WIRED

FBI's Latest Proposal for a Wiretap-Ready Internet Should Be Trashed

By: Julian Sanchez – May 10,2013

The FBI has some strange ideas about how to "update" federal surveillance laws: They're calling for legislation to penalize online services that provide users with *too much* security.

I'm not kidding. The proposal was revealed in *The Washington Post* last week — and a couple days ago, a front-page story in *The New York Times* reported the Obama administration is preparing to back it.

Why? Federal law enforcement agencies like the FBI have long feared their wiretap capabilities would begin "going dark" as criminals and terrorists — along with ordinary citizens — shift from telephone networks, which are required to be wiretap-ready under the 1994 Communications Assistance for Law Enforcement Act (CALEA), to the dizzying array of online communications platforms available today.

While it's not yet clear how dire the going-dark scenario really is, the statutory "cure" proposed by the FBI — with fines starting at $25,000 a day for companies that aren't wiretap capable — would surely be worse than the disease.

The FBI's misguided proposal would impose costly burdens on thousands of companies (and threaten to entirely kill those whose business model centers on providing highly secure encrypted communications), while making cloud solutions less attractive to businesses and users. It would aid totalitarian governments eager to spy on their citizens while distorting business decisions about software design. Perhaps worst of all, it would treat millions of law-abiding users with legitimate security needs as presumed criminals — while doing little to hamper *actual* criminals.

It Stifles Innovation

The FBI's plan would effectively make an entire category of emerging secure platforms — such as the encrypted voice app Silent Circle or the Dropbox-like cloud storage service Spider Oak — illegal overnight. Such services protect user confidentiality by ensuring that not even the company's employees can access sensitive data; only the end users retain the encryption keys needed to unlock their content.

This is hugely attractive for users who might otherwise be wary about relying on cloud services — whether they're businesses negotiating multi-million dollar mergers, lawyers and therapists handling confidential documents, activists in authoritarian states, or just couples looking to back up their newborn photos.

But if the FBI gets its way, companies won't be able to adopt that "end to end" encryption model, or offer their users the security it provides. A wiretap interface is essentially an *intentional* security vulnerability, as network engineer Susan Landau points out — which means requiring companies to be wiretap-capable is also mandating them to design less secure services.

That comes with a potentially large economic downside — and not just to cloud companies: If cloud providers can't promise iron-clad confidentiality, corporations may well keep operating their own outdated systems, even though shifting to a secure cloud solution would be more efficient and less expensive.

It's Tech-Ignorant

Typically, the FBI is claiming that they just want internet platforms to be subject to the same requirements as phone networks (which are familiarly accessible to them under CALEA).

But as a group of renowned computer scientists point out in an important new paper, "Going Bright: Wiretapping without Weakening Communications Infrastructure," this misleading analogy ignores key differences between the architectures of these networks.

For one, online platforms are altered and updated far more frequently than phone networks — and there are a hell of a lot more online services than there are phone carriers. That means an interception mandate imposes a greater burden on a larger number of much smaller firms.

It also means that as platforms evolve, the code firms deploy to provide wiretap functionality is bound to have vulnerabilities. This provides hackers with ample incentive to simultaneously compromise an entire user base — and the sweetly ironic prospect of doing so through a law enforcement interface would be irresistible to them.

More fundamentally, the internet is a *decentralized* packet-switched network that operates very differently from a centrally-switched phone network — and many types of online communication follow the same design principle. For example, video-chat services like Skype rely on a peer-to-peer design that doesn't require a centralized hub to route calls. Because it doesn't depend on a single company's servers to handle all the traffic, this architecture makes the service resilient and allows it to scale more easily — as well as more difficult for repressive regimes to block.

But the lack of a central hub also makes peer-to-peer communications inherently trickier to intercept. And threatening hefty fines for companies that can't reliably provide access to user communications could easily deter companies from choosing the approach, even when it makes the most sense on economic or engineering grounds.

Instead of being decided by what's best for the vast majority of users, communications architectures would be determined by what makes things easiest for law enforcement – essentially trading off the costs of the rare and tiny fraction of users who might be criminals with the the benefits of the many.

That's utterly at odds with the spirit of permissionless innovation that has made the internet such a spectacular engine of economic and cultural growth.

And Ironically, It Won't Really Protect Us

But if slowing innovation and weakening security is the price of catching terrorists and child pornographers, isn't it a price worth paying?

Not if it doesn't work.

Once it's clear that online companies can't promise true security, the most sophisticated and dangerous criminals will simply implement their own client-side encryption. DIY encryption may be too difficult or inconvenient for ordinary users, who benefit from services that take the hassle out of security — but the criminals the FBI is most interested in will doubtless find it worth the extra trouble.

As security researcher Matt Blaze and Susan Landau noted here in Wired, criminals, rival nation states, and rogue hackers routinely seek out and exploit vulnerabilities in our computers and networks … much faster than we can fix them. We don't need to add wiretapping interfaces as new and "particularly juicy" targets to this cybersecurity landscape.

What we need to do is urge the FBI to find other ways to gather the evidence it needs — approaches that don't indiscriminately compromise user security and online innovation. Instead of looking to Congress to add new vulnerabilities, the Bureau could focus on becoming better hackers of existing systems (for example, by exploiting bugs as backdoors).

In short, the FBI proposal is all cost for little to no benefit. The Obama administration needs to dump this ill-conceived scheme on the trash heap where it belongs.