IN BIZARRE MOVE, DIANNE FEINSTEIN ATTACKS TECH COMPANIES FOR PROFITING OFF SPYING ON THEIR CUSTOMERS

Dianne Feinstein attacked PRISM providers' use of encryption in yesterday's Senate Judiciary Committee hearing with Loretta Lynch in really bizarre fashion.

> Feinstein: Google, Microsoft, Dropbox, and other email and cloud servers use forms of encryption to protect customer data. Their encryption techniques are strong and that makes them relatively well protected against outside attack. But the reality is that many companies only protect data like your email in ways that they can still use it themselves, and profit from it. I believe that the amount of personal information in the hands of private corporations and what some of those corporations are doing with that data is concerning. Isn't it true that private companies can encrypt data so that it is protected from outsiders but at the same time those same companies can use our personal content data to target advertisements?
>
> Attorney General Lynch: Thank you Senator for raising this important issue. It certainly is the case that many companies – those that you mentioned and others – have strong encryption, which we think is a very positive thing, and yet retain the ability to use the data that is transmitted along their systems, both

> for security purposes as well as for marketing purposes. And so it is certainly the case, as we have seen in our talks with various companies, that strong encryption can be accompanied with the ability to still access the data and use the data in relevant ways. And we think that this is something that's part of the overall debate on this important issue as we all consider – as you have also noted – how much personal information we willingly turn over to private companies and how we want that information handled. And certainly as we continue to discuss this issues I thank you for raising them and making them part of the debate.
>
> Feinstein: Well, thank you very much because with my own devices, and I'm not the most "hep" person when it comes to all of this [raising phone] I've been amazed to learn what I can't control. And my understanding is that it's private information like web browsing history, email content, geolocation information, even when encrypted on smart phones. So I think it is an area of concern as companies want to defy a probable cause warrant, that they can use this data for their own profit making motives, and that's of concern.

First, let me remind you: this woman represents Silicon Valley! And yet it's not clear precisely what she means here.

Don't get me wrong: I'd love to have a service with the facility of Google but without all the snooping on content and location. It concerns me that Google keeps much of that information even if you opt out of most data sharing.

But why is the Ranking Member of the Collect It All Committee raising these concerns – aside from maybe just now learning how much companies have on her? Indeed, it seems there are at least

three reasons why a Collect It All fan should prefer this option:

- The proprietary information these companies collect — at least the cookies and location data — is available both with a subpoena and under PRISM. Indeed, it should provide some of the most interesting information about intelligence and law enforcement targets.
- DiFi has just championed a bill that makes the packet sniffing DiFi claims to be concerned about — which allows Google to target us for advertising — more useful for government cybersecurity purposes, too, as Google can not only sniff for their own security purposes, but also share what they find with the government.
- The Administration is in the middle of a campaign — successful with at least Facebook and probably with some services on Google as well — to ask tech companies to use their marketing algorithm function to disfavor ISIS propaganda and favor counter-propaganda.

In other words, DiFi should *love* this state of

affairs!

The only explanation (aside from some recent discovery of how much of her own data these companies have) I can think of is that DiFi has learned how little data iMessage and Signal collect on people, and was supposed to complain that she is furious that companies that, by collecting so little, limit how cooperative they can be in cases of legal requests, also offer security for their customers. But she appeared to be reading from a written statement, so that doesn’t make sense either.

The only other possibility I can imagine is that the government is trying to expand its access to this proprietary information under PRISM, and providers are balking. Which would be rather interesting.