WhatsApp, Encryption and the Battle with Law Enforcement

It is widely accepted that much of today's communications are digital – and as a result, the encryption of data, the privacy laws governing that data, and the role that governments play when national security and law enforcement issues are at stake is a very hot topic.

Encryption fundamentally ensures the protection of data (protecting content from being accessed or understood should it fall into the wrong hands) – and for the most part, that is exactly as it should be. The challenge comes when there is absolutely no way to unencrypt that data (thanks to non-key recovery encryption methods), especially where it concerns the criminal activity of gangs, drug cartels and even terrorists,

Matters came to a very public head in December 2015 following the San Bernadino shooting. The FBI was unable to access the iPhone content of the shooter due to its advanced security features, including encryption of user data. The FBI first asked the National Security Agency (NSA) to break into the phone but they were unable to. At that point the FBI asked Apple to create new software that would enable the FBI to unlock the phone. And Apple declined to do so.

In Brazil, WhatsApp and parent company Facebook have been locked in a year-long back and forth with law enforcement over access to user information as part of a criminal investigation.

At the root of the disagreement is WhatsApp's extraordinary level of encryption – which has seen the company adding end-to-end encryption to every form of communication on its service. The result is it is now impossible for the data sent over its network to be accessed, effectively making it impossible to comply with court orders requesting this information.

In this article, we will examine the status of encryption today, what it means in terms of law enforcement and what we can learn from the scenario in Brazil.

A BRIEF HISTORY OF ENCRYPTION

Communications is a critical need of any military force, and timely access to communications used by the enemy can be a key strategic factor in ensuring victory. For this reason, encryption technologies were developed to ensure sensitive content could not be deciphered by the opposition. Much as with actual weapons technologies, encryption is today considered a national security capability to be controlled by the Directorate of Defense Trade Controls.

As the information age dawned and digital communications became more prevalent, the National Bureau of Standards (NBS) put out a call seeking an encryption standard. The winner was an algorithm originally developed by IBM for money transfer, which was approved (and apparently improved) by the National Security Agency (NSA).

This standard, called DES (Data Encryption Standard) ushered in a new era of "asymmetric cryptography" where a combination of a public key and a private key – themselves consisting of large prime numbers – are used to encryption data.

By the 1990s, the use of DES in the private sector became prevalent, especially in commercial and academic circles. This trend began to raise flags with governments around the world, particularly law enforcement and national security agencies. They argued that foolproof encryption could allow criminals and terrorists to operate with impunity.

Fast forward to today, and the use of bulk encryption has only escalated. Techniques have only improved, the Internet has enabled communication on an unprecedented level, and more and more data on personal devices is being encrypted.

At the same time, the requirements by law enforcement agencies to at times access this data has escalated at a similar pace. Relying on a mixture of judicial support to request user data and government investment in combating sophisticated encryption methods, the desire to find workarounds is strong.

It is a contentious topic on ever level.

From a tactical point of view, there are three ways content can be legitimately investigated by law enforcement:

- A device where the content resides: This could be a computer, a smartphone, tablet or other device where there is information.
- Information in transit: When conversation content leaves the communication device of origin and is in transit to its destination.
- Intermediary communications server: Depending on the type of communication, it can be common to find persistent conversation content on another device used to bridge communications between sender and recipient.

Law enforcement requires judicial authorization to access any of the locations above for investigation purposes.

WHATSAPP AND ENCRYPTION

WhatsApp has historically encrypted its data – but for some time, it was possible for law enforcement to break it when necessary. Since 2012, however, WhatsApp has improved encryption to the point where government agencies had trouble deciphering the content. But given that WhatsApp still had access to the content via its servers, the information was still ultimately accessible when necessary.

Then in April 2016, WhatsApp announced that the company had added end-to-end encryption to every form of communication on its service. With that in place, not even WhatsApp's employees can read the data sent across its network. In other words, WhatsApp has no way of complying with a court order demanding access to the content traveling through its service.

While much of Silicon Valley has clashed with governments and law enforcement over privacy, and strong encryption is wholeheartedly supported in the technology field, the move by WhatsApp was unprecedented – effectively ensuring the content of a billion users remained

private under all circumstances.

