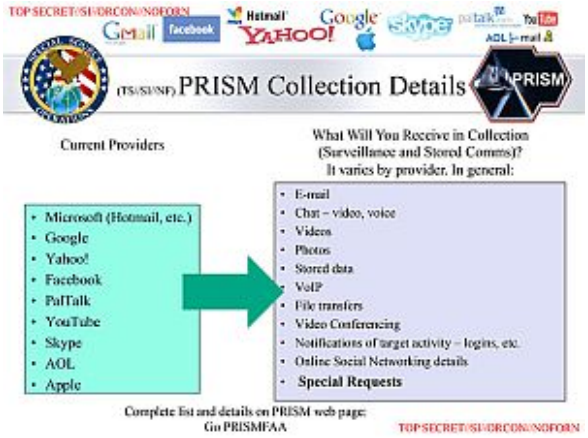


[NSA presentation, PRISM collection dates, via Washington Post]

Note the use of the word *collection* here in the title.

Note also that the entire slide does NOT mention metadata (nor do any of the other slides released by Guardian-UK and WaPo).

Let's look next at the slide entitled "PRISM Collection Details" from the WaPo's site. Again, no redactions were made by either Guardian or WaPo.



[NSA presentation, PRISM collection details, via Washington Post]

Note again the use of the word *collection*, and the lack of the word metadata in the description of materials obtained by collection process. (Note, too, just how much content is available without making a special request.)

Granted, the same slide makes reference to a NSA internal site PRISMFAA, suggesting the FISA Amendments Act may have been utilized to collect content, but this, too, is another interesting feature. Why is PRISM so tightly integrated with FAA?

Does the possibility they are not completely separate explain why Director of National Intelligence James Clapper, Senate Intelligence Committee Chair Dianne Feinstein, and House Intelligence Committee Chair Mike Rogers appear to confuse PRISM with Section 215 of the the Patriot Act?

The slide entitled FAA702 Operations contains some points which have not been examined very closely by the media, apart from the Guardian. This slide was included by itself in a followup report dated 08-JUN-2013:

[NSA presentation, FAA702 operations, via Guardian-UK]

Note that FAA is once again tied to a section of the Patriot Act, this time to Section 702. (See Marcy's previous post about 702's intended use with regard to hacking in addition to counterterrorism and counter-proliferation.)

This slide suggests to its audience that two major forms of collection should be used, one of which is PRISM. The other appears to be network sniffing capabilities farther away from the subject entities of PRISM, installed somewhere on the communications system wide area network.

Given this duality of methods, it might be implied that PRISM consists solely of collection of content on these nine social media firms, and not telcos.

Further, the Guardian reported in its initial article on PRISM:

> "…Companies are legally obliged to comply with requests for users' communications under US law, but the Prism program allows the intelligence

> services direct access to the companies' servers. The NSA document notes the operations have "assistance of communications providers in the US". …" [emphasis added]

It's not clear from the FAA702 slide which US communications providers are assisting, or whether they do so voluntarily. We can only guess that the court order granted by Foreign Intelligence Surveillance Court to the FBI in late April allowing collection of Verizon users' data demonstrates the kind of assistance provided by telcos in the absence of other publicly available information.

The slide also indicates four programs are used on the upstream network, the names of two having been redacted. The WaPo only describes one of them – BLARNEY – as tool which "gathers up 'metadata'" and is "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks."

What does this suggest about the other three programs, two of which have not been revealed in any fashion?

Finally, the background image used in the slide raises more questions; underseas cable routes are shown, as are major network trunks across the US. Are there collection systems installed on these underseas cables routing a substantive portion of all communications into/out of the US?

This calls to mind another older program, ECHELON, about which the public already knows. It isn't mentioned in this slide, and the chances it is a redacted name are slim. Has it been replaced by a new program?

Given the analysis methodology described by WaPo:

> "Analysts who use the system from a Web

> portal at Fort Meade, Md., key in "selectors," or search terms, that are designed to produce at least 51 percent confidence in a target's "foreignness." That is not a very stringent test. Training materials obtained by The Post instruct new analysts to make quarterly reports of any accidental collection of U.S. content, but add that "it's nothing to worry about."
> […]
> Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially. The same math explains the aphorism, from the John Guare play, that no one is more than "six degrees of separation" from any other person.

Does this mean that all communications between individuals who do not have an Anglo-Saxon name are likely to be sniffed if not collected?

Does this sketchy "(foreign) + (less than 3 hops)" approach executed by humans explain known false-positives? Could the relationships between the false-positives be as tenuous as shopping at the same store? What happens in the case of targets possessing a highly common name like "Ahmed" – the equivalent of Smith in terms of frequency among Arabic surnames – is collection so large it could be called a dragnet?

And what happens with searches or collections related to cyber attacks, in which names mean nothing?

Once again, many questions remain with the prospect of few straightforward, truthful answers ahead.

UPDATE – 1:26 PM EDT – I missed this rather obvious detail while combing through the content of the slides. The PRISM logo on the Guardian-UK's title slide is different from the title slide the Washington Post published. Did these

two outlets receive different sets of slides? Or did they publish different title pages from the same collection of NSA slides furnished by Edward Snowden? Why the logo change at all?

UPDATE – 3:45 PM EDT – Per readers in comments below, the differences in the PRISM logo are believed to be differences in rendering dependent upon the news outlets' use of either open source OpenOffice's Impress or proprietary Microsoft Powerpoint applications. If there are other likely explanations, please feel free to share in comments.