RingCentral

Transparency Report

Introduction

RingCentral is pleased to release our Annual Transparency Report ("**the Report**") for the year of 2021. This report is RingCentral's Second Annual Transparency Report, which covers data requests received between January 1, 2021 and December 31, 2021. This report reflects our commitment to transparency to our customers. We hope that this report is able to provide clarity to our customers into the types of government requests we receive on a yearly basis.

The Report covers **Total Global Government Requests**, which include **Data Requests, Emergency Requests, Intercept Requests, Pen Register and Trap and Trace Requests, Preservation Requests, and US National Security Requests**.

The Report identifies (1) the number of requests that resulted in the disclosure of data, (2) the requesting country, and (3) the categories of data, if any, that we provided to authorities.

Definitions

Request Types

The following definitions cover the types of requests for customer data submitted by law enforcement and government agencies around the world.

- **Data Requests** are requests for information relating to a RingCentral customer account in connection with an official criminal or administrative investigation or proceeding. Examples of legal processes that may serve as the basis for a Data Request include the following:
  - — Subpoenas
  - — Court Orders
  - — Search Warrants

  Data Requested may include: Account Information, Call/Fax/SMS Logs, and Content Data, as defined below.
- **Emergency Requests** are requests for Account Information that involve the risk of serious bodily harm or death and must be responded to immediately. These can sometimes also include Content Data.
- **Government Requests** are any of the requests for information listed below that come from government agencies or law enforcement authorities.
- **Intercept Requests** mean requests for the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
- **MLAT Requests** are requests made pursuant to a Mutual Legal Assistance Treaty (**"MLAT"**) by a non-US authority for data maintained in the US. A non-US agency must make an MLAT request to US authorities in order to seek disclosure of data maintained in the US.
- **National Security Letters ("NSLs")** are requests made by the US Federal Bureau of Investigation for subscriber information, billing records, or

electronic communication transactional records. NSLs cannot include requests for Content Data.

- **Pen Register/Trap and Trace ("PRTT")** consist of Pen Registers, which are devices that capture the phone numbers dialed on outgoing telephone calls, and Trap and Trace, which are devices that capture the numbers identifying incoming calls. They do not reveal the content of communications.
- **Preservation Requests** are requests to preserve account information in connection with an official criminal or administrative investigation or proceeding.
- **US National Security Requests** are requests for customer data pursuant to the Foreign Intelligence Surveillance Act (**"FISA"**).

Response Types

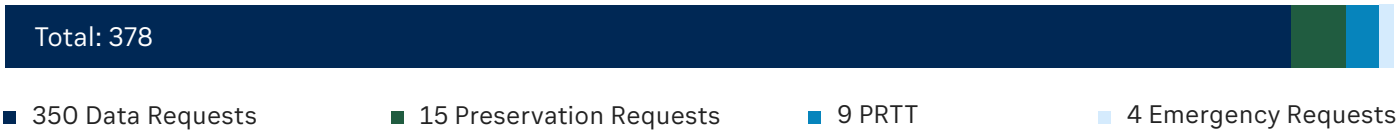
These are categories of data we may provide in response to requests for customer data.

- **Account Information** may include the following information:
  - Subscriber information: customer's full name, contact telephone number, company name (if applicable), physical or mailing address, email address, date of account signup or deactivation date which is submitted by the customer upon registration
  - Additional numbers or extensions
  - Billing history (note that RingCentral does not maintain complete credit card numbers)
  - Comment logs
  - Device descriptions and serial numbers (if devices are registered to the account)
  - WEB sessions (if the account was accessed via a web browser)

  The Account Information disclosed depends on the contents of each specific request.
- **Call/Fax/SMS Logs** display a complete record of incoming and outgoing calls/faxes/SMS, as well as company number and specified extensions. They contain origin, destination, and duration of the service but no content.
- **Content Data** may include the content of faxes, voice messages, and SMS messages, call and video recordings, and messaging data. The extent and type of Content Data disclosed depends on the contents of each specific request. Content Data includes Account Information.

