WILL NSA LOSE ACCESS TO ALL VERIZON CELL METADATA IN 12 DAYS TIME?

Last week, NSA selectively leaked a claim it only obtains 20 to 30% of US call data because it doesn't collect some or all cell provider data. (WSJ, WaPo, LAT, NYT)

I believe the claim itself is true only in a narrow sense and the premises given to journalists underlying it are laughably false as presented (though have grains of truth).

I suspect this leaked propaganda campaign might better be explained by the possibility that NSA will lose some of its existing access to Verizon cell data on February 21, when the Vodaphone/Verizon split becomes legally official.

Some aspect of Verizon's structure — and a good deal suggests it's that dual-country ownership — has created problems in the metadata program since 2009. On May 29, 2009, Judge Reggie Walton started breaking out directions to Verizon's Custodian of Records in its own paragraph of the Primary Order so as to clarify that it should only provide entirely domestic or one-end domestic calls under the Section 215 order, not entirely foreign calls. Then, in a July 9, 2009 Primary Order the government is still withholding, Walton actually shut down production from Verizon, apparently entirely. He restored production with the September 3, 2009 Primary Order, permitting retroactive collection of any records still in existence. We know Verizon was this provider because ODNI failed to redact Verizon's name in the Verizon-specific paragraph in a recent document dump.

While we don't know why including foreign production presented such a problem (that 3 month period is the only period I know of during

which production of any part of the phone dragnet was shut down), it did.

But we do have hints of why Verizon's international collection might be so sensitive. In August (a month before Verizon and Vodaphone agreed to split), Suddeutsche newspaper revealed that Verizon was among the 7 providers included in GCHQ's Tempora program.

> BT, Vodafone Cable, and the American firm Verizon Business – together with four other smaller providers – have given GCHQ secret unlimited access to their network of undersea cables. The cables carry much of the world's phone calls and internet traffic.
>
> In June the Guardian revealed details of GCHQ's ambitious data-hoovering programmes, Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. It emerged GCHQ was able to tap into fibre-optic cables and store huge volumes of data for up to 30 days. That operation, codenamed Tempora, has been running for 20 months.

The Guardian explained that providers were compelled, under licensing requirements, to participate under the UK's Telecom Act.

> Telecoms providers can be compelled to co-operate with requests from the government, relayed through ministers, under the 1984 Telecommunications Act,
>
> [snip]
>
> Vodafone said it complied with the laws of all the countries in which its cables operate. "Media reports on these matters have demonstrated a misunderstanding of the basic facts of European, German and UK legislation and of the legal obligations set out within every telecommunications operator's licence …

> Vodafone complies with the law in all of our countries of operation," said a spokesman.

That would seem to suggest Verizon's legal presence in the UK made it subject to orders to participate in Tempora. This requirement, which started as early as 2008, involves the massive collection of both phone and Internet metadata which gets stored for 30 days. The kind of metadata that last week's propaganda campaign claimed NSA didn't get access to.

Given Verizon's role in Tempora, I suspect it is one of the corporate partners which accesses data (including, but no way limited to, cell location data) from the telephone links between networks under the FASCIA program.

> A sigad known as STORMBREW, for example, relies on two unnamed corporate partners described only as ARTIFICE and WOLFPOINT. According to an NSA site inventory, the companies administer the NSA's "physical systems," or interception equipment, and "NSA asks nicely for tasking/updates."
>
> STORMBREW collects data from 27 telephone links known as OPC/DPC pairs, which refer to originating and destination points and which typically transfer traffic from one provider's internal network to another's. That data include cell tower identifiers, which can be used to locate a phone's location.
>
> The agency's access to carriers' networks appears to be vast.
>
> "Many shared databases, such as those used for roaming, are available in their complete form to any carrier who requires access to any part of it," said Matt Blaze, an associate professor of computer and information science at the University of Pennsylvania. "This 'flat'

> trust model means that a surprisingly large number of entities have access to data about customers that they never actually do business with, and an intelligence agency – hostile or friendly – can get 'one-stop shopping' to an expansive range of subscriber data just by compromising a few carriers."

And as Blaze describes (Mindrayge describes some of why this is so in this comment), accessing data at these points would give Verizon access to everyone's cell data, not just its own.

I believe that collection – because it was obligated by the UK, not the US, and because it took place offshore – would count as EO 12333 data, not Section 215 data. This is why I believe NSA **does** get comprehensive coverage of all cell data, just not under Section 215. NSA gets all the data it wants, just via GCHQ's greater ability to obligate production than NSA's. And it gets cell location data if it wants it too!

Or it did, so long as the joint corporate structure of Vodaphone and Verizon created the obligation behind that production.

Now, obviously, the hardware linking Verizon and Vodaphone won't disappear in 12 days time. Verizon will still presumably operate the hardware where this massive data collection takes place. But if I'm understanding the legal leverage of the UK's licensing law correctly, the UK and US' collective ability to obligate production will change. As one possibility (there are others I'll explain in a later post), NSA may have to rely on Section 215 to obligate production, rather than the UK's more expansive law.

Which, I suspect, is the real logic behind last week's propaganda campaign on cell data. For the first time, NSA may have to rely on Section 215 rather than UK licensing laws to access Verizon's (and probably some other providers')

cell phone metadata. And that's happening at a time when Verizon is the dominant cell provider in the US. But even as it will need to rely on Section 215, the FISC has narrowed the scope of its interpretation of the law, to specifically exclude the cell location data that has been included in this collection for years.

In other words, I believe the confluence of two events — the change in Verizon's corporate structure and FISC's effort to prohibit the application of Section 215 to location data — may have created significant new difficulties in maintaining what (I strongly believe) has always been comprehensive dragnet collection.

Update: On March 4, Verizon's General Counsel said the Vodaphone/Verizon split will have no effect on their legal obligation.