XKEYSCORE SUFFERS FROM SAME GIANT OVERSIGHT LOOPHOLE AS PHONE DRAGNET AND SIGDEV: NO TECH AUDITS

I’ve long pointed to a giant oversight hole in key NSA programs: in both the domestic phone dragnet and SIGDEV (research and development), tech activities are excluded from auditing requirements.

In a piece reviewing what happens with XKS today, Intercept’s Micah Lee points out that the same loophole appears to exist in XKeyscore, the querying system that filters through the globally collected data. Sysadmins not only don’t have their own audited log-ins (a condition that appears to be what was in existence for the PRTT dragnet until 2009), but they can access the system outside of the normal querying process that gets audited.

> When systems administrators log into XKEYSCORE servers to configure them, they appear to use a shared account, under the name “oper.” Adams notes, “That means that changes made by an administrator cannot be logged.” If one administrator does something malicious on an XKEYSCORE server using the “oper” user, it’s possible that the digital trail of what was done wouldn’t lead back to the administrator, since multiple operators use the account.
>
> There appears to be another way an ill-intentioned systems administrator may be able to cover their tracks. Analysts wishing to query XKEYSCORE sign in via a web browser, and their searches are logged. This creates an audit trail, on

> which the system relies to assure that users aren’t doing overly broad searches that would pull up U.S. citizens’ web traffic. Systems administrators, however, are able to run MySQL queries. The documents indicate that administrators have the ability to directly query the MySQL databases, where the collected data is stored, apparently bypassing the audit trail.

Now, Lee is just pointing out a problem that exists technically, based on the documents describing the system.

But as we’ve seen, with the phone dragnet, at least, this is by design. The NSA simply doesn’t track tech functions as closely as it does analysts, which are more closely watched (but some, not all, of whose activities are still subject to randomness of audits), even though some techs have more direct access to raw data (by necessity). Indeed, what Snowden accomplished would have been impossible — or at least, would have been tracked more quickly than months — if this weren’t the case.

Whether or not you support NSA’s dragnet, this is a bureaucratic problem, one that rightly raises questions about the good faith of the system.

NSA said that after Snowden they instituted two person sign-off for some activities. They’d do well to release evidence they have actually done so.