Swampland

MUST READS

Five Revelations from Snowden's Newest Leak

New report reveals how the NSA has been able to crack online encryption. "This is the golden age of spying," says one former analyst

By Denver Nicks @DenverNicks | Sept. 05, 2013 | 23 Comments

NSA / Reuters

The National Security Agency headquarters building in Fort Meade, Md.

A new round of disclosures from the former National Security Agency contractor Edward Snowden has revealed the intelligence agency's ultimate goal: undo Internet privacy as we know it. According to some 50,000 leaked documents provided to the *Guardian*, *ProPublica*, and *The New York Times*, the NSA has circumvented or cracked some of the most widely used encryption software in its effort to monitor global communications. Still, documents reveal, some encryption systems continue to stymie the agency, and the NSA, according to the *Times*, is working toward a future in which it can “decode, in real time, all of the information flying over the world’s fiber optic cables and through its Internet hubs.”

The document dump unveils some of the U.S. and its allies’ most closely guarded state secrets—whereas highly classified information is often disseminated on a “need to know” basis, “there will be NO ‘need to know,’” with respect to the highly-classified program known as Bullrun, according to one document quoted by the *Times*.

“This is the golden age of spying,” one former NSA analyst told the *Times*. Here are five things you need to know about Snowden’s latest leak.

1. Often the NSA circumvents encryption by simply collaborating with cooperative technology companies (which are unidentified in the documents). At other times, it seems, the NSA has acquired encryption keys by hacking into a company’s servers. The documents indicate that the NSA is careful to reveal decrypted messages to other agencies only when such communications could plausibly have been acquired legally.
2. By 2006, according to *The New York Times*, the NSA had cracked the communications of three foreign airlines, one travel reservation system, one foreign government’s nuclear department and a different foreign government’s Internet service. By 2010, the British GCHQ (the UK’s counterpart to the NSA) was reportedly deciphering encrypted VPN communications “for 30 targets and had set a goal of an additional 300.” According to the leaked documents, by 2012 the GCHQ had acquired “new access opportunities” into Google’s systems.
3. The full extent of the NSA’s highly classified encryption cracking program Bullrun is only known by top officials in the NSA and its counterpart agencies in Britain, Canada, Australia and New Zealand. Bullrun has successfully foiled several of the world’s standard encryption methods, including SSL (Secure Sockets Layer), VPN (virtual private networks), and the encryption on 4G (fourth generation) smartphones.
4. Strong, non-commercial encryption systems still seem to thwart the NSA’s efforts. The PGP (short for Pretty Good Privacy) encryption protocol, for instance, has been a cause for NSA anxiety for decades. When PGP-inventor Phil Zimmerman announced the Zfone telephone encryption technology, NSA analysts reportedly received the news in an email titled “This can’t be good.”
5. The NSA requested that The New York Times not publish its article describing the agency’s effectiveness in thwarting encryption methods, arguing that its success relies entirely on its ability to operate stealthily. Language in the documents themselves seems to echo this position. “These capabilities are among the Sigint [Signals Intelligence] community’s most fragile,” reads one document, according to the *Times, “*and the inadvertent disclosure of the simple ‘fact of’ could alert the adversary and result in immediate loss of the capability.” Some experts argue, however, that the NSA’s effort to monitor communications by cracking encryption methods may be undermining its other primary purpose: protecting the security of American communications. Many of the protocols it has cracked are the very things Americans use every day for activities like online banking and sending private emails under the assumption that the encryption is secure. “Those back doors could work against U.S. communications, too,” one academic told the *Times*.

[The New York Times]