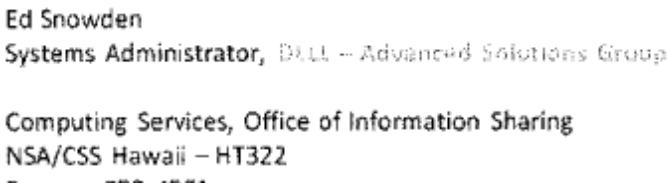
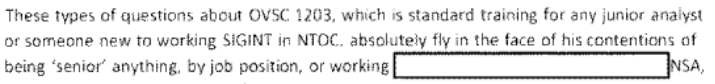
HOW DID BOOZ EMPLOYEE ANALYST-TRAINEE EDWARD SNOWDEN GET THE VERIZON 215 ORDER?

One thing I've been pondering as I've been going through the Snowden emails liberated by Jason Leopold is the transition Snowden made just before he left. They show that in August 2012, Snowden was (as we've heard) a Dell contractor serving as a SysAdmin in Hawaii.


Ed Snowden
Systems Administrator, DELL – Advanced Solutions Group

Computing Services, Office of Information Sharing
NSA/CSS Hawaii – HT322

The training he was taking (and complaining about) in around April 5 – 12, 2013 was in preparation to move into an analyst role with the National Threat Operations Center.


These types of questions about OVSC 1203, which is standard training for any junior analyst or someone new to working SIGINT in NTOC, absolutely fly in the face of his contentions of being 'senior' anything, by job position, or working [redacted] NSA,

That would mean Snowden would have been analyzing US vulnerabilities to cyberattack in what is a hybrid "best defense is a good offense" mode; given that he was in HI, these attacks would probably have been launched predominantly from, and countermeasures would be focused on, China. (Before Stewart Baker accuses me of showing no curiosity about this move, as Baker did about the Chinese invitation to Snowden's girlfriend to a pole dancing competition, I did, but got remarkably little response from anyone on it.)

It's not clear why Snowden made the switch, but we have certainly seen a number of cybersecurity related documents – see the packet published by Charlie Savage in conjunction with his upstream

cyber article. Even the PRISM PowerPoint — the second thing released — actually has a cybersecurity focus (though I think there's one detail that remains redacted). It's about using upstream to track known cyberthreat actors.

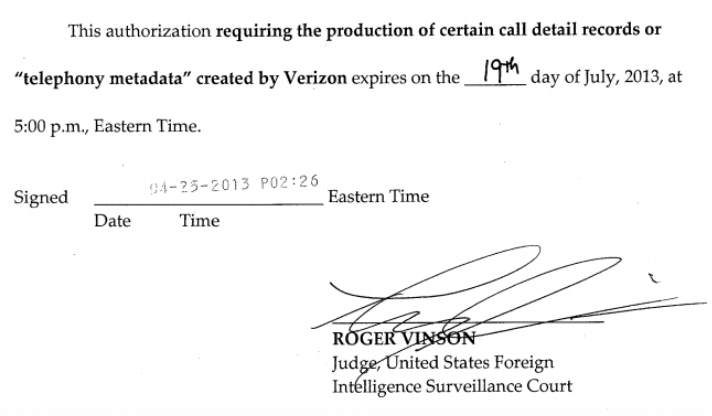
I suspect, given the inaccuracies and boosterism in this slide deck, that it was something Snowden picked up while at *Booz* training, when he was back in Maryland in April 2013. Which raises certain questions about what might have been available at Booz that wasn't available at NSA itself, especially given the fact that all the PRISM providers' names appear in uncoded fashion.

Incidentally, Snowden's job changes at NSA also reveal that there are Booz analysts, not NSA direct employees, doing Section 702 analysis (though that is technically public). In case that makes you feel any better about the way the NSA runs it warrantless surveillance programs.

Anyway, thus far, all that makes sense: Snowden got into a cybersecurity role, and one of the latest documents he took was a document that included a cybersecurity function (though presumably he could have gotten most of the ones that had already been completed as a SysAdmin before that).

But one of the most sensitive documents he got — the Verizon Section 215 primary order — has nothing to do with cybersecurity. The Section 215 dragnet was supposed to be used exclusively

for counterterrorism. (And as I understand it, there are almost no documents, of any type, listing provider names in the Snowden stash, and not all that many listing encoded provider names). But the Verizon dragnet order it is dated April 23, 2013, several weeks into the time Snowden had moved into a cybersecurity analytical role.



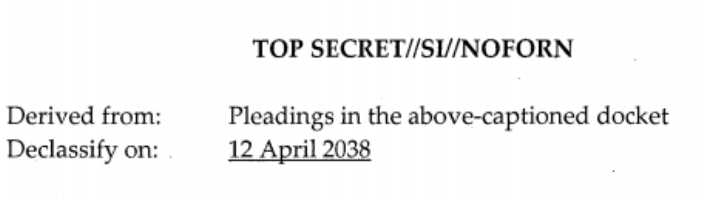
This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

There's probably an easy explanation: That even though NSA is supposed to shift people's credentials as they move from job to job, it hadn't happened for Snowden yet. *If that's right*, it would say whoever was responsible for downgrading Snowden's access from SysAdmin to analyst was slow to make the change, resulting in one of the most significant disclosures Snowden made (there have been at least some cases of credentials not being adjusted since Snowden's leaks, too, so they haven't entirely addressed what would have to be regarded as a major fuck-up if that's how this happened).

Interestingly, however, the declassification stamp on the document suggests it was classified on April 12, not April 23, which may mean they had wrapped up the authorization process, only to backdate it on the date it needed to be reauthorized. April 12, 2013 was, I believe, the last day Snowden was at Fort Meade.



TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

Whatever the underlying explanation, it should be noted that the most sensitive document Snowden leaked — the one that revealed that the government aspired to collect phone records from every single Verizon customer (and, significantly, the one that made court challenges possible) — had to have been obtained after Snowden formally left his SysAdmin, privileged user, position.