

LAWFUL ACCESS



(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

APP	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
<p>Information Accessed</p>									
	<p>Legal Process & Additional Details</p> <ul style="list-style-type: none"> • Message Content: Limited • Subpoena: can render basic subscriber information • 18 U.S.C. §2709(d): can render 25 days of iMessage lookups to and from a target number¹ • Pen Register: no capability² • Search Warrant: can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud 	<ul style="list-style-type: none"> • Message Content: Limited⁴ • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage <p>³Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applies and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)</p>	<ul style="list-style-type: none"> • No Message Content • Date and time a user registered • Last date of a user's connectivity to the service 	<ul style="list-style-type: none"> • No Message Content • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP address and phone number to relevant authorities 	<ul style="list-style-type: none"> • No Message Content • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last logs 	<ul style="list-style-type: none"> • No Message Content • Provides account (i.e. phone number) registration data and IP address at time of creation • Message history: time, date, source number and destination number 	<ul style="list-style-type: none"> • No Message Content • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active 	<ul style="list-style-type: none"> • Message Content: Limited⁴ • Subpoena: can render basic subscriber records • Court Orders: Subpoena return as well as information like blocked users • Search Warrant: Provides address book contacts and WhatsApp users who have the target in their address book contacts • Pen Register: Sent every 15 minutes, provides source and destination for each message <p>³If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content.</p>	<ul style="list-style-type: none"> • No Message Content • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number
	<p>SUBSCRIBER DATA</p>	<p>MESSAGE SENDER-RECEIVER DATA</p>	<p>DEVICE BACKUP</p>	<p>IP ADDRESS</p>	<p>ENCRYPTION KEY(S)</p>	<p>DATE/TIME INFORMATION</p>	<p>REGISTRATION TIME DATA</p>	<p>USER'S CONTACTS</p>	

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

¹ (U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry between parties does not indicate a conversation took place. These query logs have also contained errors.
² (U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.