Charts

Types of Government Requests



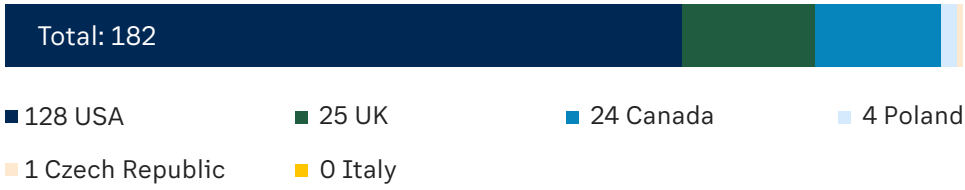
Government Requests by Country

Data Provided by Type

Data Provided by Country

Data Not Provided

Account Information



Call/Fax/SMS Logs

Communications Content

NSLs and National Security Requests

RingCentral reports NSLs and National Security Requests within ranges permitted by law pursuant to the USA FREEDOM Act of 2015, as amended. RingCentral is not authorized to disclose account-specific or sensitive information regarding the number and content of NSL or National Security Request types. Instead, we report the number of NSLs and National Security Requests received in bands of 0–99 on an annual basis. RingCentral cannot further disclose what information or data may be sought through these requests.

NSLs and National Security Requests	
January 1, 2021–December 31, 2021	0–99
Total Accounts/Users	0–99

Frequently Asked Questions

How did RingCentral prepare this Transparency Report?

Our Legal and Privacy teams reviewed Government Requests for customer data received in 2021 to determine which requests we received, from which countries, and how we responded to such requests. We are including in the Report the total number of requests received, the countries of origin, and what category of data we disclosed in response to such requests.

How does RingCentral's methodology for compiling this report differ from previous years?

We used the same methodology we used in compiling our Transparency Report for 2020 in completing this report. The data underlying the two reports is different.

Does RingCentral reject any requests for customer data?

RingCentral reserves the right to respond or object to any request for data in any manner consistent with applicable law. RingCentral rejects or challenges requests that are, among other reasons, not accompanied by any valid legal process or valid legal basis.

What kind of information does RingCentral provide in response to Government Requests?

In response to Data Requests from a government agency or law enforcement, if validly served and supported by valid legal processes, RingCentral may provide Account Information, Calls/Fax/SMS Logs, or Content Data.

Does RingCentral notify its customers of Data Requests?

RingCentral notifies its customers of any Data Requests related to their data, to enable them to respond to the request directly, unless precluded from doing so by law or court order. If law enforcement officials believe that notification would jeopardize an investigation, RingCentral requires law enforcement to y obtain an appropriate court order or other valid legal process that specifically prohibits RingCentral from notifying the customer(s) prior to submitting their request to RingCentral.

What is the impact of CALEA to RingCentral services?

Commission on Accreditation for Law Enforcement Agencies (“CALEA”) is a US law requiring carriers and interconnected VoIP providers to implement the technical capability to enable law enforcement to access wire and electronic communications or call-identifying information for

communications and calls to/from the PSTN. Law enforcement must obtain appropriate legal authorization (i.e., a warrant) to obtain access. CALEA does not apply to communications via "Information Services," such as video and messaging.

Is RingCentral Subject to Section 702 of FISA?

As an electronic communication service provider, RingCentral is subject to Section 702 of FISA. Section 702 allows the US government to request information about non-US persons who are located outside of the US.

How can law enforcement agencies and government authorities submit Data Requests?

To learn more about how to submit Data Requests, please visit our RingCentral Data Request Guidelines. Please reference the guidelines before submitting a request, as RingCentral will only consider complete and valid requests.

Who should I contact for more information on RingCentral's Transparency Report?

For more information or questions about our Transparency Report, email privacy@ringcentral.com.

About RingCentral

RingCentral, Inc. (NYSE: RNG) is a leading provider of business cloud communications and contact center solutions based on its powerful Message Video Phone™ (MVP™) global platform. More flexible and cost effective than legacy on-premises PBX and video conferencing systems that it replaces, RingCentral empowers modern mobile and distributed workforces to communicate, collaborate, and connect via any mode, any device, and any location. RingCentral offers three key products in its portfolio including RingCentral MVP™, a unified communications as a service (UCaaS) platform including team messaging, video meetings, and a cloud phone system; RingCentral Video®, the company's video meetings solution with team messaging that enables Smart Video Meetings™; and RingCentral cloud Contact Center solutions. RingCentral's open platform integrates with leading third-party business applications and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

For more information, please contact a sales representative.
Visit ringcentral.com or call 855-774-2510.

RingCentral

865753803 04/2022

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com