Responding to Law Enforcement Agencies

2022.01.19

We provide our users with a variety of services that have become staples in their day-to-day life, first and foremost being the LINE communication app. As a result, we handle a large amount of our users' private data.

We want our users to feel that the LINE app allows them to easily, enjoyably, safely, and securely communicate with close friends and family. Owing to the nature of the app, it's essential that we carefully protect the privacy of our users. In principle, we don't provide users' information to third parties without their consent. User information is also not used for other purposes that exceed the necessary boundaries of the services we provide. We don't respond to such external requests for user information and we implement a number of security measures to prevent any unintentional breach of privacy. We don't in any way support any activities that unfairly threaten the human rights of our users, such as eavesdropping or censorship by state authorities. These principles and policies apply not only to the LINE app, but also to all of the services we provide.

However, we do make exceptions to the above when responding to investigations from law enforcement agencies. When we receive a request for disclosure from law enforcement, we may provide the information required for the investigation, within an appropriate scope, in limited instances when compliance is appropriate per applicable law.

Our stance concerning responding to law enforcement agencies

The following is our stance concerning our response to law enforcement agencies.

Under what type of legislation and in which circumstances will information be disclosed to a law enforcement agency?

We conduct our operations in accordance with Japanese law.

Under Japanese law, if deemed necessary for the investigation of an offense, a prosecutor, a prosecutor's assistant officer, or a judicial police official may perform search and seizure under a warrant issued by a judge, and the requested businesses are obliged to comply with the court order (Article 218, paragraph (1) of the Code of Criminal Procedure).

In addition, the law enforcement agency may ask for a report on necessary matters relating to the investigation (Article 197, paragraph (2) of the Code of Criminal Procedure).

Furthermore, there may be circumstances considered appropriate for unavoidable disclosure of information in terms of averting present danger (Article 37, paragraph (1) of the Penal Code) to prevent

present danger to human life or body, such as in the case of the need to protect life from the threat of suicide or abduction.

In this way, we may respond to the law enforcement agency within the scope assessed appropriate, and only ① in the case of an order for seizure for investigation, ② if there is a request for cooperation with an investigation with a legal basis (such as Investigation-Related Inquiry in Japan), and ③ if judged that it would avert present danger.

These laws not only apply to us but similarly apply to other business operators in Japan.

What does it mean to respond to a law enforcement agency?

When we respond to a law enforcement agency, we will submit the information registered by our services (including usage data) for a relevant person such as a suspect or victim to the law enforcement agency, such as the police, to aid in solving cases when a crime has been committed or a person's life, body, or property are threatened only where ① to ③ above apply. When responding to a law enforcement agency, we will not submit or provide information on unspecified users.

Why do we respond to law enforcement agencies?

We respond to help in the apprehension of suspects, to mitigate damages , and to prevent crime, such as fraud, murder, assault, or other criminal offenses committed in whole or in part through our services in the interest of protecting human life, body, or property.

As a service provider, we have a responsibility to offer a safe and secure environment for users to feel at ease using our services. As explained below, we may respond to law enforcement agencies only within the restraints of the law and in cases that meet our strict standards.

In the case of international requests

We handle requests from overseas in accordance with frameworks for international investigation cooperation such as 'The Act on International Assistance in Investigation and Other Related Matters' and mutual legal assistance treaties (MLAT) with specific countries. This includes instances where the Japanese police may receive a request via the International Criminal Police Organization (ICPO), or Japan's Ministry of Foreign Affairs may receive a request via an embassy. The same rules regarding warrants and verification by privacy protection organizations and other handling rules apply.

What is the process for deciding whether to respond?

After we receive a request from a law enforcement agency or after recognizing that a present danger requires action, our privacy protection teams shall immediately and thoroughly examine the legal, security, and governmental details of the case to verify the propriety of the investigation and whether to respond from the standpoint of legality and the protection of users. We will refuse the request at this point if there is legal inadequacy for examination in the case of a request from a law enforcement agency. In the event that the scope of the request is too broad for the purpose of the investigation, we will request the investigating body to provide an explanation of its intent. Should the explanation be insufficient, we will not respond to

the request for cooperation. In addition, should the user data that is the target of the investigation be already expired, we will explain to the authorities that the information has already been deleted.

We will only respond to the law enforcement agency in accordance with strict information handling rules, and only when a thorough verification confirms the legalities and propriety of the investigation. Information provided to the law enforcement agency shall only be in accordance with our strict internal procedures. The law enforcement agency is not allowed to eavesdrop or build a backdoor against our user privacy protection system. Furthermore, we do not comply with requests in which the cause of the crime is not related to the use of our services, such as a request in terms of national security (public safety, counterterrorism measures) which has not yet turned out to be a criminal act and based on the grounds of abstract risk or a request for censorship.

What kind of information do we disclose?

Provision is strictly limited to information required for the relevant investigation and trial. When internal review processes determine the law enforcement agency's request in accordance with such as a warrant is too broad for its purpose of use, we will ask the law enforcement agency for additional explanation, and reject the request unless we find there are reasonable grounds. We do not submit the data of unspecified users irrelevant to the investigation. The following data regarding specified user accounts will be disclosed to law enforcement agencies:

LINE

・ Registered account data (profile image, display name, email address, phone number, LINE ID, date of registration, etc.)

