New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 261—NO. 112
WEDNESDAY, JUNE 12, 2019

WHITE-COLLAR CRIME

Expert Analysis

The International Encryption Debate: Privacy Versus Big Brother

By **Robert J. Anello**

And **Richard F. Albert**

Many governments, including the United States, are attempting to restrict the use of encryption services like WhatsApp and Snapchat to allow for a greater opportunity for surveillance. Although increased reliance on technology such as emails and texts has provided greater opportunity to gather evidence of criminal activity, in part because many communications are now memorialized forever, law enforcement agencies around the world complain that encryption technologies make it difficult to catch criminals and terrorists and therefore should be restricted.

Turning the traditional concept of privacy on its head, governments appear to be positing that the totality of every individual's digital communications should be left open for scrutiny by government investigators in case some come to be suspected of wrongdoing at a later time. Not surprisingly, this Big-Brother-is-watching approach has met with resistance from public rights and civil liberty activists.

ROBERT J. ANELLO *and* RICHARD F. ALBERT *are partners at Morvillo Abramowitz Grand Iason & Anello.* GRETCHAN R. OHLIG, *an attorney, assisted in the preparation of this article.*

Before the technology explosion, two individuals desiring a private conversation might have opted for a phone call, secure in the expectation that the information shared during the call was not subject to eternal preservation. Indeed, such privacy generally is perceived as a human right. A detailed and extensive body of wiretap statutes and case law in the United States, arising from Fourth Amendment protections against unreasonable searches, insures that telephone conversations remain private absent evidence of probable cause that the subject individuals are actively involved in criminal mischief and issuance of a warrant by a court. The shift from oral conversation to digital communications should not change these fundamental privacy protections and assumptions.

> Governments across the globe have been struggling with how to balance law enforcement needs with the privacy arguments posed by civil liberty advocates. In many foreign countries, particularly those with totalitarian or potentially oppressive governments, encryption of daily communications by most people is common.

International response to the increased reliance on encrypted technologies has varied. Across the globe, in democratic and non-democratic countries alike, the questions being debated are similar—whether encryption should be allowed and, if so, whether law enforcement can mandate telecommunication companies that provide such encryption services also decrypt the communications (a particularly poignant question in countries where individuals lawfully cannot be forced to provide a decryption key if such production might incriminate them).

Some countries recognize that encryption is intertwined with individual rights to privacy and secrecy, while others restrict the use of encryption technologies. When it comes to whether service providers are required to assist law enforcement efforts to access encrypted communications, some nations

have passed laws requiring service providers to decrypt such data and imposing fines for failure to comply, while the law in other countries is less severe, mandating assistance where possible, but recognizing that many systems do not allow for such access.

What Is Encryption?

Encryption is the process of converting data into a code to ensure its confidentiality. Data in motion may be encrypted such that only the original sender and the intended recipient can access the information. This is referred to as end-to-end encryption and typically is applied in popular applications such as WhatsApp, Snapchat, and Facebook Instant Messenger. Another type of encryption may be applied to stored data or data "at rest." The devices that store the data typically are locked, which prevents the contents of the device from being read by anyone who does not possess the key. An example is the ever-present iPhone. End-to-end and device encryption guarantees the security of a person's communications.

In the absence of encryption, online communications easily are intercepted, creating the possibility of a cyberbreach that may result in millions of dollars of damage to a corporation or the compromise of an individual's personal and financial information. For this reason, encryption technologies are employed by businesses, government organizations, and most individuals, and have become a critical component of the digital era. A natural tension results, however, from these private interests and the government's interest in access to encrypted communications used to further criminal and terroristic conduct. The balancing of these competing concerns is at the crux of most encryption-related debates.

A common misconception about encryption relates to the ability of technology companies such as Apple or WhatsApp to "decrypt" data. Even though a company created the device or software on which the encryption was transmitted, it does not mean they have the encryption key required to access the information. The sender and recipient of a WhatsApp message, for example, are the only holders of the private encryption key. Thus, it is not simply a matter of compelling an entity to cooperate in an investigation. Rather, law enforcement believes that technology companies should create a "back door" to allow for access to such encrypted messages.

