ARE THE AUTHORITIES CONFUSING A PRISM PROBLEM WITH AN ENCRYPTION PROBLEM?

CNN has its own version of updated reporting from the Paris attack. It provides a completely predictable detail inexplicably not included in the weekend's big NYT story: that the one phone with any content on it — as distinct from a pure burner — had Telegram loaded on it.

> Several hours earlier, at 2:14 p.m., while they were still at the Alfortville hotel, the Bataclan attackers had downloaded the encryption messaging app Telegram onto their Samsung smart phone, according to police reports. No recovered content from the messaging app is mentioned in the French police documents, suggesting there were likely communications by the Bataclan attackers that will never be recovered.
>
> As well as offering end-to-end encryption, the Telegram messaging app offers an option for users to "self-destruct" messages. At 4:39 p.m. on November 13, one of the attackers downloaded detailed floor plans of the Bataclan venue onto the Samsung phone and conducted online searches for the American rock band playing there that night, the Eagles of Death Metal.

I predicted as much in my post on that NYT story.

> My suspicion is that, as had been reported, rather than emails ISIS relied on Telegram, but used in such a fashion that would make it less useful on burner phones ("secret" Telegram chat are device specific, meaning you'd need a

> persistent phone number to use that function). But if these terrorists did use Telegram, they probably eluded authorities not because of encryption, but because it's fairly easy to make such chats temporary (again, using the secret function). Without Telegram being part of PRISM, the NSA would have had to obtain the metadata for chats via other means, and by the time they IDed the phones of interest, there may have been no metadata left.

If ISIS' use of Telegram (which was publicly acknowledged when Telegram shut down a bunch of ISIS channels in the wake of the attack) is what anonymous sources keep insisting is an encryption problem, then it suggests the problem is being misportrayed as an encryption one.

True, Telegram does offer the option of end to end encryption for its messaging. There are questions about its encryption (though thus far it hasn't been broken publicly). So it does offer users the ability to carry out secret chats and to then destroy them, which may be where the concern about all the "scoured" "email" in the NYT piece comes from, the assumption these terrorists have used Telegram but deleted those messages.

But as the Grugq points out, it's a noisy app in other ways that the NSA should be able to exploit.

> ## *Contact Theft*
>
> When registering an account with Telegram, the app helpfully uploads the entire Contacts database to Telegram's servers (optional on iOS). This allows Telegram to build a huge social network map of all the users and how they know each other. It is extremely difficult to remain anonymous while using Telegram because the social network of everyone

> you communicate with is known to them (and whomever has pwned their servers).
>
> Contact books are extremely valuable information. We know that the NSA went to great lengths to steal them from instant messenger services. On mobile the contact lists are even more important because they are very frequently linked to real world identities.
>
> ## *Voluminous Metadata*
>
> Anything using a mobile phone exposes a wide range of metadata. In addition to all the notification flows through Apple and Google's messaging services, there is the IP traffic flows to/from those servers, **and** the data on the Telegram servers. If I were a gambling man, I'd bet those servers have been compromised by nation state intelligence services and all that data is being dumped regularly.
>
> This metadata would expose who talked with who, at what time, where they were located (via IP address), how much was said, etc. There is a huge amount of information in those flows that would more than compensate for lacking access to the content (even if, big assumption, the crypto is solid).

He spends particular time on Telegram's Secret chat function (the one that allows a person to destroy a chat). But he doesn't talk about how that might play into the extensive use of burners that we've seen from ISIS. Secret chats are device specific (that is, they can be sent only to a numbered device, not an account). That would make the function very hard to integrate with disciplined burner use, because the whole point of burners is not to have persistent telephone numbers. How will a terrorist remember the new number he wants to associate with a

Telegram secret chat? Write it on a piece of paper?

In other words, it seems you could use one (disciplined burners) or another (full use of Telegram with persistent phones), the latter of which would provide its own kind of intelligence. It may well be ISIS does merge these two uses, but if so we shouldn't expect to see Telegram on their true burner phones. Plus, assuming the bearer of the phone speaks that dialect the Belgians were struggling to translate, voice calls on burners would be just as useful as transient use of Telegram.

But that's probably not the real problem for authorities. In fact, if known terrorists had been using, say, WhatsApp rather than Telegram for such encrypted chats, authorities might have had more information on their network than they do now. That's because WhatsApp metadata would be available under PRISM, whereas to get Telegram data, non-German authorities are going to have to go steal it.

If that supposition is correct, it would suggest that the US should drop all efforts to make Apple phones' encryption weaker. So long as it has the presumed best security (notwithstanding the iMessage vulnerability just identified by researchers at Johns Hopkins), people from around the world will choose it, ensuring that the world's best SIGINT agency could have ready access. If Telegram is perceived as being better — or even being close, given the location — people of all sorts will prefer that.

That won't give you the content, in either case (even if you had the Moroccan translators you needed to translate, if that indeed remained a problem for authorities). But you're better off having readily accessible metadata than losing it entirely.