PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 17 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Government Backdoors in Encryption: Security vs. Surveillance

A backdoor for security can become a doorway of surveillance

By **Minahil Younas** | University of Agriculture | Published: September 2026
minahilyounas473@gmail.com | Position: Student

Introduction

As we all know, this is the digital era, and everything happens digitally. No doubt it makes our lives faster and easier, but there is also a threat to security and privacy. That's why Encryption is used to help you protect your data from unauthorized access. Encryption uses a key method for protection. The key method is basically a process of sending and receiving the data from the key to make it in the same form as the attacker or unauthorized person.

Encryption is process of converting readable data into unreadable form and only authorized person can read and access data using key. With end-to-end encryption, only the person who sends data (sender) and the person who receive data (receiver) can access the message, and only they can make changes in it. The key is a cipher text that hides the real meaning of the message, allowing important information to be kept secret; it is used not only in the modern era but also in the ancient era. The biggest and most usable app that is used is What's App, and some other applications like IMessages and Email, etc., to protect billions of conversations daily.

> ***"Encryption protects more than messages, it protects freedom, trust, and the right to communicate without fear."***

Do Governments Need Backdoors?

Backdoors is basically a way to pass the encryption to the government for protective purposes. Government argues that they needed the encrypted data because the criminals and attackers also use the apps for encryption to attack. Attackers basically use the encrypted apps to decrypt the data and information without the key; they use different types of methods to decrypt the data.

The Government also wants to get a backdoor for the investigations, like to get critical evidence against the criminal, and also they want to detect any kind of disturbance before anything happen means the crimes may go undetected. Basically, these concerns are real, and we can't deny the fact about the difficulty, and we can't ignore them.

Vol. 01, Issue 17 • ISSN: 3136-2729

Figure 1: Encryption and Surveillance| Source: AI-generated image.

Why Backdoors Are Risky

1. There is no such thing as a "**safe**" Backdoor because any built-in access can create a vulnerability. Hackers or cybercriminals find a way to enter into the system and get the data by using the system's weakness. Also, the foreign actors, spy and other person can detect the information of the targeted country and then use it against them. The data that is more sensitive will become less secure after this because there is not secrecy left after the backdoor, because after that, it is not only in the sender or the receiver.

2. **Criminal will adapt** different kinds of tools and software for encryption if the government reduces their privacy and security protection. Attackers use different private or open-source platforms to avoid detection by the government. This means ordinary users lose privacy while criminals avoid detection.

3. **Global consequences** means the if one country enforces the backdoors, then the other countries will also follow. If all the countries are ready for the backdoor, then they can also use one country's data for surveillance and control, which could threaten journalists, activists, and everyday citizens.

Who Is Most Affected?

The most affected from the Backdoors are: journalists who protecting our sources so that the identity of the source must be hidden and confidential by using encryption. Also, the people who face abuse need a confidential communication so that they can freely communicate without being monitored. Also, LGBTQ people face a suffocated environment, but encryption helps to hide their identity, and also businesses need to protect their customers' data by using encryption so that their personal information can loose and can maintain or gain their trust.

Encryption is not only about hiding information, but it also plays an important role in maintaining trust and avoiding the misuse of data, and can give confidence to the user that their data will be secure and they are free to communicate.

Better Alternatives

Instead of weakening the encryption from the backdoor, there are some experts who suggest that there are safer ways instead of using the backdoor method to investigate crimes.

Metadata analysis means authorities can learn from the communication patterns , which is done without reading the actual message, just studying the pattern, like who contacted to whom and when. Also, one way is using the court-approved devices like only allows access to the suspect's device legally form the court order. Otherwise, use only the traditional investigation method, such as surveillance, interviews, and evidence collection. These methods are helpful for law enforcement and also for the ordinary user's safety.

What's Next?

The debate is about the trust not only in technology, because encryption is the name of trust , people encrypt messages for secure communication, while weakening it may lead of misuse, trust issue and a great risk of loss sensitive information.

> ***"Should any system exist that allows access to everyone's private data, even with good intentions?"***

About the Author

Minahil Younas is an IT student who is focused on enhancing and improving her skills for better development. She can be reached at minahilyounas473@gmail.com.

Keywords: Encryption; Cyber Security; Privacy Rights; Government Access; Data Protection

References

[1] Third Way, "Surveillance and encryption." Available: **https://www.thirdway.org/memo/surveillance-and-encryption.**

[2] S. Landau, "Encryption and surveillance," *Communications of the ACM*, Available: **https://cacm.acm.org/opinion/encryption-and-surveillance/.**