

CONFIRMED: OBAMA'S DRAGNET "FIX" ISN'T ABOUT US

After Obama rolled out his phone dragnet fix, I noted the real reason he was doing it was not so much a concern for civil liberties, but rather a recognition that by outsourcing the data to providers, it would solve the legal-technical problems NSA had been having in two (probably related) areas: collection of cell data and operation of an alert function.

The Obama plan is an improvement over the status quo (though I do have grave concerns about its applicability in non-terrorist contexts, and my concerns about what the government does with the data of **tens to hundreds of thousands of innocent Americans remain**).

But don't be fooled. Obama's doing this as much because it's the easiest way to solve legal and technical problems that have long existed because the government chose to apply a law that was entirely inapt to the function they wanted to use it for.

Shockers! A more privacy protective solution also happens to provide the best technical and legal solution to the problem at hand.

Yesterday, David Sanger confirmed that was the case, at least for the cell data problem.

At the N.S.A., there is grumbling about the continuing disclosures of material stolen by Mr. Snowden, but comparatively little complaint on the new limits Mr. Obama has proposed. In some cases, the N.S.A. gained some access to data even as it lost some autonomy. For example, its program to collect metadata missed a

large percentage of cellphone calls. Under Mr. Obama's plan, if it becomes law, the N.S.A. would have to leave that data in private hands, but when the N.S.A. does get it, under court order, the agency should have access to a lot more than it does today.

"It's a pretty good trade," said one senior intelligence official who has been working on the issue. "All told, if you are an N.S.A. analyst, you will probably get more of what you wanted to see, even it's more cumbersome."

And given Spencer Ackerman's report that the White House wants to give the telecoms immunity under this new "fix," the issue may well go beyond the cell data, though cell data has its own legal risks.

In a statement of principles privately delivered to lawmakers some weeks ago to guide surveillance reforms, the White House said it wanted legislation protecting "any person who complies in good faith with an order to produce records" from legal liability for complying with court orders for phone records to the government once the NSA no longer collects the data in bulk.

[snip]

A congressional aide said the telecommunications companies were expected to "fight hard" for the provision to survive in any surveillance bill. Those firms, including Verizon and AT&T, have typically kept far more silent in public about NSA surveillance and their role in it than internet giants, like Yahoo and Google, which have [pushed for reforms](#).

Ackerman's wrong about Verizon's silence – not only has it already issued a somewhat critical

statement on proposed reforms, it also made a flaccid challenge to a recent order. But its stated concerns refusing to create new records is probably related to the real legal concerns underlying demands for immunity. To get cell records without location information (the latter of which would probably violate US v. Jones), Verizon apparently would and will need to make new records not otherwise required for its business purposes (which, again, may be the source of the cell data problem). That's a very different legal role than simply as a communications provider, one it apparently is not thrilled about playing.

And all that's before you consider the possibility, under the House Intelligence RuppRoge "reform," that these "reforms" would also get Internet content-as-metadata again.

The fact is the government can't legally do what it wants to do. They're trying a new plan, by outsourcing to the providers. But it's not clear that's legal either.