Resolution on Lawful Access

November 15, 2019

FINAL DRAFT v1.8

Resolution: Be it resolved, the law enforcement attendees of the 37th Meeting of the INTERPOL Specialists Group on Crimes against Children, November 12-15, 2019, Lyon, France, who are committed to the protection of children throughout the world, strongly urge providers of technology services to allow for lawful access to encrypted data enabled or facilitated by their systems.

Statement of Problem: Globally, children are being sexually exploited and the imagery of this abuse is being widely distributed across the Internet. Service providers, application developers and device manufacturers are developing and deploying products and services with encryption which effectively conceals sexual exploitation of children occurring on their platforms, from their own eyes, and from Law enforcement seeking to identify the involved offenders and victims.

We are concerned where companies deliberately design their systems in a way that precludes any form of access to content, even in cases of the most serious crimes committed against children. This approach puts vulnerable citizens and society at risk by severely eroding a company's ability to identify and respond to the most harmful illegal content, such as child sexual exploitation, as well as law enforcement agencies' ability to investigate serious crime. Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format. Those companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content. Law enforcement agencies are increasingly prevented from accessing communications made on diverse platforms, as well as data stored on cell phones or computers, despite having legal authority based on the premise of probable cause, to access it.

Lawful access refers to a legal request for electronic data related to a criminal investigation that has been authorized by a competent legal authority. Today, criminal investigations related to individuals involved in the online sexual exploitation of children are often stalled by encryption techniques designed by service and product providers. Investigators from INTERPOL member nations, acting with legal authority, to help rescue children from sexual abuse and to identify the producers and distributors of child sexual abuse material are increasingly encountering computer systems and online accounts and communication platforms that have been encrypted with unbreakable technology.

Call to action: Private industry has the ability to implement and deploy products and technology to its customer base which allows for lawful access to data, while maintaining customer privacy. Technologists agree such a solution can be implemented in a way that would enhance privacy while maintaining strong cyber security. Most providers of such technology abide by industry-agreed acceptable-use standards that prohibit platforms from hosting or transmitting child sexual abuse material. In order to honor and enforce these standards, providers should fully comply with court orders authorizing law enforcement agencies access to data related to criminal investigations involving the sexual exploitation of children.

The current path towards default end-to-end encryption, with no provision for lawful access, does not allow for the protection of the world's children from sexual exploitation.

Technology providers must act and design their services in a way that protects user privacy, on the one hand, while protecting user safety, on the other hand. Failure to allow for Lawful Access on their platforms and products, provides a safe haven to offenders utilizing these to sexually exploit children, and inhibits global law enforcement efforts to protect children.