TRUCK-SIZED HOLES: JOURNALISTS CHALLENGED BY TECHNOLOGY BLINDNESS

[photo: liebeslakritze via Flickr]

Note: The following piece was written just before news broke about Booz Allen Hamilton employee Edward Snowden. With this in mind, let's look at the reporting we've see up to this point; problems with reporting to date may remain even with the new disclosures.

ZDNet bemoaned the failure of journalism in the wake of disclosures this past week regarding the National Security Administration's surveillance program; they took issue in particular with the Washington Post's June 7 report. The challenge to journalists at WaPo and other outlets, particularly those who do not have a strong grasp of information technology, can be seen in the reporting around access to social media systems.

Some outlets focused on “direct access.” Others reported on “access,” but were not clear about direct or indirect access.

Yet more reporting focused on awareness of the program and authorization or lack thereof on the part of the largest social media firms cited on the leaked NSA slides.

Journalists are not asking what “access” means in order to clarify what each corporation understands direct and indirect access to mean with regard to their systems.

Does “direct access” mean someone physically camped out on site within reach of the data center?

Does “direct access” mean someone with global administrative rights and capability offsite of the data center? Some might call this remote access, but without clarification, what is the truth?

I don’t know about you but I can drive a Mack truck through the gap between these two questions.

So which “direct access” have the social media firms not permitted? Which “direct access” has been taken without authorization of corporate management? ZDNet focuses carefully on authorization, noting the changes in Washington Post’s story with regard to “knowingly participated,” changed later to read “whose cooperation is essential PRISM operations.”

This begs the same questions with regard to any other form of access which is not direct. Note carefully that a key NSA slide is entitled, “Dates when PRISM Collection Began For Each Provider.” It doesn’t actually say “gained access,” direct or otherwise.

The next challenge surrounds the questions of authorization and participation. Some news outlets point to the denials by social media firms Yahoo and Google, in which these firms claim no participation in PRISM. Yet the NSA

slides show “acquired access to servers” for these firms.

Again, I can deftly maneuver a 40-foot dry van between these two attributes. The NSA’s acquisition of access does not require conscious authorization or active participation in PRISM. Of course this also hinges on the meaning of “access.”

[Insert Princess Bride pop culture reference here: “I do not think that word means what you think it means.”]

There’s one more wrinkle further clouding reporting, about which journalists are not demanding clarification, and that is the program itself.

> An Apple spokesman said it had “never heard” of Prism.

[Guardian, 13-JUN-2013]

The natural followup for all other reporters:

> — Have any Apple employees, management or its board of directors heard of PRISM?
> — Have any Apple employees, management or its board of directors heard of US-984XN?
> — Have any Apple employees, management or its board of directors heard of any U.S., state/local, or international government project not named PRISM or US-984XN through which non-corporate employees are granted direct access, remote access, or access in any shape or form to data flowing into or out of data center servers?
> — Are any of Apple employees, management or its board of directors aware of any government-installed or government-monitored network installations directly outside the data centers, through which incoming and/or outgoing data flows into the WAN?
> — How many federal or state court orders requiring copies of data, apart from National Security Letters, have the social media providers complied with — top secret

or otherwise?

Insert Google, Yahoo, Paltalk, AOL here instead of Apple and ask the same questions. (Don't waste time with Stuxnet-enabler Microsoft.)

Having brought up US-984XN, the next challenge is compartmentalization, by which I mean a program inside a program. What if PRISM is inside US-984XN, or vice versa? What does the larger of the two programs look like, if this is the case? Can a compartmentalized program explain the carefully worded denials or lack of recognition when it comes to PRISM?

Does the larger program – directed by Presidential Policy Directive 20 (pdf) issued 16-OCT-2012 and likely shaped by predecessor National Security Presidential Directive 54 issued 08-JAN-2008 – included monitoring systems sitting outside the social media corporate data centers, installed somewhere along the WAN?

Will any journalist start asking the network service providers? Granted, they'll likely offer non-denial denials, but it'd be nice to have them on record. The truth may be disclosed by the shape of the black hole formed by their reluctant responses.

Perhaps ZDNet will look more carefully at the Guardian's report, which spawned much of the subsequent confusion among its technologically uninformed competitors. Where exactly did the Guardian obtain the fact or come to the conclusion that the NSA had obtained "direct access" to major social medial providers' servers? The public cannot see this in the slides they have revealed so far.

Don't even get me started on the possibility of wireless network sniffing systems invisibly monitoring content sent between towers and the internet's backbone.

Or the lack of questions about the NSA slide tagline, "The SIGAD Used Most in NSA Reporting" (boldface theirs).

Or questions about the WaPo’s redaction of the title, “PRISM Collection Manager, S35333” from the slide the Guardian had already published.