DOJ'S CLAIMS ABOUT THE ADEQUACY OF SHITTY WIFI RENDERED INOPERATIVE

Over at Vice, I have a piece reviewed DOJ's explanation for why they turned off some alleged Asian mobsters DSL so they could then go in as fake DSL repairmen and collected evidence.

The whole thing has a Keystone cops character, especially since the DSL contractor they had roped into working with them screwed up turning off the DSLs, which is why they now claim he was on a "private frolic" when he collected information on his own (that is a technical legal term meaning "freelancing," but one doing far more than the evidence allows, in my opinion).

My favorite part, though, is how DOJ claims that turning off someone's DSL would not create any kind of urgency which would eliminate the notion of consent, because after all they could have used the shitty hotel WiFi.

> Perhaps the most disturbing claim, though, is that we all have to be satisfied with crummy hotel Wi-Fi. To dismiss the argument that by turning off the villas' DSL, FBI had created an urgent need that obviated any kind of consent when the villa residents let in the FBI agents pretending to be DSL repairmen, the government claims that there is no legitimate need to seek better internet access than hotel Wi-Fi or personal cell phone tethers: "Defendants do not identify a single legitimate service or application that could not be adequately supported through the hotel's WI-FI system, their personal hotspots, or personal cellphones, nor could they."

> The FBI is now claiming, the experience of travelers the world over notwithstanding, that nothing legal could require better Internet access than a hotel's slow Wi-Fi connection. (Perhaps the Wi-Fi in high-roller villas is better than it is for average travelers, but DOJ's brief doesn't make that case by describing the internet speeds Caesars Palace makes available to privileged guests.) Moreover, the government admits that—as many travelers reliant on hotel Wi-Fi can attest—the Wi-Fi just wasn't all that fast. "The DSL service was faster," the brief reads.

I mean, I'm not a Malaysian gangster or anything, but I often find myself trying to do things in hotel rooms where neither the WiFi nor my cell phone's tether provides remotely adequate speed. You know — simple things like posting on a blog. Apparently that's illegitimate now.

And yes, I have called hotel technicians to help me get the hotel WiFi working and let them right into my room.

Even as I was working on that piece, Kaspersky Lab came out with a warning that hackers (possibly working out of South Korea) have been targeting businessmen through hotel WiFis for 7 years.

> Business executives visiting luxury hotels in Asia have been infected with malware delivered over public Wi-Fi networks, Russian security firm Kaspersky Lab has discovered.
>
> The so-called 'Darkhotel' hackers managed to tweak their code to ensure that only machines belonging to specific targets were infected, not all visitors' PCs, and may have included state-sponsored hacking.

> They also seemed to have advance knowledge of their victims' whereabouts and which hotels they would be visiting, Kaspersky said.
>
> CEOs, senior vice presidents, sales and marketing directors and top research and development staff were amongst those on the attackers' hit list, though no specific names have been revealed.
>
> As soon as they logged onto the hotel Wi-Fi, targets would be greeted with a pop-up asking them to download updates to popular software, such as GoogleToolbar, Adobe Flash and Windows Messenger. But giving permission to the download would only lead to infection and subsequent theft of data from their devices.

You think alleged Asian organized crime members might know that hotel wifi is totally insecure (even setting aside China's habit of stealing it this way)? You think they may have heard of their peers getting hacked in luxury hotels?

Maybe that's why they ordered up so many DSL lines.

In any case, DOJ's argument that there's no legitimate need for wired Internet access just went out the window.