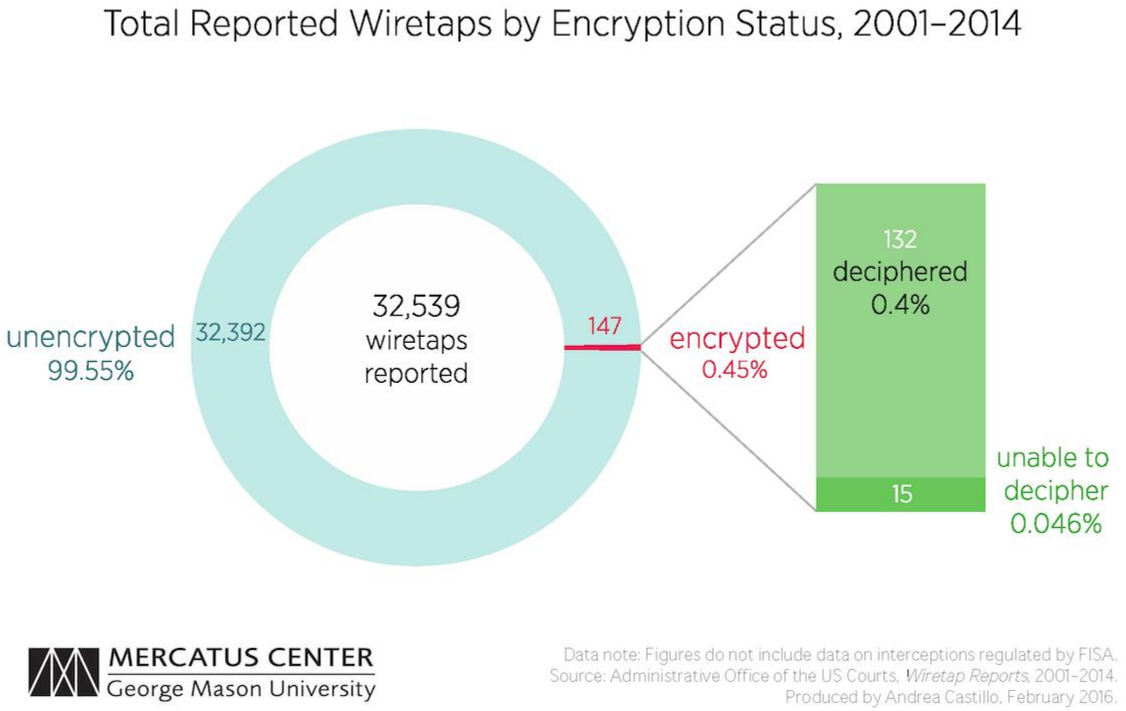
Going Dark? Federal Wiretap Data Show Scant Encryption Problems

Andrea Castillo, Eli Dourado | Feb 26, 2016

The recent conflict between the Department of Justice and Apple over retrieving data from a locked iPhone has revived the debate over encryption and security in the United States. FBI Director James Comey argues that strong encryption techniques for secure communications and computing allow criminals to evade law enforcement by "going dark."

To overcome this purported problem, leaders in policy and law enforcement have called for new laws that would compel technology companies to build so-called "backdoors" into secure protocols for government access. However, few have considered the relevant empirical data required to perform a proper benefit-cost analysis.

These charts use data from the annual *Wiretap Reports* published by the Administrative Office of the US Courts to display the portion of total reported wiretap orders that have been undermined by encryption technologies from 2001 to 2014. (This dataset only examines domestic wiretap requests. Information relating to wiretap requests regulated by the Foreign Intelligence Surveillance Act of 1978 is not available.) The charts show that, contrary to popular assumption, encryption technologies have only complicated a minuscule percentage of reported wiretap investigations in recent years.