In the absence of encryption, online communications easily are intercepted, creating the possibility of a cyberbreach that may result in millions of dollars of damage to a corporation or the compromise of an individual's personal and financial information. A natural tension results, from these private interests and the government's interest in access to encrypted communications used to further criminal and terroristic conduct.

Law Enforcement Objections To Encryption

In 2014, former FBI Director James Comey opined that law enforcement and intelligence agencies were hampered by advancing technology, stating "Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority." In fiscal year 2017, the FBI reported it was unable to gain access to the contents of between one thousand and two thousand seized devices due to encryption. District attorney's offices around the United States have released similar statistics citing the number of times law enforcement officers supposedly were "hindered" from obtaining evidence from lawfully seized devices due to encryption.

Conspicuously absent from these figures and purported concerns, however, is the recognition that prior to the digital age, the potential treasure trove represented by such seized devices would not have existed and such conversations would have evaporated. Nevertheless, law enforcement officials point to these numbers in asserting that without access to both encrypted devices and data sent through end-to-end encryption, crimes will go unsolved and some criminals will not be brought to justice.

In response, cryptography experts express concern that the creation of a "technological architecture" that provides access to law enforcement seriously would compromise user security and privacy. Further, as summarized by one commentator, no way exists to provide access to the "good guys" without also making the system vulnerable to the "bad guys." These experts believe that opening access to law enforcement is likely to increase the number of

cyber-threats and attacks on private individuals and entities.

The conflict between private and public interests was at the forefront of a case brought in the U.S. District Court for the Central District of California where the FBI sought the contents of an iPhone belonging to an individual involved in a mass shooting in San Bernardino in 2015. Apple's encryption technology prevented the FBI from accessing the phone's data without the attacker's password. Relying on the All Writs Act of 1789, which allows federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principals of the law," the FBI sought to compel Apple to create a new software that would enable agents to access the data on the phone.

Apple resisted, arguing that a court order forcing the company to "decrypt" the iPhone would violate the First Amendment. The day before the scheduled hearing on the matter, the FBI announced it had found a third-party who was able to assist in unlocking the iPhone and withdrew its request.

The government's reliance on the All Writs Act in a separate but similar case was rejected by Eastern District of New York Magistrate Judge James Orenstein. He wrote, "The implications of the government's position are so far-reaching—both in terms of what it would allow today and what it implies about congressional intent in 1789—as to produce impermissibly absurd results." *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court,* 15-MC-1902 (E.D.N.Y. Feb. 29, 2016).

The Spectrum of Global Response

Governments across the globe have been struggling with how to balance law enforcement needs with the privacy arguments posed by civil liberty advocates. In many foreign countries, particularly those with totalitarian or potentially oppressive governments, encryption of daily communications by most people is common.

In the United States, the Communications Assistance to Law Enforcement Act (CALEA) provides that a telecommunications provider is *not* responsible for decrypting or ensuring the government's ability to decrypt any communication "encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."

In most instances, because the telecommunications companies do not have the "key" to decrypt the communication, the CALEA is not useful. Because law enforcement agents face Fifth Amendment concerns when they seek to compel individuals to provide the encryption key, the government often is without recourse to obtain this information.

The United Kingdom's Investigatory Powers Act, passed in 2016, expands the government's power to obtain plaintext data through compelled decryption and technical assistance from telecommunication carriers. Specifically, the carriers must "provide facilities or services" and remove "electronic protection applied by or on behalf of that operator to any communications or data." What is unclear is whether this applies to end-to-end encryption providers who do not maintain the capability of decrypting users' messages. If it does, these users would be required to redesign their systems.

