

Are Google and Apple On Your Side?

Subverting Device Encryption? Let Me Count the Ways

By **Bill Blunden**, September 21, 2014

In the past couple of days both Google¹ and Apple² have announced that they're enabling default encryption on their mobile devices so that only the user possessing a device's password can access its local files. The public relations team at Apple makes the following claim:

"Apple cannot bypass your passcode and therefore cannot access this data... So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8"

The marketing drones at Google issued a similar talking point:

"For over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement... As part of our next Android release, encryption will be enabled by default out of the box, so you won't even have to think about turning it on."

Quite a sales pitch? Cleverly disguised as a news report no less. Though it's not stated outright the tacit message is: open your wallet for the latest gadget and you'll be safe from Big Brother. Sadly, to a large degree this perception of warrant protection is the product of Security Theater aimed at rubes and shareholders. The anti-surveillance narrative being dispensed neglects the myriad of ways in which such device-level encryption can be overcome. A list of such techniques has been enumerated by John Young, the architect who maintains the *Cryptome* leak site³. Young asks readers why he should trust hi-tech's sales pitch and subsequently presents a series of barbed responses. For example:

Because they can't covertly send your device [updated software \[malware\]](#) that would change all these promises, for a targeted individual, or on a mass basis?

Because this first release of their encryption software has [no security bugs](#), so you will never need to upgrade it to retain your privacy?

Because the US export control bureaucracy would never try to [stop Apple from selling secure mass market proprietary encryption](#) products across the border?

Because the countries that [wouldn't let Blackberry sell phones](#) that communicate securely with your own corporate servers, will of course let Apple sell whatever high security non-tappable devices it wants to?

Because they want to [help the terrorists win](#)?

Because it's always better to wiretap people after you [convince them that they are perfectly secure](#), so they'll spill all their best secrets?

Another thing to keep in mind is that local device encryption is just that. Local. As Bruce Schneier points out this tactic does little to protect user data that's stored in the cloud⁴. When push comes to shove executives will still be able to hand over anything that resides on corporate servers.

Marketing spokesmen are eager to create the impression that companies are siding with users in the struggle against mass surveillance (never mind the prolific corporate data mining⁵). Especially after business leaders denied participating in the NSA's PRISM program. Yet the appearance of standing up to government surveillance is often a clever ploy to sell you stuff, a branding mechanism. It's important to recognize that Internet companies, especially billion dollar hi-tech multinationals like Yahoo⁶ and Cisco⁷, exist to generate revenue and have clearly demonstrated the tendency to choose profits over human rights when it's expedient.

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.

End Notes

¹ Craig Timberg, "[Newest Androids will join iPhones in offering default encryption, blocking police](#)," *Washington Post*, September 18, 2014.

² Craig Timberg, "[Apple will no longer unlock most iPhones, iPads for police, even with search warrants](#)," *Washington Post*, September 18, 2014.

³ John Young, "[Apple Wiretap Disbelief](#)," *Cryptome*, September 19, 2014.

⁴ Bruce Schneier, "[iOS 8 Security](#)," *Schneier on Security*, September 19, 2014.

⁵ Bill Blunden, "[The NSA's Corporate Collaborators](#)," *Counterpunch*, May 9-11, 2014.

⁶ Bill Blunden, "[Yahoo's Innocent Victim Narrative](#)," *Dissident Voice*, September 12, 2014.

⁷ Cindy Cohn and Rainey Reitman, "[Court Lets Cisco Systems Off the Hook for Helping China Detain, Torture Religious Minorities](#)," *Electronic Frontier Foundation*, September 19, 2014.