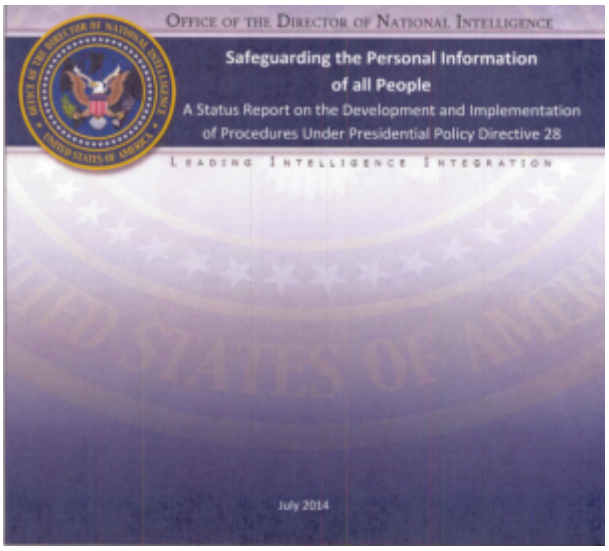
I CON THE RECORD'S INTERNATIONAL PRIVACY GUIDELINES SWALLOWED UP BY EXCEPTIONS

Sometimes I Con the Record outdoes itself.



On Tuesday, the Guardian noted a scathing report UN Counterterrorism special rapporteur Ben Emmerson issued last month attacking British and US collection of bulk communications.

> "Merely to assert – without particularization – that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use. The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful."
>
> [snip]
>
> "It is incompatible with existing concepts of privacy for states to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of

> communication is that infringements must be exceptional, and justified on a case-by-case basis."

Today, I Con the Record released a "Status Report" on an initiative President Obama ordered in his PPD-28 back in January to extend privacy protections to foreigners.

> As we work to meet the January 2015 deadline, PPD-28 called on the Director of National Intelligence to prepare an interim report on the status of our efforts and to evaluate, in coordination with the Department of Justice and the rest of the Intelligence Community, additional retention and dissemination safeguards.
>
> The DNI's interim report is now being made available to the public in line with our pledge to share as much information about sensitive intelligence activities as is possible, consistent with our national security.

One thing this interim report requires is that "elements shall publicly release their PPD-28 implementation policies and procedures to the maximum extent possible." Which requirement, you might assume, this release fulfills.

Which is why it's so curious I Con the Record chose not to release an unclassified report mandated and mandating transparency — dated July 2014 — until October 2014.

Lest I be called a cynic, let me acknowledge that there are key parts of this that may represent improvements (or may not). The report asserts:

- Foreigners will be treated with procedures akin to — though not identical to — those imposed by Section 2.3

of EO 12333

- Just because someone is a foreigner doesn't mean their information is foreign intelligence; the IC should "permanently retain or disseminate such personal information only if the personal information relates to an authorized intelligence requirement, is reasonably believed to be evidence of a crime, or meets one of the other standards for retention or dissemination identified in section 2.3" of EO 12333
- The IC should consider adopting (though is not required to) retention periods used with US person data for foreign personal information (which is 5 years); the IC may get extensions, but only in 5-year chunks of time
- When disseminating "unevaluated personal information," the IC should make that clear so the recipient can protect it as such

Those are good things! Yeah us!

There are, however, a series of exceptions to these rules.

First, the guidelines in this report restate

PPD-28's unbelievably broad approval of the use of bulk data, in full. The report does include this language:

> [T]he procedures must also reflect the limitations on the use of SIGINT collected in bulk. Moreover, Intelligence Community element procedures should include safeguards to satisfy the requirements of this section. In developing procedures to comply with this requirement, the Intelligence Community must be mindful that to make full use of intelligence information, an Intelligence Community element may need to use SIGINT collected in bulk together with other lawfully collected information. In such situations, Intelligence Community elements should take care to comply with the limitations applicable to the use of bulk SIGINT collection.

Unless I'm missing something, the only "limits" in this section are those limiting the use of bulk collection to almost all of NSA's targets, including counterterrorism, cybersecurity, and crime, among other things. Thus, the passage not only reaffirms what amounts to a broad permission to use bulk, but then attaches those weaker handling rules to anything used in conjunction with bulk.

Then there are the other exceptions. The privacy rules in this document don't apply to:

- Evaluated intelligence (exempting foreigners' data from the most important treatment US person data gets, minimization in finished intelligence reports; see footnote 3)
- Personal information collected via other means

than SIGINT (excluding most of what the CIA and FBI do, for example; see page 1)
- Information collected via SIGINT not collecting communications or information about communications (seemingly excluding things like financial dragnets and pictures and potentially even geolocation, among a great many other things; see footnote 2)

And, if these procedures aren't loosey goosey enough for you, the report includes this language:

> It is important that elements have the ability to deviate from their procedures when national security requires doing so, but only with approval at a senior level within the Intelligence Community element and notice to the DNI and the Attorney General.

OK then.

Congratulations world! We're going to treat you like Americans. Except in the majority of situations when we've decided not to grant you that treatment. Rest easy, though, knowing you're data is sitting in a database for only 5 years, if we feel like following that rule.