WHATSAPP AND BRAZILIAN LAW ENFORCEMENT

On December 16, 2015, the 1st Criminal Court in Sao Bernardo do Campo, decreed an outage for WhatsApp nationwide on the grounds of non-cooperation with an investigation into a bank robbery gang. The next afternoon, the 11th Criminal Chamber of the Court reversed the decision.

Three months later, the Vice President of Facebook Latin America was arrested in São Paulo for failing to provide information requested by another criminal investigation.

On June 30, 2016 media reports revealed that the Federal Court of Londrina decreed the Facebook-owned bank accounts containing BRL 19.5 million be frozen as security for fines applied for non-compliance with court orders. The aim in doing so was to force WhatsApp to deliver certain users' conversation content

Finally, on 19 July 2016, the Rio Criminal Justice again ruled in favor of a WhatsApp outage in Brazil. On the same day, the decision was suspended, this time by the President of the Supreme Court.

LAW ENFORCEMENT'S POSITION

The move by WhatsApp raises multiple question on the ethics of balancing the right to privacy with national security and public safety. With this kind of encryption in place, companies are saying they have no control or responsibility for the traffic that passes over their networks – and can ostensibly ignore court orders as a result.

This runs counters to the historical law enforcement practice of intercepting communications in the interest of combating crimes and when approved by independent judicial means.

Some lawmakers have called on technology companies to facilitate an encryption 'backdoor' to be exclusively available for law enforcement use (as in the San Bernadino case). But as of today, that has fallen on deaf ears.

Right now, the balance of power is with the private sector. For example, Google states that it does not automatically collaborate with warrants which may invade user privacy. Facebook has created the "Law Enforcement Online Request System", to review that type of content requested by government agencies for investigation purpose, even warrants. Facebook requires details about the case and explanations of the importance of content being requested and does not automatically obey judicial warrants.

GETTING AROUND ENCRYPTION

So are there any options available to law enforcement to circumnavigate end-to-end encryption? And when would this be warranted? The answer to the first question is yes, at least in theory. Given that apps run on a user's device, it should be able to create a version which enables communication content capture between two or more persons/phone numbers of interest to law enforcement. The means to implement these features are numerous and relatively simple

but costly and not without risk.

A hypothetical example of how this hidden functionality within the application could be implemented would look as follows:

- Law enforcement requests the legal right to monitor one or more targets
- A judge issues a court order to WhatsApp
- WhatsApp, through its legal access to the internal system (which would need to be built) permits the targeting of specific telephone numbers/application IDs and from that point onward will capture conversations
- Each time a connection to WhatsApp servers is made, a query is conducted to see if that number/ID connecting is in a list of monitored numbers. If so, every message sent and received by that number/ID from that point on is sent without end to end encryption to WhatsApp servers or with a cryptographic key that WhatsApp has access to. This would be another feature that would have to be built in the application – in addition, the investigation target would need to update their version of WhatsApp to incorporate these changes.
- The content of these conversations could then be stored in a location accessible only by law enforcement or the WhatsApp department responsible for meeting judicial obligations.

The cost involved alone is doing this would be significant including construction of an internal monitoring system, construction of functionality to monitor specific targets and construction of supporting functionality on the server side for example. And the purpose of this hypothetical monitoring system is ultimately at odds with WhatsApp's stated goal of ensuring user privacy.

However, while WhatsApp cannot save the content of users' messages, that does not necessarily mean they do not have access to communications metadata such as who talks to whom; how long their interaction is; potential connections between suspected targets and the volume of data between one suspect and another. While no substitute for the content of a message, these data is not without merit for law enforcement.

CONCLUSION

The saga of WhatsApp and the Judicial System of Brazil illustrates the need for some sort of compromise to be reached between law enforcement, national security and technology communications companies. And dramatic gestures such as disabling service as we saw in Brazil detrimentally impact the daily lives of people – and many businesses and public services. Right now, it appears we are at a stalemate with technology communications companies opting to prioritize user privacy over potential crime or terrorist concerns. Given many of these companies effectively monetize user metadata for marketing purposes, it is also raises questions about the validity of some of these claims to absolute privacy.

What is clear is that this battle is far from over.