**Update 9/26/14:** Recently Apple has [announced](https://www.apple.com/privacy/government-information-requests/) that it is providing basic encryption on mobile devices that they cannot bypass, even in response to a request from law enforcement. Google has promised to take similar steps in the near future. Predictably, law enforcement has responded with [howls of alarm](http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-3-where-do-you-draw-the-line-and-whats-the-privacy-tradeoff/).

We've seen this movie before. Below is a slightly adapted blog post from one we posted in 2010, the last time the FBI was seriously hinting that it was going to try to mandate that all communications systems be easily wiretappable by mandating "back doors" into any encryption systems. We marshaled eight "epic failures" of regulating crypto at that time, all of which are still salient today. And in honor of the current debate, we've added a ninth.

*They can promise strong encryption. They just need to figure out how they can provide us plain text.* - FBI General Counsel Valerie Caproni, September 27, 2010

*[W]e're in favor of strong encryption, robust encryption. The country needs it, industry needs it. We just want to make sure we have a trap door and key under some judge's authority where we can get there if somebody is planning a crime.* - FBI Director Louis Freeh, May 11, 1995

If the government howls of protest at the idea that people will be using encryption sound familiar, it's because regulating and controlling consumer use of encryption was a monstrous proposal officially [declared dead](https://secure.wikimedia.org/wikipedia/en/wiki/Crypto:_How_the_Code_Rebels_Beat_the_Government%E2%80%94Saving_Privacy_in_the_Digital_Age) in 2001 after threatening Americans' privacy, free speech rights, and innovation for nearly a decade. But like a zombie, it's now rising from the grave, bringing the same disastrous flaws with it.

For those who weren't following digital civil liberties issues in 1995, or for those who have forgotten, here's a refresher list of why forcing companies to break their own privacy and security measures by installing a back door was a bad idea 15 years ago:

1. **It will create security risks.** Don't take our word for it. Computer security expert Steven Bellovin [has explained](http://www.cs.columbia.edu/~smb/blog/2010-10/2010-10-16.html) some of the problems. First, it's hard to secure communications properly even between two parties. Cryptography with a back door adds a third party, requiring a more complex protocol, and as Bellovin puts it: "Many previous attempts to add such features have resulted in new, easily exploited security flaws rather than better law enforcement access." It doesn't end there. Bellovin notes:

Complexity in the protocols isn't the only problem; protocols require computer programs to implement them, and more complex code generally creates more exploitable bugs. In the most notorious incident of this type, a cell phone switch in Greece was hacked by an unknown party. The so-called 'lawful intercept' mechanisms in the switch — that is, the features designed to permit the police to wiretap calls easily — was abused by the attacker to monitor at least a hundred cell phones, up to and including the prime minister's. This attack would not have been possible if the vendor hadn't written the lawful intercept code.

More recently, as security researcher Susan Landau [explains](http://www.huffingtonpost.com/susan-landau/moving-rapidly-backwards-_b_760667.html), "an IBM researcher found that a Cisco wiretapping architecture designed to accommodate law-enforcement requirements — a system already in use by major carriers — had numerous [security holes](http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html#Cross) in its design. This would have made it easy to break into the communications network and surreptitiously wiretap private communications."

The same is true for Google, which had [its "compliance" technologies hacked by China](http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html).

This isn't just a problem for you and me and millions of companies that need secure communications. What will the government itself use for secure communications? The FBI and other government agencies currently use many commercial products — the same ones they want to force to have a back door. How will the FBI stop people from un-backdooring their deployments? Or does the government plan to stop using commercial communications technologies altogether?

1. **It won't stop the bad guys.** Users who want strong encryption will be able to get it — from Germany, Finland, Israel, and many other places in the world where it's offered for sale and for free. In 1996, the National Research Council did a study called ["Cryptography's Role in Securing the Information Society,"](http://www.nap.edu/openbook.php?record_id=5131) nicknamed CRISIS. Here's what they said:

Products using unescrowed encryption are in use today by millions of users, and such products are available from many difficult-to-censor Internet sites abroad. Users could pre-encrypt their data, using whatever means were available, before their data were accepted by an escrowed encryption device or system. Users could store their data on remote computers, accessible through the click of a mouse but otherwise unknown to anyone but the data owner, such practices could occur quite legally even with a ban on the use of unescrowed encryption. Knowledge of strong encryption techniques is available from official U.S. government publications and other sources worldwide, and experts understanding how to use such knowledge might well be in high demand from criminal elements. — CRISIS Report at 303

None of that has changed. And of course, more encryption technology is more readily available today than it was in 1996. So unless the goverment wants to mandate that you are forbidden to run anything that is not U.S. government approved on your devices,  they won't stop bad guys from getting  access to strong encryption.

