THE WALL STREET JOURNAL.

http://www.wsj.com/articles/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474

BUSINESS (HTTP://WWW.WSJ.COM/NEWS/BUSINESS) | LEADERSHIP (HTTP://WWW.WSJ.COM/NEWS/TYPES/JOURNAL-REPORTS-LEADERSHIP)

Should Law Enforcement Have the Ability to Access Encrypted Communications?

Growing encryption heightens the debate over online privacy and law enforcement

PHOTO: THOMAS TRUTSCHEL/GETTY IMAGES

April 19, 2015 11:11 p.m. ET

People's distress over the privacy of their communications has never been more acute. Whether the fear is over U.S. surveillance or breaches by hackers of unknown origins, many consumers fear that there is no such thing as privacy online.

Such concerns have created a market for products with ever-greater encryption. Apple Inc. claims that its latest mobile devices feature encryption that no one, not even Apple itself, has the ability to decipher. The devices use codes that are freshly generated with each message.

This is a

THE FBI WEIGHS IN ON THE DEBATE

- **The FBI's Stance on Encrypted Communications** (http://blogs.wsj.com/experts/2015/04/20/the-fbis-stance-on-encrypted-communications/)

concern to U.S. law-enforcement and security forces, who say the producers of highly encrypted communication devices must make available to them—within the framework of the law—a way to decipher those messages. They argue they need access to private emails, social-media messages and other electronic communications to foil terrorist plots and keep U.S. citizens safe.

But the issue is of equal concern to defenders of civil liberties, who fear that as the government keeps extending its ability to monitor private communications, there will soon be no right to privacy left.

Arguing for the government's right, within the purview of the courts, to decipher and monitor private communications is Carrie Cordero, a former counsel in the Justice Department's national security division and director of national security studies at Georgetown Law. Defending the right of private citizens to communicate without government interference is Marc Zwillinger, a private attorney in Washington, D.C.

YES: We Need That Ability to Fight Terrorism

By Carrie Cordero

We can't fight terrorism and violent crime in the dark. But that is where we're headed if law-enforcement and intelligence officials are denied the legal access they need.

The fact is, communications companies often hold information that law-enforcement and national-security agencies require to pursue criminal investigations and forestall potential threats. Up until recently, agents of the government could generally file requests for court orders that, if approved, compel the companies to provide the requested information. Congress in the 1990s passed the Communications Assistance for Law Enforcement Act, or Calea, to facilitate private-sector cooperation with law enforcement. This act required telecommunications companies to configure their systems in a way that would enable them to effectively respond to court orders.

But Calea predated email, cloud storage and social-media platforms. Officials now have to cope with situations and technologies that the law did not anticipate. Moreover, recent congressional proposals, such as the Secure Data Act, threaten to prohibit the government from requiring that companies design or modify communications systems or products to facilitate government requests for data.

Justice denied?

Driven by increased concerns about government surveillance and consumer privacy,

the

JOURNAL REPORT

- Insights from The Experts (http://blogs.wsj.com/experts/category/leadership/?mod=experts_leadership)
- Read more at WSJ.com/LeadershipReport (http://online.wsj.com/public/page/journal-report-leadership.html?mg=inert-wsj)

MORE IN INFORMATION SECURITY

- Five Simple Things Companies Should Do to Protect Their Computer Systems (http://www.wsj.com/articles/five-simple-steps-to-protect-corporate-data-1429499477)
- Consumers' Weakest Online Security Link: Their Children (http://www.wsj.com/articles/your-weakest-security-link-your-children-1429499471)
- How to Get People to Take Computer Security More Seriously (http://www.wsj.com/articles/make-me-change-my-password-please-1429499482)
- Encryption Uncoded: A Consumers' Guide (http://www.wsj.com/articles/encryption-uncoded-a-consumers-guide-1429499476)
- Take Our Quiz on Data Privacy (http://www.wsj.com/articles/how-much-do-you-know-about-data-privacy-1429499471)

technology industry has accelerated the deployment of advanced encryption technology for consumers and businesses. Apple Chief Executive Tim Cook has said that his company won't even be able to comply with court subpoenas involving its iMessage service because the encryption is undecipherable by Apple itself.

Therein lies the problem. If companies can't decode messages or retain a means to unlock devices of their customers, court orders requiring the companies to hand over messages, passwords or keys will be meaningless. An alternative suggested by some that courts compel suspects to hand over their devices and passwords is not realistic, considering the types of crimes and threats the U.S. government is most worried about. As a result, a violent crime may go unsolved; a terrorist attack may not be thwarted; a victim may not see justice.

