THE HEMISPHERE DECKS: A COMPARISON AND SOME HYPOTHESES

Last week, Dustin Slaughter published a story using a new deck of slides on the Hemisphere program, the Drug Czar program that permits agencies to access additional telecommunications analytical services to identify phones, which then gets laundered through parallel construction to hide both how those phones were found, as well as the existence of the program itself.

It has some significant differences from the deck released by the New York Times last year. I've tried to capture the key differences here:

	NYT	Declaration
Scope	AT&T network; CDRs for any telephone carrier that uses an AT&T switch Access to AT&T subscriber info Roaming provided, location available	"Telecom propriety" (2) though "only calls that hit the Hemisphere switches" (12) Some subscriber information unavailable (elsewhere references to "official subscriber information") Local, long distance, international, cell Temporary roaming and location provided with CDRs
Timing	1 hour response/CDRs 1 hour old	1-hour exigent; 2-5 day typical response/CDRs few hours old/CDRs 2 hours old
Customers	Fed, state, local administrative and grand jury subpoenas (mentions recent WA approval) DEA and DHS mentioned	Administrative order, CA court order , or grand jury 6 federal agencies, including FBI and US Marshals
Features	Dropped phones, additional phones, international phones, IMEI & ISEI search on AT&T network, mapping, pinging	Dropped, additional phones, international phones, temporary roaming, location
Dropped phone success rate	Candidates for the replacement phone are ranked by probability	94%
Aging	26 year old long distance and international records available in 2013 Program started in 2007	10 year old records, date unknown

The biggest difference is that the NYT deck – which must date to no earlier than June 2013 – draws only from AT&T data, whereas the Declaration deck draws from other providers as well (or rather, from switches used by other providers).

In addition, the Declaration deck seems to reflect approval for use in fewer states (given the mention of CA court orders and the recent authorization to use Hemisphere in Washington in the AT&T deck), and seems to offer fewer analytical bells and whistles.

Thus, I agree with Slaughter that his deck

predates — perhaps by some time — the NYT/AT&T deck released last year. That would mean Hemisphere has lost coverage, even while it has gained new bells and whistles offered by AT&T.

While I'm not yet sure this is my theory of the origin of Hemisphere, some dates are worth noting:

From 2002 to 2006, the FBI had telecoms onsite to provide CDRs directly from their systems (the FBI submitted a great number of its requests without any paperwork). One of the services provided — by AT&T — was community of interest tracking. Presumably they were able to track burner phones (described as dropped phones in these decks) as well.

In 2006, FBI shut down the onsite access, but retained contracts with all 3 providers (AT&T, Verizon, and probably Sprint). In 2009, one telecom — probably Verizon — declined to renew its contract for whatever the contract required.

AT&T definitely still has a contract with FBI, and in recent years, it has added more services to what it offers the FBI.

It's possible the FBI multi-provider access moved under ONCDP (the Drug Czar) in 2007 as a way to retain its authorities without attracting the attention of DOJ's excellent Inspector General (who is now investigating this in any case). Though I'm not sure that program provided the local call records the deck at least claims it could have offered. I'm not sure that program got to the telecom switches the way the deck seems to reflect. It's possible, however, that the phone dragnet in place before it was moved to Section 215 in 2006 did have that direct access to switches, and the program retained this data for some years.

The phone dragnet prior to 2006 and NSL compliance (which is what the contracts with AT&T and one other carrier purportedly provide now) are both authorized in significant part (and entirely, before 2006) through voluntary compliance, per David Kris, the NSA IG Report,

and the most recent NSL report. That's a big reason why the government tried to keep this secret — to avoid any blowback on the providers.

In any case, if I'm right that the program has lost coverage (though gained AT&T's bells and whistles) in the interim, then it's probably because providers became unwilling, for a variety of reasons (and various legal decisions on location data are surely one of them) to voluntarily provide such information anymore. I suspect that voluntary compliance got even more circumscribed with the release of the first Horizon deck last year.

Which means the government is surely scrambling to find additional authorities to coerce this continued service.