1. **It will harm innovation.** In order to ensure that no "untappable" technology exists, we'll likely see a technology mandate and a draconian regulatory framework. The implications of this for America's leadership in innovation are dire. Could Mark Zuckerberg have built Facebook in his dorm room if he'd had to build in surveillance capabilities before launch in order to avoid government fines? Would Skype have ever happened if it had been forced to include an artificial bottleneck to allow government easy access to all of your peer-to-peer communications? This has especially serious implications for the open source community and small innovators. Some open source developers have [already taken a stand](http://tahoe-lafs.org/pipermail/tahoe-dev/2010-October/005353.html) against building back doors into software.
2. **It will harm US business.** If, thanks to this proposal, US businesses cannot innovate and cannot offer truly secure products, we're just handing business over to foreign companies who don't have such limitations. Nokia, Siemens, and Ericsson would all be happy to take a heaping share of the communications technology business from US companies. And it's not just telecom carriers and VOIP providers at risk. Many game consoles that people can use to play over the Internet, such as the Xbox, allow gamers to chat with each other while they play. They'd have to be tappable, too.
3. **It will cost consumers.** Any additional mandates on service providers will require them to spend millions of dollars making their technologies compliant with the new rules. And there's no real question about who will foot the bill: the providers will pass those costs onto their customers. (And of course, if the government were to pay for it, they would be using taxpayer dollars.)
4. **It will be unconstitutional.** Of course, we wouldn't be EFF if we didn't point out the myriad constitutional problems. The details of how a cryptography regulation or mandate will be unconstitutional may vary, but there are serious problems with nearly every iteration of a "no encryption allowed" proposal that we've seen so far. Some likely problems:
   * The First Amendment would likely be [violated](http://osaka.law.miami.edu/~froomkin/articles/clipper.htm) by a ban on all fully encrypted speech.
   * The First Amendment would likely not allow a ban of any software that can allow untappable secrecy. Software is speech, after all, and this is one of the key ways [we defeated this bad idea last time](http://www.eff.org/cases/bernstein-v-us-dept-justice).
   * The Fourth Amendment would not allow requiring disclosure of a key to the backdoor into our houses so the government can read our "papers" in advance of a showing of probable cause, and our digital communications shouldn't be treated any differently.
   * The Fifth Amendment would be implicated by required disclosure of a private papers and the forced utterance of incriminating testimony.
   * Right to privacy. Both the right to be left alone and informational privacy rights would be implicated.
5. **It will be a huge outlay of tax dollars.** As noted below, wiretapping is still a relatively rare tool of government (at least for the FBI in domestic investigations -- the NSA is another matter as we now all know). Yet the extra tax dollars needed to create a huge regulatory infrastructure staffed with government bureaucrats who can enforce the mandates will be very high. So, the taxpayers would end up paying for more expensive technology, higher taxes, and lost privacy, all for the relatively rare chance that motivated criminals will act "in the clear" by not using encryption readily available from a German or Israeli company or for free online.
6. **The government hasn't shown that encryption is a problem.** How many investigations have been thwarted or significantly harmed by encryption that could not be broken? In 2009, the government reported only one instance of encryption that they needed to break out of 2,376 court-approved wiretaps, and it ultimately [didn't prevent investigators from obtaining the communications they were after](http://www.wired.com/threatlevel/2010/09/fbi-backdoors/).This truth was made manifest in a recent [Washington Post](http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/) article written by an ex-FBI agent. While he came up with a scary kidnapping story to start his screed, device encryption simply had nothing to do with the investigation.  The case involved an ordinary wiretap. In 2010, the New York Times reported that the government officials pushing for this have only come up with a few examples (and it's not clear that all of the examples actually involve encryption) and no real facts that would allow independent investigation or confirmation. More examples will undoubtedly surface in the FBI's PR campaign, but we'll be watching closely to see if underneath all the scary hype there's actually a real problem demanding this expensive, intrusive solution.
7. **Mobile devices are just catching up with laptops and other devices.**Disk encryption just isn't that new. Laptops and desktop computers have long had disk encryption features that the manufacturers have absolutely no way to unlock. Even for simple screen locks with a user password, the device maker or software developer doesn't automatically know your password or have a way to bypass it or unlock the screen remotely. Although many law enforcement folks don't really like disk encryption on laptops and have never really liked it, and we understand that some lobbied against it in private, we haven't typically heard them suggest in public that it was somehow improper for these vendors not to have a backdoor to their security measures. That makes us think that the difference here is really just that some law enforcement folks think that phones are just too popular and too useful to have strong security. But strong security is something we all should have. The idea that basic data security is just a niche product and that ordinary people don't deserve it is, frankly, insulting.  Ordinary people deserve security just as much as elite hackers, sophisticated criminals, cops and government agents, all of whom have ready access to locks for their data.

The real issue with encryption may simply be that the FBI has to use more resources when they encounter it than when they don't. Indeed, Bellovin argues: "Time has also shown that the government has almost always managed to go around encryption." (One circumvention that's worked before: [keyloggers](http://news.cnet.com/8301-10784_3-9741357-7.html).) But if the FBI's burden is the real issue here, then the words of the CRISIS Report are even truer today than they were in 1996:

It is true that the spread of encryption technologies will add to the burden of those in government who are charged with carrying out certain law enforcement and intelligence activities. But the many benefits to society of widespread commercial and private use of cryptography outweigh the disadvantages.

The mere fact that law enforcement's job may become a bit more difficult is not a sufficient reason for undermining the privacy and security of hundreds of millions of innocent people around the world who will be helped by mobile disk encryption. Or as Chief Justice of John Roberts [recently observed](http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf)in another case rejecting law enforcement's broad demands for access to the information available on our mobile phones:   "Privacy comes at a cost."