・ Communication history of specified users (message delivery date, IP address of sender, port number of sender)*

*There is no disclosure through Investigation-Related Inquiry

・ Specified users' text chats**

Only when end-to-end encryption has not been applied (if end-to-end encryption has been enabled, we cannot decrypt/extract the contents of text chats, so no disclosure of the contents of text chats is possible). End-to-end encryption is applied by default since July 1, 2016. For more details, please see **Data Security.

**Even if unencrypted text chats are disclosed, as per our policy, only up to seven days of text chats will be disclosed.

**Only when receiving an effective warrant issued by the court.

**Video / picture / files / location information / phone call audio and other such data will not be disclosed.

LINE Pay

・ Registered account data (name, address, email address, phone number, bank account information, date of registration/deletion of account, etc.)

・ Account usage details (deposit and withdrawal history, remittance history, payment history, exchange history, etc.)

・ Personally identifying account info

・ Information used to register a LINE Pay card (recipient's name, address, date applied, etc.)

Other Services

The following information will generally be disclosed for other services:

・ Information used to register an account on the relevant service.

・ Usage history of the relevant service.

When a request is received after the temporary storage period required for service operation is elapsed, we will be unable to provide said information because it has already been deleted.

Do we notify affected users prior to disclosing their information to law enforcement agencies?

The user will not be notified if doing so is forbidden by law, or if doing so would be inappropriate given the facts of the investigation (ex: threats of suicide or criminal activity), or if it would otherwise be deemed unreasonable. In other cases the user will be notified.

Request types

Investigations in which we may cooperate include the following:

・ Personal injury (murder, bodily injury, etc.)

・ Monetary damage (fraud, blackmail, etc.)

・ Child abuse (child prostitution, child pornography, etc.)

・ Illegal trade (drug trading, bank account fraud, money laundering, etc.)

・ Threats of illegal activity (suicide threats, murder threats, bomb threats, etc.)

1. Case study

If we received a warrant from law enforcement to disclose the communication history between a suspect and victim for a murder case in which the suspect used the LINE app to lure the victim to the murder scene, we would comply.

2. Case study

If we received a warrant from law enforcement to disclose the past six-month communication history of a user suspected of repeated theft, we would reject the request on the basis that the specified investigation period is too long.

3. Case study

If a suicidal user had declared to a friend using the LINE app that he or she will jump in front of a train, and the friend approached law enforcement for help because the user could no longer be contacted, we may be requested by law enforcement to disclose the IP address and registered information of the suicidal user. In such a case, we would determine whether or not to respond based on the following conditions for “Averting Present Danger” (Article 37, paragraph (1) of the Penal Code): (a) urgency (based on information provided by law enforcement regarding the date and time, location, and method of suicide); (b) indispensability (the case cannot be resolved without the information that LINE could provide); (c) balance of legal benefits (the value of the legal benefit of disclosure is equal to or higher than the legal benefit of protecting a person's privacy). Additionally, we may directly alert law enforcement of such threats of self-harm or criminal activity when detected by our Timeline/OpenChat monitoring or when reported by other users, while taking these factors into account.

4. Case study (Finance)

In the potential cases described below, the registered data of a suspect or 3 months of a suspect's LINE Pay usage data would be provided to law enforcement once provided with a request for information. ① If LINE Pay was used in a suspected money laundering scheme. ② If money was sent between friends via LINE Pay to purchase a product, but the product was never delivered to the buyer. ③ If the victim's bank account was linked with the suspect's LINE Pay account and money was fraudulently deposited into the suspect's LINE Pay account. However, disclosure of usage history will be left to our discretion, and policy dictates that we will deny any requests for usage details exceeding 3 months in total. Furthermore, identifying information of anyone besides the suspect will not be included in the usage history, even if the party receiving bank transfers is suspected of being involved in money laundering. Law enforcement agencies must provide a separate request for the information of the second party involved in suspected money laundering.

5. Case study (Finance)

In cases where money is suspected to have been obtained fraudulently and then deposited into a LINE Pay account, or if that money was used to purchase stocks through LINE Securities, information will not be disclosed to law enforcement agencies if doing so would adversely affect the user's assets on LINE Pay or LINE Securities, or if such methods were not deemed to be the principle means through which a crime was committed. However, information will be disclosed if a court warrant is issued.

LINE Transparency Report

The LINE Transparency Report discloses information about user data requests we receive from law enforcement.

We believe that responding to requests to apprehend suspects, mitigate damages, save human lives, and prevent crime is part of our responsibility as a provider of internet services that are used by a large number

of people. At the same time, we understand that excessive information disclosure requests from law enforcement to internet service providers may threaten user privacy.

It is essential for us to provide transparency in how often we receive and respond to requests from law enforcement in order to protect the privacy of LINE users and fulfill our social responsibility as a service provider.

We will regularly update this report to maintain transparency.

Report: **https://linecorp.com/en/security/transparency/top**

We will continually implement new initiatives that will enhance the transparency of how we treat and handle user information.