Factsheet For Policymakers:

6 Ways "Lawful Access" Puts Everyone's Security At Risk

What is Encryption?

Encryption is the process to scramble or hide information so it can only be read by someone with the means (or keys) to return it to its original state. **End-to-End (E2E) encryption provides the strongest level of security and trust**, because ideally only the intended recipient holds the key to decrypt the message. No third party should have a key.

Encryption technologies are tools that help keep people safe online by protecting the integrity and confidentiality of digital data and communications. They secure web browsing, online banking, and critical public services like electricity, elections, hospitals and transportation – and every citizen that relies on them. In 2018, more than 1.7 billion users used E2E encrypted messaging services to protect their communications[1].

Some governments are concerned encryption could make it harder to collect information to prevent or punish terrorists and criminals. They have rushed to enact **"lawful access" mandates** to give law enforcement and intelligence agencies the power to intercept and access encrypted communications, or ask companies to do it for them. **This is dangerous to everyone online.**

While it is often argued these mandates will not affect the encryption and instead use other ways to provide access, user security is still at risk. Any point of entry to a secure service is a weakness.

"Lawful access" measures weaken the security of the Internet and put the global economy, the critical services we depend on, and the lives of all citizens at greater risk of harm. Here's how:

[1] https://telegram.org/blog/200-million
https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad

1 **Forced Weakness Weakens Us All:**
There is no digital lock that only 'good guys' can open and 'bad guys' cannot. "Lawful access" will make it easier for others, such as criminals and hostile governments, to gain access to sensitive data.

2 **Risks to National Security and Personal Safety:**
By making personal information, bank data and state secrets less secure, "lawful access" could unintentionally facilitate espionage, identity theft, blackmail, market manipulation and more.

3 **Terrorists Will Find New Cloaks:**
If terrorists and criminals know encrypted messaging services could be accessed by law enforcement, they will use their own alternatives. The communications of criminals and terrorists could then be immune from observation while those of everyday users would be more vulnerable.

4 **Life-Threatening:**
End-to-end encrypted communications protect the identity of journalists, activists, protected witnesses, undercover police, and many others. Vulnerable communications put these lives at risk.

5 **Internet Infrastructure Risks:**
"Lawful access" measures threaten key security components of the Internet's infrastructure layer, such as authentication mechanisms, critical to everyone's safety online.

6 **Impact on Trade and Investment:**
"Lawful access" could have a significant impact on the global economy. For most multi-national companies, a significant portion of their revenue and potential growth is generated in current and emerging markets overseas. People may be reluctant to buy products or use services from countries where governments could have access to their private information and communications.

Every country has a right and duty to protect its citizens. However, hasty attempts to facilitate access, even if well-intentioned, pose a great risk to the security of law-abiding citizens and the Internet at large.

Don't take away our strongest digital tools to protect ourselves, our countries and our economic livelihood. Tell world leaders to support strong encryption for all.

Internet Society internetsociety.org