DIANNE FEINSTEIN INADVERTENTLY CALLS TO EXPOSE AMERICA'S CRITICAL INFRASTRUCTURE TO HACKERS

For days now, surveillance hawks have been complaining that terrorists probably used encryption in their attack on Paris last Friday. That, in spite of the news that authorities used a phone one of the attackers threw in a trash can to identify a hideout in St. Denis (this phone in fact might have been encrypted and brute force decrypted, but given the absence of such a claim and the quick turnaround on it, most people have assumed both it and the pre-attack chats on it were not encrypted).

I suspect we'll learn attackers *did* use encryption (and a great deal of operational security that has nothing to do with encryption) at some point in planning their attack — though the entire network appears to have been visible through metadata and other intelligence. Thus far, however, there's only one way we know of that the terrorists used encryption leading up to the attack: when one of them paid for things like a hotel online, the processing of his credit card (which was in his own name) presumably took place over HTTPS (hat tip to William Ockham for first making that observation). So if we're going to blindly demand we prohibit the encryption the attackers used, we're going to commit ourselves to far far more hacking of online financial transactions.

I'm more interested in the concerns about terrorists' claimed use of PlayStation 4. Three days before the attack, Belgium's Interior Minister, said all countries were having problem with PlayStation 4s, which led to a frenzy

mistakenly claiming the Paris terrorists *had* used it (there's far more reason to believe they used Telegram).

> One of those alternatives was highlighted on Nov. 11, when Belgium's federal home affairs minister, Jan Jambon, said that a PlayStation 4 (PS4) console could be used by ISIS to communicate with their operatives abroad.
>
> "PlayStation 4 is even more difficult to keep track of than WhatsApp," said Jambon, referencing to the secure messaging platform.
>
> Earlier this year, Reuters reported that a 14-year-old boy from Austria was sentenced to a two-year jail term after he downloaded instructions on bomb-building onto his Playstation games console, and was in contact with ISIS.
>
> It remains unclear, however, how ISIS would have used PS4s, though options range from the relatively direct methods of sending messages to players or voice-chatting, to more elaborate methods cooked up by those who play games regularly. Players, for instance, can use their weapons during a game to send a spray of bullets onto a wall, spelling out whole sentences to each other.

This has DiFi complaining that Playstation is encrypted.

> Even Playstation is encrypted. It's very hard to get the data you need because it's encrypted

Thus far, it's not actually clear most communications on Playstation are encrypted (though players may be able to pass encrypted objects about); most people I've asked think the communications are not encrypted, though Sony

isn’t telling. What is likely is that there’s not an easy way to collect metadata tracking the communications within games, which would make it hard to collect on whether or not some parts of the communications data are encrypted.

But at least one kind of data on Playstations — probably two — is encrypted: Credit cards and (probably) user data. That’s because 4 years ago, Playstation got badly hacked.

> “The entire credit card table was encrypted and we have no evidence that credit card data was taken,” said Sony.
>
> This is the slimmest amount of good news for PlayStation Network users, but it alone raises very serious concerns, since Sony has yet to provide any details on what sort of encryption has been used to protect that credit card information.
>
> As a result, PlayStation Network users have absolutely no idea how safe their credit card information may be.
>
> But the bad news keeps rolling in:
>
> “The personal data table, which is a separate data set, was not encrypted,” Sony notes, “but was, of course, behind a very sophisticated security system that was breached in a malicious attack.”
>
> A very sophisticated security system that ultimately failed, making it useless.
>
> Why Sony failed to encrypt user account data is a question that security experts have already begun to ask. Along with politicians both in the United States and abroad.
>
> Chances are Sony’s not going to have an answer that’s going to please anyone.

After one in a series of really embarrassing hacks, I assume Sony has locked things down more since. Three years after that Playstation hack, of course, Sony's movie studio would be declared critical infrastructure after *it* also got hacked.

Here's the thing: Sony is the kind of serially negligent company that we need to embrace good security if the US is going to keep itself secure. We should be saying, "Encrypt away, Sony! Please keep yourself safe because hackers love to hack you and they've had spectacular success doing so! Jolly good!"

But we can't, at the same time, be complaining that Sony offers some level of encryption as if that makes the company a material supporter of terrorism. Sony is a perfect example of how you can't have it both ways, secure against hackers but not against wiretappers.

Amid the uproar about terrorists *maybe* using encryption, the ways they may have — to secure online financial transactions and game player data — should be a warning about condemning encryption broadly.

Because next week, when hackers attack us, we'll be wishing our companies had better encryption to keep us safe.