September 21, 2013
Close the N.S.A.'s Back Doors
By THE EDITORIAL BOARD

In 2006, a federal agency, the National Institute of Standards and Technology, helped build an international encryption system to help countries and industries fend off computer hacking and theft. Unbeknown to the many users of the system, a different government arm, the National Security Agency, secretly inserted a "back door" into the system that allowed federal spies to crack open any data that was encoded using its technology.

Documents leaked by Edward Snowden, the former N.S.A. contractor, make clear that the agency has never met an encryption system that it has not tried to penetrate. And it frequently tries to take the easy way out. Because modern cryptography can be so hard to break, even using the brute force of the agency's powerful supercomputers, the agency prefers to collaborate with big software companies and cipher authors, getting hidden access built right into their systems.

The New York Times, The Guardian and ProPublica recently reported that the agency now has access to the codes that protect commerce and banking systems, trade secrets and medical records, and everyone's e-mail and Internet chat messages, including virtual private networks. In some cases, the agency pressured companies to give it access; as The Guardian reported earlier this year, Microsoft provided access to Hotmail, Outlook.com, SkyDrive and Skype. According to some of the Snowden documents given to Der Spiegel, the N.S.A. also has access to the encryption protecting data on iPhones, Android and BlackBerry phones.

These back doors and special access routes are a terrible idea, another example of the intelligence community's overreach. Companies and individuals are increasingly putting their most confidential data on cloud storage services, and need to rely on assurances their data will be secure. Knowing that encryption has been deliberately weakened will undermine confidence in these systems and interfere with commerce.

The back doors also strip away the expectations of privacy that individuals, businesses and governments have in ordinary communications. If back doors are built into systems by the N.S.A., who is to say that other countries' spy agencies — or hackers, pirates and terrorists — won't discover and exploit them?

The government can get a warrant and break into the communications or data of any individual or company suspected of breaking the law. But crippling everyone's ability to use encryption is going too far, just as the N.S.A. has exceeded its boundaries in collecting everyone's phone records rather than limiting its focus to actual suspects.

Representative Rush Holt, Democrat of New Jersey, has introduced a bill that would, among other provisions, bar the government from requiring software makers to insert built-in ways to bypass encryption. It deserves full Congressional support. In the meantime, several Internet companies, including Google and Facebook, are building encryption systems that will be much more difficult for the N.S.A. to penetrate, forced to assure their customers that they are not a secret partner with the dark side of their own government.