Legislative proposals to outright ban some types of encryption have failed for the most part. For instance, in 2015, former British Prime Minister David Cameron unsuccessfully sought to ban online messaging applications that offer end-to-end encryption after the Charlie Hebdo shooting in Paris. Around the same time, the French Legislature debated a law that would require companies to provide "lawful access" to encrypted communications through the creation of back doors. Similar proposals have surfaced in the United States, most notably the Feinstein-Burr *Compliance with Court Orders Act* that was proposed in 2016, but did not become law.

In January 2019, Australia became the first Western nation to directly forbid secure encryption. The bill, which was rushed to a vote without full debate, forces companies to give encrypted data to police upon demand and to build tools to bypass encryption—the aforementioned "back door." Failure to comply can result in a fine to the company of the equivalent of approximately $7.3 million and prison sentences for individuals.

Australian authorities stated that the laws were needed to counter terrorism and organized crime. Shortly after the bill's passage, the Legislature introduced amendments in response to strong public objections to the law, including from technology companies that assert there is no way to perform the task without fundamentally reducing security. At the time this article was published, the

authors could find no evidence that any amendments had been made to the law.

In contrast, Germany has embraced encryption, focusing instead on establishing a lawful means of hacking into the such systems to obtain communication applicable to criminal investigations. In 1999, German officials adopted an encryption policy which has a key tenet that there will be "no ban or limitation on crypto products." In August 2017, an amendment to the German criminal code went in effect that authorized law enforcement to conduct hacking operations to gather evidence of crimes. Authorities must obtain a court order before engaging in such operations unless there is imminent danger.

Other countries, such as China and Russia, heavily regulate the encrypting companies themselves as a means of guaranteeing access, often without judicial review or oversight. In China, domestic companies that own popular encrypted messaging applications are not allowed to offer end-to-end encryption. Further, the companies are compelled to store such communications in plain text such that they are accessible to the government if needed. Companies that seek to disseminate or provide encryption services in Russia must apply for authorization from the government and a 2016 law requires them to forward metadata or content to Russian security services upon request, without a court order.

A brief summary of encryption laws and policies in some other countries is as follows:

• **Brazil:** No explicit right to encryption exists in Brazil, although its constitution guarantees the secrecy of correspondence and telegraphic, data, and telephonic communications. Brazilian laws require telecommunication service providers to ensure this secrecy, noting that the right can be suspended only if competent authorities request the information by court order.

• **Canada:** In Canada, although legislative power cannot be used to require providers to facilitate the decryption of encrypted communications, law enforcement officials can seek a court order under certain provisions of the criminal code to obtain a provider's assistance to access encrypted data.

• **India:** India has a law that gives the central and state governments the power to direct any agency to intercept, monitor or decrypt any information transmitted by computer if "it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence." Failure to comply is a criminal offense punishable by up to seven years' imprisonment, a fine, or both.

• **Japan:** The Criminal Procedure Code provides that telecommunications carriers may be asked to cooperate in implementing the interception of electronic communications, which includes decryption. Although carriers are obligated to cooperate, they are not penalized for failing to do so or required to develop decryption systems or software.

• **Turkey:** Companies wishing to provide encoded or encrypted communication services in Turkey must apply to the Information and Communication Technologies Authority (ICTA) for authorization. These operators are required to possess and maintain the ability to block access by users and intercept such communications upon lawful requests from law enforcement.

• **Kingdom of Saudi Arabia:** There are no data protection laws in Saudi Arabia. Accordingly, data privacy violations are evaluated by Saudi Arabian courts and adjudicatory bodies.

Conclusion

The debate about the degree to which encryption should be regulated is likely to continue as technology continues to advance. Changes in the nature of the game—from more familiar modes of communication, such as phone calls, to more sophisticated digital communication—do not alter underlying individual freedoms and privacy rights or support assertions that every communication should now be preserved and available for inspection by the government should it later put the communicator under scrutiny. The assumption that we should communicate in a way that preserves our communication for law enforcement eyes, in addition to the windfall of historical information already available in this digital era, has enormous implications for privacy in general, as well as for the criminal justice system.