IF NSA COMMITS DATABASE QUERY VIOLATIONS, BUT NOBODY AUDITS THEM, DO THEY REALLY HAPPEN?

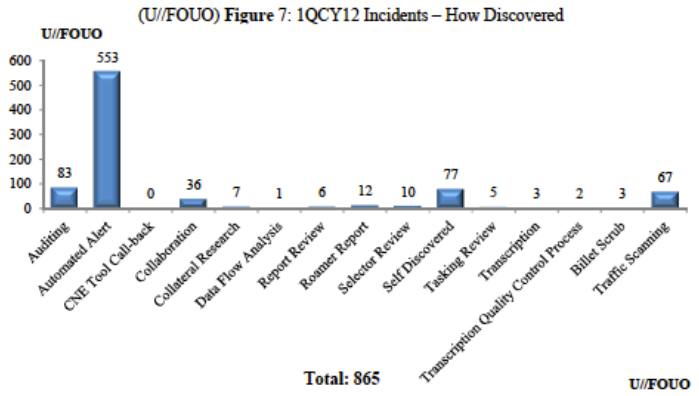
Barton Gellman, at the beginning of the worthwhile video above, addresses something I addressed here: the only way the government can claim they haven't "abused" the rules governing NSA activities is by treating all abuse done in the name of the mission as a mistake.

> The President, like a lot of people who work for him, has a very narrow definition of two key words in that passage. One is "abuse" and the other is "inappropriately." As the government depicts it — and this is language it's using that it does not, frankly, explain.
>
> Abuse — the only kind of abuse that exists would be if, say, an NSA employee were to stalk his ex-wife or spy on movie stars or something of that nature. If they are performing the mission that the NSA wants them to perform, and nevertheless overstep their legal authority, make unauthorized interceptions or searches or retentions or sharing of secret information, that is not abuse, that's a mistake.

That's how they get to pretend the 9% to 20% of violations in which a person does not follow the rules seemingly intentionally (these are distinct from human error and training violations) does not constitute an abuse.

With that in mind, I wanted to look more closely

at what the audit report says about how errors are found, as shown primarily in this figure:



That looks pretty good on the face, with 64% of all violations found via automated alert, plus a few more — data flow analysis and traffic scanning — that involve technological review.

But this detail on the roamer problem (in which valid foreign targets continue to be targeted when they travel to the US) explains what that's not all that impressive.

> The biggest class of technological mistakes comes from that. They actually for some reason only get quarterly reports of where a GSM mobile phone is in the world. And so you're monitoring a foreigner using a telephone in China, the person flies to San Francisco, and you're still monitoring. That's against the law under FISA without a specific warrant . But they only find out every three months, and they find out sooner once someone says here I am down at the waterfront in San Francisco and they say oops.

Between FISA authority and 12333 authority surveillance, there were 586 roamer violations found in the quarter in question. If roamer violations are found — as Gellman suggests — with the quarterly report (that is, an automated alert) it would mean many of the automated alerts involve roamers. Indeed, the sheer numerical scope of the automated alerts says

they are primarily roamer violations. (Adding together the two roamer-specific categories here with the automated alert accounts for 571 variations, though some of the automated alerts may be for other violations.)

Compare that to a potentially far more sensitive violation, the database query violation. That section of the report says that 70 of the 115 database query violations were found via audit. So 61% of database violations were found only through the review of another person; 84% of the violations found by auditors were database query violations.

As Gellman notes in this piece, they could automate more of the checks on database queries, but they don't.

What this means is that (like IRS violations) short of automating this review, the government is only going to find as many database violations as they provide manpower to check.

Which may explain this detail, from Gellman's original report on NSA's violations.

> Despite the quadrupling of the NSA's oversight staff after a series of significant violations in 2009, the rate of infractions increased throughout 2011 and early 2012. An NSA spokesman declined to disclose whether the trend has continued since last year.

It turns out when the NSA assigned more staff to review this (though part of this staff increase must just be the staffing of the Director of Compliance position, which was instituted in 2009), they found more violations. And probably, given the role of audits in finding database query errors, more database query errors.

Which raises the question of whether the government has an adequate number of auditors now to find the database query violations (and other more intrusive violations) that occur?

While it's a different — but related — issue,

it’s worth recalling the response to Ron Wyden’s request for a hard number of the US persons whose communications are searched after having been incidentally collected. The NSA Inspector General claimed (and the Intelligence Committee Inspector General endorsed that claim) that resource limitations prevented the NSA IG from identifying how many Americans’ records get searched through this back door.

> I defer to his conclusion that obtaining such an estimate was beyond the capacity of his office and dedicating sufficient additional resources would likely impede the NSA’s mission.

This response came just months after the IC IG said he had all the resources he needed to conduct his work. Since that time, we’ve learned he has been focusing on investigating leaks, not investigating whether the NSA commits database query violations.

Now, none of what the IC IG is doing says much about how the NSA IG spends his time.

But the apparent importance of audits to finding database query violations does raise the question: how many auditors does NSA have? What are their priorities? Do they have the appropriate number of auditors?

We don’t know one way or another — it’s one of those transparency™ things. But it’s a question that must be answered before anyone can assess the claims about the level of ~~abuses~~ ~~violations~~ mistakes.