# IMPORTANT: CHANGES TO SECTION 215 DRAGNET WILL NOT CHANGE TREATMENT OF EO 12333 METADATA

In their Angry Birds stories, both the Guardian and NYT make what I believe is a significant error. They suggest changes in the handling of the Section 215-collected phone metadata will change the way NSA handles EO 12333-collected phone metadata.

Guardian:

> Data collected from smartphone apps is subject to the same laws and minimisation procedures as all other NSA activity – procedures which US president Barack Obama suggested may be subject to reform in a speech 10 days ago. But the president focused largely on the NSA's collection of the metadata from US phone calls and made no mention in his address of the large amounts of data the agency collects from smartphone apps.

NYT:

> President Obama announced new restrictions this month to better protect the privacy of ordinary Americans and foreigners from government surveillance, including limits on how the N.S.A. can view "metadata" of Americans' phone calls — the routing information, time stamps and other data associated with calls. But he did not address the avalanche of information that the intelligence agencies get from leaky apps and other smartphone functions.

Here's what the President actually said, in part, about phone metadata:

> I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk meta-data.

That is, Obama was speaking only about NSA's treatment of Section 215 metadata, not the data — which includes a great amount of US person data — collected under Executive Order 12333.

To be clear, both Guardian and NYT were distinguishing Obama's promises from the treatment extended to the leaky mobile data app. But they incorrectly suggested that all phone metadata, regardless of how it was collected, receives the same protections.

Section 215 metadata has different and significantly higher protections than EO 12333 phone metadata because of specific minimization procedures imposed by the FISC (arguably, the program doesn't even meet the minimization procedure requirements mandated by the law). We've seen the implications of that, for example, when the NSA responded to being caught watch-listing 3,000 US persons without extending First Amendment protection not by stopping that tracking, but simply cutting off the watch-list's ability to draw on Section 215 data.

Basically, the way NSA treats data collected under FISC-overseen programs (including both Section 215 and FISA Amendments Act) is to throw the data in with data collected under EO 12333, but add query screens tied to the more strict FISC-regulations governing production under it. This post on federated queries explains how it works in practice. As recently as 2012 at least one analyst improperly searched on US person FAA-collected content because she didn't hit the right filter on her query screen.

> [T]he NSA analyst conducted a federated query using a known United States person identifier, but forgot to filter out Section 702-acquired data while conducting the federated query.

That's it. If the data is accessed via one of the FISC-overseen programs, US persons benefit from the additional subject matter, dissemination, and First Amendment protections of those laws or FISC's implementation of them (and would benefit from the minor changes Obama has promised to both Section 215 and FAA).

But if NSA collected the data via one of its EO 12333 programs, it does not get get those protections. To be clear, it does get some dissemination protection and can only be accessed with a foreign intelligence purpose, but that is much less than what the FISC programs get. Which leaves the NSA a fair amount of leeway to spy on US persons, so long as it hasn't collected the data to do so under the programs overseen by FISC. And when it collects data under EO 12333, it is a lot easier for the NSA to spy on Americans.

The metadata from leaky mobile apps almost certainly comes from EO 12333 collection, not least given the role of GCHQ and CSEC (Canada's Five Eyes' partner) to the collection. The Facebook and YouTube data GCHQ collects (just reported by Glenn Greenwald working with NBC) surely counts as EO 12333 collection.

NSA's spokeswoman will say over and over that "everyday" or "ordinary" Americans don't have to worry about their favorite software being sucked up by NSA. But to the extent that collection happens under EO 12333, they have relatively little protection.