

NSA KILLS PEOPLE BASED ON METADATA, BUT CAN'T PRESERVE ITS OWN PERSONNEL METADATA FOR A SIMPLE FOIA

Over at Vice News, I've got a story with Jason Leopold on 800 pages of FOIAed documents from the NSA pertaining to their response to Edward Snowden. Definitely read it (but go back Monday to read it after VICE has had time to recover from having NSA preemptively release the documents just before midnight last night).

But for now I wanted to point out something crazy.

There were some funny things about the documents handed over to Leopold, some of which I'll get into over time. By far the funniest is their claim that this email, from SV2 to SV and cc'ed to SV4:

From: [redacted] NSA-SV2 USA CIV (b)(7)P.L. 86-36
Sent: Thursday, April 10, 2014 11:00 AM
To: [redacted] NSA-SV USA CIV
Cc: [redacted] NSA-SV4 USA CIV
Subject: FW: (U) Information Regarding My Contact w/Leaker in April 2013
Importance: High [Below text duplicated in DOCID 4294921]

Is the same as this email, from E63 to SV and cc'ed to SV43.

DOCID: 4294921

[redacted] NSA-DJ4 USA CIV
From: [redacted] NSA-E63 USA CIV
Sent: Thursday, April 10, 2014 11:00 AM
To: [redacted] NSA-SV USA CIV
Cc: [redacted] NSA-SV43 USA CIV
Subject: FW: (U) Information Regarding My Contact w/Leaker in April 2013
Importance: High

We asked them about that – it was one of the few questions from a list of very detailed questions they actually gave us answers to. Here's how they explained it.

Due to a technical flaw in an operating

system, some timestamps in email headers were unavoidably altered. Another artifact from this technical flaw is that the organizational designators for records from that system have been unavoidably altered to show the current organizations for the individuals in the To/From/CC lines of the header for the overall email, instead of the organizational designators correct at the time the email was sent.

Remember, this is the agency that “kills people based on metadata,” per its former Director, Michael Hayden.

But “due to a technical flaw in an operational system,” it could not preserve the integrity of either the time or the aliases on emails obtained under FOIA.

Update: I asked Douglas Cox, who works on these kinds of issues at CUNY School of Law, about this. Here’s what he had to say:

This is an illustration of why most federal agencies are still “print and file” for email preservation purposes, because many can’t seem to properly preserve email in electronic format. Agencies are supposed to be managing emails electronically by the end of this year, but there are doubts many will get there that soon.

If they had a hard copy version and then screwed up the original electronic version by bringing it on to the live system, that would account for differing headers in copies of “same” email, which is bad enough. To the extent they did not have hard copy and they screwed up the only copy in electronic form that is clearly worse. It does raise a real issue.

But your point is right on, even in more mundane contexts not involving drone

strikes it is remarkable the disconnect between standards agencies impose and those they practice. When you are producing docs to a govt agency in response to doc requests, eg, you often have to abide by exacting standards in format including careful capture of metadata, but with FOIA you get things like this.

The artifact in the email – which comes from a string that shows the Compliance training woman modifying her version of the face-to-face interaction with Snowden a year after it happens – must reflect who was printing out documents in timely fashion for the FOIA, and who wasn't (or perhaps which communications threads they figured they'd include and which they wouldn't). It may also reflect which of these people are actually complying with Federal Records Act guidelines.