

“TOR STINKS” ... BECAUSE IT REQUIRES MANUAL (DIGITAL) TAILS



Stinks ^(TM)

“Tor
stinks
,” the
Guardi
an
report

s one NSA document asserting, in a new story on NSA’s efforts to break that encryption system.

And while Bruce Schneier explains how the NSA uses similar techniques to those the Chinese government uses to spy on its users – something called Egotistical Giraffe – to break Tor, and the NSA has been able to crack other users’ communications via their poor hygiene outside of Tor (as with this week’s bust of Silk Road), the NSA has thus far been unable to systematically break the system.

At base, though, NSA believes that Tor stinks because,

We will never be able to de-anonymize all Tor users all the time.

With manual analysis we can de-anonymize a very small fraction of Tor users, however no success at de-anonymizing a user in response to a TOPI request/on demand.

Another complaint the NSA has is their methods for cracking Tor right now are “difficult to combine meaningfully with passive Sigint.” That is, they can’t just feed everything into a system and get potential targets to pop out.

To me, this boils down to a complaint that if the NSA wants to track users – the ones they can identify – they have to work as hard as cops used to in physically tracking suspects. That means (as NSA’s recent success busting 2 Tor

users makes clear) they can track people. They just have to work at it.

We'll hear a lot about how breaking Tor is a noble cause and NSA (and GCHQ) have to do it to keep us safe from the "very naughty people" who use Tor. But ultimately, it seems, one question is whether the NSA should get to break the law to make it as easy to track encrypted users as using GPS to track physical location has become.

NSA wants its targets to – effectively – come to it. It doesn't want to have to identify targets and then crack their communications. But Tor, at least thus far, has made it as hard to do so as it used to be to physical track suspects.