STUPID SMARTPHONES AND THEIR LYING LIES

[Apple iPhone 5c via TheVerge.com]

If you value emptywheel's insights, donate the equivalent of a couple beers—and thanks for your readership and support.

My Twitter timelines across multiple accounts are buzzing with Apple iPhone 5s announcement news. Pardon me if I can't get excited about the marvel that is iPhone's new fingerprint-based biometric security.

Let's reset all the hype:

There is no smartphone security available on the market we can trust absolutely to keep out the National Security Agency. No password or biometric security can assure the encryption contained in today's smartphones as long as they are built on current National Institute of Standards and Technology (NIST) standards and/or the Trusted Computing Platform. The NSA has compromised these standards and TCP in several ways, weakening their effectiveness and ultimately allowing a backdoor through them for NSA use, bypassing any superficial security system.

There is nothing keeping the NSA from sharing

whatever information they are gleaning from smartphones with other government agencies. Citizens may believe that information gleaned by the NSA ostensibly for counterterrorism may not be legally shared with other government agencies, but legality/illegality of such sharing does not mean it hasn't and isn't done. (Remember fusion centers, where government agencies were supposed to be able to share antiterrorism information? Perhaps these are merely window dressing on much broader sharing.)

There is no exception across the best known mobile operating systems to the vulnerability of smartphones to NSA's domestic spying. Although Der Spiegel's recent article specifically calls out iOS, Android, and Blackberry smartphones, Windows mobile OS is just as exposed. Think about it: if your desktop, laptop, and your netbook are all running the same Windows OS versions needing patches every month to fix vulnerabilities, the smartphone is equally wide open as these devices all use the same underlying code, and hardware built to the same NIST standards. Additionally, all Windows OS will contain the same Microsoft CryptoAPI believed to be weakened by the NSA.

If any of the smartphone manufacturers selling into the U.S. market say they are secure against NSA domestic spying, ask them to prove it. Go ahead and demand it – though it's sure to be an exercise in futility. These firms will likely offer some non-denial denials and sputtering in place of a firm, "Yes, here's proof" with a validated demonstration.

Oh, and the Touch ID fingerprint biometrics Apple announced today? You might think it protects not against the NSA but the crook on the street. But until Apple demonstrates they pass a gummy bear hackability test, don't believe them.

And watch for smartphone thieves carrying tin snips.