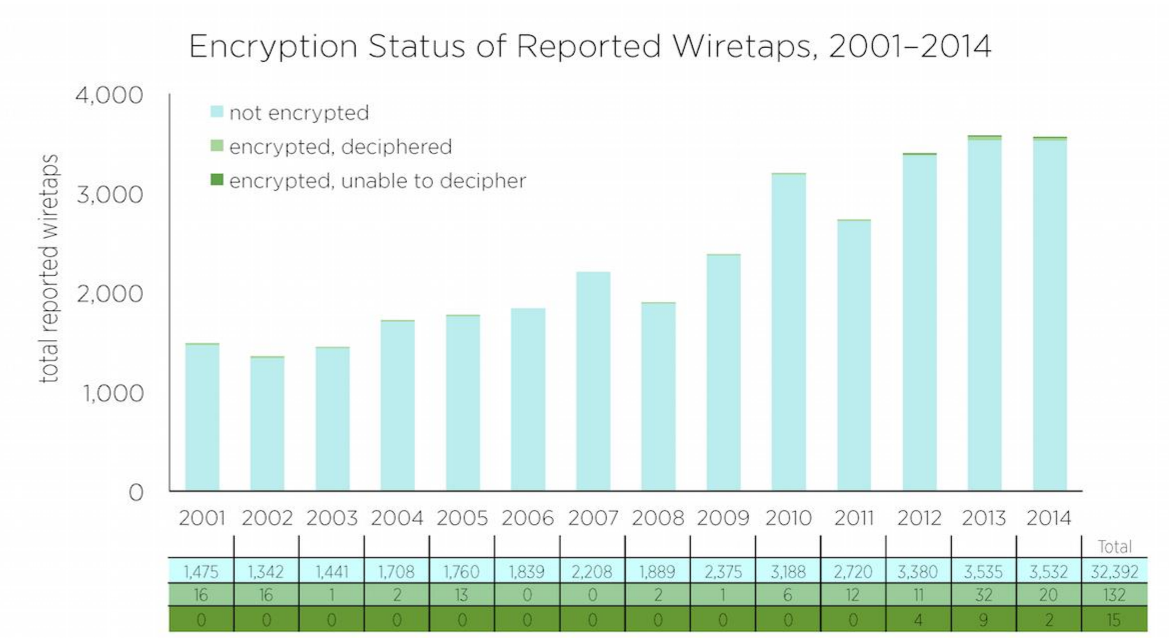
Total Reported Wiretaps by Encryption Status, 2001–2014

Data note: Figures do not include data on interceptions regulated by FISA.
Source: Administrative Office of the US Courts, *Wiretap Reports*, 2001–2014.
Produced by Andrea Castillo, February 2016.

The first chart breaks down the total reported wiretap orders from 2001 to 2014 by whether or not the target employed encryption techniques. Targets of wiretap orders that did not use encryption are displayed in light blue, while those that did employ encryption techniques are displayed in red. Encrypted communications are further broken down by whether or not investigators could decipher the encrypted communications in the bar to the right. Deciphered encrypted communications are displayed in light green, while encrypted communications that could not be deciphered are displayed in dark green.

Of the 32,539 total wiretap orders reported from 2001 to 2014, only 147, or 0.45 percent, involved encryption techniques. Law enforcement agents executed the remaining 32,392 wiretap orders without any problems related to encryption. Additionally, most of the 147 orders that were complicated by encryption were ultimately deciphered by law enforcement. Only 15 wiretap orders, or 0.046 percent of the total, employed secure encryption techniques that law enforcement officials were unable to decipher.

Encryption Status of Reported Wiretaps, 2001–2014



2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	Total
1,475	1,342	1,441	1,708	1,760	1,839	2,208	1,889	2,375	3,188	2,720	3,380	3,535	3,532	32,392
16	16	1	2	13	0	0	2	1	6	12	11	32	20	132
0	0	0	0	0	0	0	0	0	0	0	4	9	2	15

MERCATUS CENTER
George Mason University

Data note: Figures do not include data on interceptions regulated by FISA.
Source: Administrative Office of the US Courts, *Wiretap Reports*, 2001–2014.
Produced by Andrea Castillo, February 2016.

The second chart displays this same data in a time series stacked bar graph. The chart shows that law enforcement agents were able to decipher the few encrypted communications intercepted through a court wiretap warrant for over a decade. It was not until 2012 that law enforcement officials encountered encrypted communications that they were unable to decipher. Four such incidents occurred that year, followed by nine in 2013, and only two in 2014.

These charts suggest that, contrary to some claims from the law enforcement community, “going dark” is an insignificant obstacle for most domestic criminal investigations. Only around 0.046 percent of all reported domestic wiretap orders since 2001 have encountered any communications that were encrypted and unable to be deciphered. Furthermore, it is unclear that these few complications singly undermined the connected investigations. It is possible that law enforcement officials had sufficient evidence to convict even without this information.

Policymakers considering this issue must weigh the benefits and costs of compromising the protections that come with encryption technologies. Do the seemingly negligible benefits for law enforcement outweigh the costs associated with the considerable vulnerabilities to Internet security that these policies would introduce? For example, many computer security experts warn that malicious hackers or foreign governments can exploit the “backdoors” or “golden keys” that some policymakers have proposed for government access into secure technologies.
Given that only a minuscule portion of investigations suffer from undecipherable encrypted communications, it is likely that criminal investigations can better be aided by targeting other more significant barriers that officers face or by further improving on law enforcement’s existing strengths.