Lawyer Insights

Call Detail Records: The Impact of India's Revised Guidelines for Other Service Providers on Outsourcing Customers and Providers

By Randall Parks and Christina Edwards
Published in CPO Magazine | February 11, 2022


India's Department of Telecommunications now requires outsourcing providers in India to capture and store certain call records and system logs at their Indian delivery centers. Outsourcing providers are raising these new requirements with their customers, who may feel compelled to adapt their contracts and practices to address these changes. Harsh Walia, of Khaitan & Co. LLP, and Randy Parks and Christina Edwards, of Hunton Andrews Kurth LLP discuss the new requirements.

The Indian DoT's new guidelines for "other service providers"

Propelled by the ongoing COVID-19 pandemic, India's Department of Telecommunications (the "DoT") made several efforts to relax restrictions on India's business process outsourcing and call centre industry beginning in March 2020. The most recent liberalization of restrictions relating to entities classified as "other service providers" ("OSPs") occurred on June 23, 2021, when the DoT released the Revised Guidelines for Other Service Providers (the "Guidelines"). Most outsourcing service providers who perform voice based business process outsourcing, call center and help desk services using telecommunications services in India are subject to the Guidelines.

Importantly, the Guidelines require OSPs to maintain and preserve call detail records ("CDRs"), usage detail records ("UDRs"), system logs and other records at the OSP centres in India. Historically, CDRs and UDRs have played a critical role in investigations of criminal breaches, security incidents and toll bypass. Telecom service providers are in any case required to maintain and preserve CDRs and UDRs as part of the security conditions of the licenses granted by DoT.

Several flexibilities granted under the latest Guidelines (like the use of a foreign based call manager or EPABX) are contingent on the maintenance of CDRs, UDRs, system logs and other records at one of the OSP centres in India. Additionally, the Guidelines impose several CDR, UDR and system log storage and maintenance obligations on OSPs. The latest version of the Guidelines has caused an unanticipated stir by spelling out the required contents of the CDRs, UDRs and system logs.

Under the Guidelines, the CDRs and UDRs must consist of (i) calling number, (ii) called number, (iii) date, (iv) start time, end time and duration, (v) identity of the device used for making the call (for example, MAC ID, device number, etc.), (vi) user identity (or log-in name) initiating the session, and (vii) media gateway identity, softswitch ID and trunk ID. The system logs must consist of (a) user and log-in identity, (b) date

and time of log-in, (c) date and time of log-out, (d) commands and activities performed, and (e) response of command and activities. The Guidelines require OSPs to preserve the CDRs, UDRs and system logs for one year.

Prior to the recent release of the Guidelines, in the absence of such stipulated requirements, the contents of CDRs, UDRs and system logs (which were already required to be maintained by OSPs) were dependent on the features and functionalities of the equipment used. Therefore, apart from the requirement that CDRs, UDRs and system records be maintained and preserved, the rules were notably less burdensome prior to the Guidelines because OSPs had more flexibility on the contents of such records. Now, OSPs have to expend additional effort to collect the prescribed contents of the CDRs, UDRs and system logs.

Customer responses to the DoT's new guidelines

Since the data collection required by the Guidelines is mandatory, outsourcing customers – especially those that are highly regulated or have made data location commitments to their customers – need to be savvy in structuring contractual provisions that navigate competing compliance demands. The negotiation between outsourcing customers and Indian OSPs will not be focused on whether the Indian OSPs collect, store, disclose and use the required information, but how they do so.

Outsourcing customers should consider whether their existing agreements with Indian OSPs are adequate to address the requirements of the Guidelines or whether specific amendments are necessary. If specific amendments or a side agreement are needed, the agreement (a "Guidelines Agreement") should briefly summarize the applicable Guidelines, specifically identify the data required to be collected, and where and how it will be stored and processed. Clearly identifying the rules and affected data memorializes the rationale for data retention and sets a foundation from which the parties can pivot as the Guidelines are revised in the future.

The Guidelines Agreement should require the OSP to implement information security requirements appropriate for the data and its storage and use, such as encryption and segregation of the collected data. These information security requirements will depend on each customer's sensitivities and may leverage requirements already captured elsewhere in the governing agreement between the parties.

The OSP's collection, use and disclosure of the collected data should be strictly limited to the scope of, and purposes required by, the Guidelines or other related applicable law. If the OSP is legally required to disclose any of the collected information, the Guidelines Agreement should require the OSP to provide the customer with advance written notice of any required disclosure (unless such notice is prohibited by the Guidelines or other applicable law), and to cooperate with the customer in seeking protective orders or other confidential treatment for the collected information.

As mentioned above, the Guidelines require retention of the CDRs, UDRs and system logs for one year. The Guidelines Agreement should adopt this retention period and prohibit any longer retention. Following the expiration of the one-year retention period, the OSP should be required to securely delete all stored data and provide the customer with evidence or certification that the deletion is complete.

All collection, storage, disclosure, use, and disposal of the collected information should be at the OSP's expense and limited to the minimum requirements necessary for the OSP to comply with the Guidelines or other applicable laws. If the Guidelines or other applicable laws change, the Guidelines Agreement

should require the OSP to promptly provide the customer with notice of such change and a description of the effect of such change on the collected data and the provisions of the Guidelines Agreement. If the change results in reduced requirements on the OSP for the collection, storage, disclosure and use of the collected information, the OSP's collection, storage, disclosure and use of the collected information should be reduced correspondingly.

Depending on the nature of the arrangement, the customer should also consider requiring the OSP to indemnify it for all third party claims arising from the OSP's collection, storage, disclosure and use of the collected information in a manner inconsistent with the Guidelines, and a termination right if the Guidelines are found to be in conflict with any laws applicable to the customer.

The foregoing suggestions are all highly dependent on the nature of the customer's business and the sensitivity of the collected information to each customer (and its customers). While Indian OSPs face commercial, administrative and technical challenges to capture the new information required by the Guidelines, outsourcing customers should evaluate new agreements and re-evaluate existing agreements with Indian OSPs to ensure their information and that of their customers is safeguarded while complying with obligations under the Guidelines.

Randall Parks *is a Partner in the firm's Global Technology, Outsourcing & Privacy practice group in the firm's Richmond office. With over 25 years of experience, Randy is a broadly experienced transactional lawyer known for his ability to creatively and collaboratively solve client business problems for clients in a wide range of industries. He can be reached at +1 (804) 788-7375 or rparks@HuntonAK.com.*

Christina Edwards *is an Associate in the firm's Global Technology, Outsourcing & Privacy practice group in the firm's Richmond office. Christina is a trusted counsel to clients on all aspects of outsourcing and technology matters, including commercial contracting agreements, software licensing issues and managing high-volume transactions. She can be reached at +1 (540) 556-9875 or cedwards@HuntonAK.com.*