It's true that encryption wasn't on the table when Calea was passed in 1994. But it wasn't widely available to consumers then. Today, with some companies installing unbreakable codes on their devices by default, a way for law enforcement to gain access must be on the table.

Weighing the risks

To resolve this stalemate, society will need to weigh two risks: the potential risk of having some degree of vulnerability in the design of modern communications, and the

danger of failing to provide citizens with basic levels of protection and security.

Critics point out that the existence of some kind of a key entails a risk that the key will be exploited. Is that truly worse than the risk of creating a virtual law-enforcement-free zone that protects criminal activity? The Supreme Court has said that a search warrant is "an important working part of our machinery of government."

Requests for access by foreign governments will be one of the hardest issues to work through. Companies will face pressures from abroad, and will need to evaluate market opportunities in the context of trying to work with governments that have poor human-rights records. On the other hand, even those governments might have a legitimate need to access encrypted communications in order to investigate a violent crime, for example. The issues for each country, and each situation, will be different.

There must be a path forward that will enable law enforcement to do its job, while protecting our companies' freedom to innovate and our neighbors' freedom to communicate with reasonable security. How to get there will involve government and industry collaboration involving technical solutions, legislative creativity and compromise.

Ms. Cordero, a former counsel in the Justice Department's national-security division, is an attorney in private practice and the director of national-security studies at Georgetown Law. She can be reached at reports@wsj.com .

NO: It Violates Our Rights—Without Improving Security

By Marc Zwillinger

The U.S. government certainly has a compelling interest in protecting its citizens from crime, terrorist attacks and foreign threats. But this goal doesn't justify the use of any and all means.

Some methods of intelligence gathering aren't compatible with our nation's values, and aren't demonstrably effective over the long term. The government's desire to require Internet companies that provide encrypted communications to build a mechanism for law-enforcement access into all of their products is an example of such a shortsighted demand.

Secure communications are paramount to modern society. Vulnerability in their design could regularly expose physical, financial and emotional details of our lives, and our companies' most valuable trade secrets. Overseas, it could endanger the lives of critics

of oppressive governments, people who seek to exercise the same freedoms of expression and association that the U.S. supports through human-rights efforts around the world.

Devastating effects

The government claims it will use its golden key only when proper judicial process has been followed. It also contends that requiring access to encrypted Internet communications is a necessary update to the existing Communications Assistance for Law Enforcement Act, or Calea, which back in 1994 required telecommunications carriers to have interception capabilities.

These arguments have some simplistic appeal, but giving the government a decryption key would result in devastating effects.

First, multinational companies will not be able to refuse foreign governments that demand access. Governments could threaten financial sanctions, asset seizures, imprisonment of employees and prohibition against a company's services in their countries. Consider China, where U.S. companies must comply with government demands in order to do business. A related point: Nothing would stop companies in other countries from making fully secure, end-to-end encryption products. This harms both U.S. industry and national security.

Second, exploitation of the U.S. government's key by hackers will be a significant risk. Indeed, hackers accessed law-enforcement surveillance information during the state-sponsored hack of Google in 2010.

Third, the U.S. telephone network and the global Internet are not the same. Previously, telecom regulation could be accomplished domestically without opening the door for foreign government demands. Moreover, when Calea was passed, carriers weren't responsible for decrypting communications unless the carrier possessed the decryption key. In fact, Calea's legislative history is full of assurances that the Department of Justice and FBI had no intention to require providers to decrypt communications for which they did not have the key.

A bad trade-off

The truth is, law enforcement is not at risk of operating in the dark. It is living in the golden age of surveillance. And investigators will only have more and more potential data points as the trend toward smart homes, wearable devices and connected cars

increases. There are plenty of investigative options that won't compromise the security of entire communications networks. For instance, law enforcement can, in certain circumstances, compel passcodes from device owners. These are better alternatives than converting devices and apps into components of the surveillance apparatus.

The government does not have an absolute right to gain access to every way in which people communicate. The First Amendment protects our right to engage in speech, including, in some cases, anonymously. The fact that the Constitution offers a process for obtaining a search warrant does not mean it should therefore be illegal to make an unbreakable lock or use an unbreakable code. These are two distinct concepts.

There is no guarantee that impairing secure communications will solve the terrorist problem. What's more, a communications back door threatens to undermine basic human rights. Weakening security for the vast majority of users in order to gain access to the potentially illegal communications of the few is not the right trade-off.

Mr. Zwillinger is an attorney and founder and managing member of the Washington, D.C., law firm ZwillGen PLLC. He can be reached at reports@wsj.com .