THE STALKER OUTSIDE YOUR WINDOW: THE NSA AND A BELATED HORROR STORY

[photo: Gwen's River City Images via Flickr]

It's a shame Halloween has already come and gone. The reaction to Monday's Washington Post The Switch blogpost reminds of a particularly scary horror story, in which a young woman alone in a home receives vicious, threatening calls.

There's a sense of security vested in the idea that the caller is outside the house and the woman is tucked safely in the bosom of her home. Phew, she's safe; nothing to see here, move along…

In reality the caller is camped directly outside the woman's window, watching every move she makes even as she assures herself that everything is fine.

After a tepid reaction to the initial reporting last week, most media and their audience took very little notice of the Washington Post's followup piece – what a pity, as it was the singular voice confirming the threat sits

immediately outside the window.

Your window, as it were, if you have an account with either Yahoo or Google and use their products. The National Security Agency has access to users' content inside the corporate fenceline for each of these social media firms, greasy nose pressed to glass while peering in the users' windows.

There's more to story, one might suspect, which has yet to be reported. The disclosure that the NSA's slides reflected Remote Procedure Calls (RPCs) unique to Google and Yahoo internal systems is only part of the picture, though this should be quite frightening as it is.

Access to proprietary RPCs means – at a minimum – that the NSA has:

1) Access to content and commands moving in and out of Google's and Yahoo's servers, between their own servers – the closest thing to actually being inside these corporations' servers.

2) With these RPCs, the NSA has the ability to construct remote login access to the servers without the businesses' awareness. RPCs by their nature require remote access login permissions.

3) Construction through reverse engineering of proprietary RPCs could be performed without any other governmental bodies' awareness, *assuming the committees responsible for oversight did not explicitly authorize access to and use of RPCs* during engineering of the MUSCULAR/SERENDIPITY/MARINA and other related tapping/monitoring/collection applications.

4) All users' login requests are a form of RPC – every single account holder's login may have been gathered. This includes government employees and elected officials as well as journalists who may have alternate accounts in either Gmail or Yahoo mail that they use as a backup in case their primary government/business account fails, or in the case of journalists, as a backchannel for handling news tips.

5) The public may not understand, nor may they ever receive adequate clarification with regard to the breadth of NSA's access over time to Google's and Yahoo's content, given the rolling application of masking methodology which ostensibly protected non-targets' data. In 2006, Google researchers disclosed that as many as 60 applications used "Bigtable" [PDF] – a proprietary distributed storage system for structured data. That number is likely larger today, but some applications have come and gone since then. What Google applications don't use Bigtable, and are otherwise not included in the "defeat" list believed to be the applications excluded from tapping/monitoring/collection applications? We don't know on the face of it; Google engineers do, of course, though they may not be able to communicate this publicly for proprietary and security reasons. Further, what content was monitored and collected from the initial tap to today's partially masked state? There was a slow ramp up of the defeat list over time; the applications on the list to be masked off from NSA's screening/collection were not present initially. We can only assume that the same challenges exist with Yahoo's content and applications – or worse, given the business's somewhat disorganized approach to its application portfolio up until 2012.

6) The data screened/collected including the RPCs may also include metadata – it may indicate users' location by IP address, which in some cases is the same as a physical address. It's not at all clear this was masked out for any user.

7) To bypass the Secure Sockets Layer (SSL) employed to secure transmissions between users and the social media businesses' servers, the NSA tapped either private and/or leased lines directly between servers, not the public transmission lines between users and servers, in order to access Google's and Yahoo's content as it moved between servers. This is yet another example of the NSA ignoring property rights, though they may claim that because the taps were

located outside the US they were not limited by US law.

In spite of these challenges, the media and the public continue on blithely as if there were no new problems revealed this last week with regard to the NSA's behavior.

What should truly shake them up is not merely the threats revealed so far, or the initial angry reaction of Google engineers shared by the Washington Post in the 30-OCT revelatory article.

It's the persistent and increasing anger of Google engineers who are now going public, though speaking not for Google but as individuals about the breach of Google's systems by the NSA. The degree of anger suggests there is far more to this story than appears on the surface. What would torque off engineers enough to be so deeply angry, so very openly?

As @Public_Archive tweeted earlier this week,

> We've reached a point in history where the writings of JG Ballard & Philip K Dick have clattered into the quotidian realm of realism.

Be afraid; the horror is no longer a mere story. Happy much-belated Halloween.