PUREVPN DOESN'T NEED TO KEEP LOGS GIVEN HOW MANY GOOGLE KEEPS

There's a cyber-stalking case in MA that has a lot of people questioning whether or not VPNs keep serial cyber-stalkers safe from the FBI. In it, Ryan Lin is accused of stalking a former roommate, referred to by the pseudonym Jennifer Smith in the affidavit, as well as conducting some bomb hoaxes and other incidences of stalking (if these accusations are true he's a total shithole with severe control problems).

Because the affidavit in the case refers to tying Lin's usage to several VPNs, it has been read to confirm that PureVPN, especially, has been keeping historic logs of users, contrary to their public claims. To be clear: you can never know whether a VPN is honest about keeping logs or not, and simply having a VPN on your computer might provide means of compromise (sort of like an anti-virus), that makes you more vulnerable. But I don't think the affidavit, by itself (particularly with a great deal of the evidence in the case still hidden), confirms PureVPN is keeping logs. Rather, I think the account matching described in the affidavit says the FBI could have identified which VPNs Lin used via orders to Google, Facebook, and other tech companies, and using that, obtained a pen register on PureVPN collecting prospective traffic. I don't think what is shown proves that FBI obtained historic logs (though it doesn't disprove it either).

One thing to understand about this case is that Lin would have been the suspect right from the start, because his stalking started while he still lived with Smith, and intensified right after his roommates got him evicted. Plus, some of his stalking of Smith and others involved his real social media accounts. That means that, at

a very early stage in this investigation, FBI would have been able to get all this information from Google and Facebook, which his victims knew he used.

> A. The following information about the customers or subscribers of the Account:
> 1. Names (including subscriber names, user names, and screen names);
> 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
> 3. Local and long distance telephone connection records;
> 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
> 5. Length of service (including start date) and types of service utilized;
> 6. Telephone or instrument numbers (including MAC addresses);
> 7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol ("IP") addresses (including carrier grade natting addresses or ports)); and
> 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
>
> B. All records and other information (not including the contents of communications) relating to the Account, including:
> 1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
> 2. Information about each communication

> sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);
> 3. Records of any accounts registered with the same email address, phone number(s), method(s) of payment, or IP address as [] the accounts listed in Part 1; and Records of any accounts that are linked to either of the accounts listed in Part 1 by machine cookies (meaning all Google user IDs that logged into any Google account by the same machine as [] the accounts in Part 1). [my emphasis]

So very early in the investigation (almost certainly 2016), the FBI would have started obtaining every IP address that Lin was using to access Google and Facebook, and any accounts tied to the IP addresses used to log into his known accounts.

Instragram IDs WAN usage

Now consider the different references to VPNs in the affidavit. First, in February 2017, Lin registered a new Instagram account via WAN Security, one of the three VPNs listed.

> February 2017: Lin registers Instagram account via WAN Security, also uses it to send email from ryan@ryanlin.com to local police department

That would mean that from the time FBI learned he used WAN to register with Instagram, the FBI would have known he used that service, and probably would have a very good idea which WAN server he default logged into.

Gmail ties WAN usage to other pseudonymous accounts

Then, FBI tracked April 2017 activity to connect Lin to an anonymous account at a service called Rover that he used to stalk people.

- April 14, 2017, 14:55:52: Lin's Gmail address accessed from IP address tied to WANSecurity server
- April 14, 2017, 15:06:27: "Ashley Plano," using teleportx@gmail.com, accessed Rover via same WANSecurity server
- April 17, 2017, 21:54:25: "Ashley Plano" accesses Rover via Secure Internet server
- April 17, 2017, 23:19:12: Lin's Gmail address accessed via same Secure Internet server
- April 18, 2017, 23:48:28: Lin's Gmail address accessed via same Secure Internet server
- April 19, 2017, 00:30:11: Ashley Plano account accessed via same Secure Internet server
- April 24, 2017 (unspecified times): Lin's Gmail and teleportx@gmail.com email account accessed via

same Secure Internet server

The WAN Security usage would have been accessible from Lin's Gmail account (and would have been known since at least February). A subpoena to Rover after reports it was used for stalking would have likewise shown the WAN Security usage and times (assuming their logs are that detailed).

The Secure Internet use would have likewise shown up in his Gmail usage. Matching that to the Rover logs would have been the same process as with the WAN Security usage. And matching Lin's known Gmail to his (alleged) pseudonymous teleportx email would have been done by Google itself, matching other accounts accessed by the IP Lin used (though they would have had to weed out other multiple Secure Internet server users).

In other words, this stuff could have come — and almost certainly did — from 2703(d) order returns available with a relevance standard, probably starting months before this activity.

Work computer confirms PureVPN usage, may provide account number

Then there's this information, tying Lin's work computer to PureVPN.

> July 24, 2017: Lin fired by his unnamed software company employer — he asks, but is denied, to access his work computer to sign out of accounts
>
> August 29, 2017: FBI agents find "Artifacts indicat[ing] that PureVPN, a VPN service that was used repeatedly in the cyberstalking scheme, was installed on the computer."

What is not mentioned here is whether the "artifact" that showed Lin, like a fucking

moron, loaded PureVPN onto his work computer also included him loading his PureVPN account number onto the computer. I think the vagueness here is intentional — both to keep the information from us and from Lin (at least until he signs a protection order). I also think this discussion, while useful for establishing probable cause to search his house, is also a feint. I suspect they already had Lin tied to PureVPN, and probably to a specific account there.

FBI's not telling when and how they IDed Lin's PureVPN usage, but Google would have had it

Which leads us to this language, which is the stuff that has everyone wigged out about PureVPN keeping logs.

> Further, records from PureVPN show that the same email accounts—Lin's gmail account and the teleportfx gmail account—were accessed from the same WANSecurity IP address. Significantly, PureVPN was able to determine that their service was accessed by the same customer from two originating IP addresses: the RCN IP address from the home Lin was living in at the time, and the software company where Lin was employed at the time.
>
> [snip]
>
> PureVPN also features prominently in the cyberstalking campaign, and the search of Lin's workplace computer showed access of PureVPN.

Unlike almost every reference in this affidavit, there's no date attached to this knowledge. It

appears after the work computer language, leaving the impression that the knowledge came after the work computer access. But particularly since FBI alleges Lin used PureVPN for a lot of his stalking, they probably were looking at PureVPN much earlier.

One thing is certain: FBI could have easily IDed a known PureVPN server accessing Lin's Gmail account and the teleportfx one FBI identified at least as early as April, months before finding PureVPN loaded onto his work computer.

The FBI doesn't say which victims Lin accessed via PureVPN or when, only that it figured prominently. It does say, however, that PureVPN identified use from both Lin's home and work addresses.

Most importantly, FBI doesn't say when they asked PureVPN about all this. Nothing in this affidavit rules out the FBI serving PureVPN with a PRTT to track ongoing usage tied to Lin's known accounts (rather than historical usage tied to them). Mind you, there's nothing to rule out historical logs either (as the affidavit also notes, Lin at one point tweeted something indicating knowledge that VPNs will at least keep access information tied to users).

Here's the thing, though: if you're using the same Gmail account tied to the same home IP to access three different VPN providers, often on the same day, your VPN usage is going to be identified from Google's extensive log keeping. It is an open question what the FBI can do with that knowledge once they have it — whether they can only collect prospective information or whether a provider is going to have some useful historical knowledge to share. But the FBI didn't need historic logs from PureVPN to get to Lin.