Smartphone Users Are Paying Big Bucks for Their Own Surveillance

By Bill Blunden, Truthout | News Analysis

(Photo: Melissa BARRA)

In the movie *Sneakers*, a motley gang of security experts chase after a little black box that can crack any form of encryption. Though the idea of a digital skeleton key may seem like the stuff of Hollywood thrillers, there are researchers at the University of Michigan who've recently created just that. They've built a stealthy hardware back door that can be inserted into the blueprints of a computer chip to give intruders complete access to a system after executing an obscure series of commands.

Consider the implications: This kind of low-level attack is extremely difficult to detect and even more challenging to defend against. If a small group of university professors can successfully cook up their own little black box, imagine what an intelligence service with federal backing can do. William Binney, the National Security Agency's (NSA) former technical leader for intelligence, claims that with the NSA's budget of over $10 billion a year, "they have more resources to acquire your data than you can ever hope to defend against."

But it's not just the government that's watching us. IBM recently filed a patent for "monitoring individuals using distributed data sources," a stark reminder that much of what people do with their mobile devices is scooped up and stored in corporate data silos for later analysis. It's an inconvenient fact that Silicon Valley prefers to drown out with marketing pitches.

A Misplaced Faith in Markets

Thanks to whistleblower Edward Snowden, we know that NSA spies think of smartphone users as "zombies" who pay for their own surveillance. Hence, in the aftermath of the Snowden revelations, corporate leaders in Silicon Valley have focused intently on linking technical innovation with cybersecurity. It's an approach that aligns the average user's desire for better privacy with the business interests of large tech companies.

NSA spies think of smartphone users as "zombies" who pay for their own surveillance.

The basic narrative is fairly straightforward: To protect oneself against prying eyes, simply get the latest mobile gadget. Ostensibly, even the FBI will be hard-pressed to access its data. But how, exactly, is the public supposed to believe that clandestine agreements between intelligence directors and CEOs are strictly a thing of the past?

Glenn Greenwald asserts that market incentives will take care of this problem. In a recent interview, he explained that, "consumers are now demanding that privacy be safeguarded and refusing to use companies that won't do that."

Can market forces really save us? Those who recall what happened in 2008 have their doubts.

There is evidence that suggests that Greenwald's faith in Silicon Valley and the marketplace is misplaced.

The public record reveals that US intelligence services, with plenty of help from the tech industry, succeeded in making commercial products "exploitable" as part of "an aggressive, multi-pronged effort to break widely used internet encryption technologies." The campaign to secretly alter technology has been going on for a long time. For instance, more than two decades ago, an anonymous source in the CIA disclosed that spies were actively tampering with chips used in weapons systems bought by other countries.

The more adamantly vendors offer assurances about protection, the more skeptical people should become.

If the past is any guide, the more adamantly vendors offer assurances about protection, the more skeptical people should become. Recall how bold public displays of rebellion in the early 1990s were staged on behalf of shareholder value while the executives colluded secretly with spies behind closed doors.

There are reasons for this collusion. Major corporate players recognize the role that intelligence services play in terms of opening up markets and providing access to global resources. Extreme pressure can be placed on those who don't fall into line. World leaders who fall out of favor with the US establishment have sometimes been forced into "early retirement" by covert operations. Entire countries have been lit on fire through US-sponsored destabilization. US policy makers send an unspoken message conveyed through raw force: "Don't forget who owns all of those megaton nuclear intercontinental ballistic missiles."

Lower-Tech Devices Are More Secure

Genuine security is the result of a disciplined process. It arises from a set of policies and standards that are carefully implemented and maintained, not a gadget that's purchased off the shelf. Moreover, higher levels of security often entail sacrificing convenience and connectivity in the name of confidentiality. The Russian Federal Guard Service, for instance, has switched over to typewriters in light of the NSA's apparent mastery of computer espionage. German intelligence services have considered doing likewise.

There's definitely something to be said for old school methods. They worked just fine pre-internet and they can still work. In fact, old school tradecraft may turn out to be the Achilles heel for security services as they've become heavily reliant on signal intelligence to function.

It's a numbers game. Think about it: Gathering human intelligence is resource-intensive and introduces any number of additional risks. FBI agents have estimated that tailing a single suspect around the clock can require somewhere in the neighborhood of 30 to 40 operatives. For security services, this puts a modest upper bound on the number of 24x7 surveillance operations, something like a few dozen targets. Compounding this issue, taking away sources of data can rob spies of their signal intelligence advantage. It forces them to employ black bag groups like the CIA's Special Collection Service, which are so expensive that they're primarily focused on a tiny set of high priority targets.

Even if a phone call is encrypted, the very act of making a call provides a wealth of data to spies.

In this sense, non-smartphones can be viewed as superior to smartphones as they generate a smaller data footprint. Going a step further, a pager can be viewed as superior to a non-smartphone because communication on the user's end is further constrained, as well as not anchored to a particular phone line. Unfortunately, there are still effective countermeasures to be concerned about, like voice recognition software, radio tower spoofing (e.g. "stingrays") and the steady proliferation of telescreens throughout urban areas.

Even if a phone call is encrypted, the very act of making a call provides a wealth of data to spies. The metadata is the message, my friends. Some operators have responded by deploying small sets of phones that only call each other, establishing a closed circuit of cellphones. In the extreme case, there are only two phones talking to each other, a practice that's known as "mirroring." The downside of this approach is that it's conspicuous. Any intelligence agency sorting through aggregated phone records will easily spot a closed circuit and presumably take interest.

The threat of centralized monitoring explains why larger groups, which have access to the necessary resources, have gone out-of-band. They've developed their own dispersed communication networks built on top of their own dedicated physical infrastructure. Granted, while this strategy isn't perfect, it does drive up the cost of interception and analysis. For example, the Los Zetas cartel in Mexico developed an encrypted radio network. Likewise, the Hezbollah militia in Lebanon went so far as to set up its own fiber optic network that reached across the country.

Perhaps, in certain cases, the best solution is to follow the lead of Russian spymasters and simply opt out.

Given the NSA's widespread technical mastery, safeguarding oneself against surveillance may entail swallowing a bitter pill. One must face the prospect that technology is more often a tool of control rather than an antidote against surveillance, despite what the executives in Silicon Valley tell you. And perhaps, in certain cases, the best solution is to follow the lead of Russian spymasters and simply opt out.

Bill Blunden

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics and institutional analysis. He is the author of several books, including *The Rootkit Arsenal*, and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.

Related Stories

NSA Insiders Reveal What Went Wrong

By Veteran Intelligence Professionals for Sanity, Former NSA Senior Executives, Consortium News | Open Letter

NSA Creates Google-Like Search Engine to Help Other Agencies Access Collected Phone, Email Records

By Amy Goodman, Democracy Now! | Video Interview

NSA Documents Suggest a Close Working Relationship Between NSA, US Companies

By Julia Angwin, Jeff Larson, ProPublica | Report