“DUDE, THAT’S WHAT THEY WANT.”

Babak Pasdar’s affidavit on Verizon’s Quantico Circuit reveals something about the government’s back-door access to all of Verizon’s data, one which might be familiar to you from the missing White House emails saga.

When the Steven McDevitt tried to reconstruct all OVP the emails from the period when Scooter Libby and Dick Cheney were coordinating their cover story, he discovered no logs from the emails of that period existed; thus, there’s no way to be sure that the 250 pages of email turned over to Patrick Fitzgerald constitute all the missing emails.

Golly. What a surprise, then, that the government didn’t want any logs taken of its back-door access to (presumably) Verizon’s data.

Pasder notes that (presumably) Verizon’s log collection system was very primitive.

> I specifically remembered being shocked at the primitiveness and inadequacy of their log collection system. After all, this was a major carrier. After a cursory overview I was able to point out to C1 and C2 that their log collection system might not have been collecting all logs. This surprised C1 and C2. A subsequent test showed that the client’s log collection system was missing as many as 75% of the logs being generated, essentially rendering the whole system useless.

Mind you, that covered the whole system, not just the Quantico Circuit the government was using to access the system. But when Pasdar describes learning about the Circuit itself, he explains that there was no logging system for the Circuit. None.

This is a little narrative he tells about learning of the Circuit when testing the firewalls of the new system he was putting in.

> At one point I overheard C1 and C2 talking about skipping a location. Not wanting to do a shoddy job I stopped and said "we should migrate all sites."
>
> C1 told me this site is different.
>
> I asked, "Who is it? Carrier owned or affiliate?"
>
> C1 said, "This is the ‘Quantico Circuit.’"

Pasdar goes on to learn that this is a 45 mega bit per second circuit that supports data and voice communication. The consultants he was working with made it clear they weren’t supposed to put any access controls on it.

> C1 said that this circuit should not have any access control. He actually said it should not be firewallled.
>
> I suggested to migrate it and implement an "Any-Any" rule. ("Any-Any" is a nickname for a completely open policy that does not enforce any restrictions.) That meant we could log any activity making a record of the source, destination and type of communication. It would have also allowed easy implementation of access controls at a future date. "Everything at least SHOULD be logged," I emphasized.
>
> C1 said, "I don’t think that is what they want."

As Pasdar continued to insist on securing the circuit, the consultants called in the Director of Security for (presumably) Verizon, the Director drove to the location to insist that Pasdar do nothing with the wide open circuit. After the Director left, Pasdar persisted.

> I shifted the focus. "Forgetting about who [the circuit] is, don't you think it is unusual for some third party to have completely open access to your systems like this? You guys are even firewalling your internal offices, and they are part of your own company!"
>
> C1 said, "Dude, that's what they want."

Finally, Pasdar asks whether there is any logging tied to the circuit.

> "Does this thing have any logging or access list tied to it?", I asked C1.
>
> He paused, shook his head in the negative and said, "I don't think so."
>
> For the balance of the evening and for some time to come I thought about all the systems to which this circuit had complete and possibly unfettered access. The circuit was tied to the organization's core network. It had access to the billing system, text messaging, fraud detection, web site, and pretty much all the systems in the data center without apparent restrictions.
>
> What really struck me was that it seemed no one was logging any of the activity across this circuit. **And if they were, the logging system was so abysmal that they wouldn't capture enough information to build any type of picture of what had transpired. Who knw what was being sent across the circuit and who was sending it? To my knowledge no historical logs of the communications traversing the "Quantico Circuit" exists**. [my emphasis]

In other words, not only did they tap right into (presumably) Verizon's circuits directly. But they refused to allow a record of what they were doing, once they got into the circuits, be made.

No wonder the Republicans refuse to allow segregation of US person data. No wonder they refuse to pull out information collected afterwards if it was later found to be an improper search. At the circuit level, at least, they're not tracking that information.

And they didn't want anyone to come afterwards and be able to track what they had done, either.