

iTalk Global Communications, Inc.
2019 Annual CPNI Certification
EB Docket 06-36

I, William A. Burge, certify that I am an officer of iTalk Global Communications, Inc. and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules pursuant to 47 C.F.R. Section 64.2001 et seq.

Attached to the certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in Section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions against data brokers in the past year. The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may be subject to enforcement action.



William A. Burge, Vice President
iTalk Global Communications, Inc.

February 26, 2019

499 Filer No. 827024

STATEMENT REGARDING OPERATING PROCEDURES

1. *Section 64.2005; Use of customer proprietary network information without customer approval.*

iTalk Global Communications, Inc. (“iTalk”) uses individually identifiable CPNI for the provision of interconnected VoIP service from which the CPNI is derived, to provide customer support related to such service, and to bill and collect for such service. iTalk also uses individually identifiable CPNI to protect its rights or property, or to protect users of its interconnected VoIP service and other carriers from fraudulent, abusive, or unlawful use of or subscription to such services.

iTalk does not use individually identifiable CPNI for marketing except to market service offerings among the categories of service to which its customers already subscribe. iTalk does not provide Commercial Mobile Radio Services (“CMRS”) or local exchange services.

iTalk does not use individually identifiable CPNI to track customers that call competing service providers.

iTalk does not provide inside wiring installation, maintenance or repair services. iTalk does not conduct research on the health effects of CMRS. iTalk may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features.

iTalk may use CPNI to protect its rights or property, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

iTalk provides customers with an opt-out or “No-Disturb” approval option to be excluded from the use of CPNI for marketing purposes of service offerings among the categories of service to which its customers already subscribe.

2. *Sections 64.2007-8; Approval required and notification for use of customer proprietary network information.*

iTalk does not use or permit the use of individually identifiable CPNI for marketing purposes, or in any manner which would require customer approval under the FCC’s rules. Thus, it does not seek customer approval for use of CPNI, and does not maintain records of approval for use of CPNI for marketing purposes.

iTalk does not solicit customer approval for use of CPNI. As such, it is not required to provide notice to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

3. *Section 64.2009; Safeguards required for use of CPNI.*

iTalk does not solicit customer approval for use of CPNI because iTalk does not use CPNI for any purpose which would require customer approval under the FCC's rules. As such, iTalk does not maintain a system which indicates the status of a customer's CPNI approval.

iTalk does train personnel as to when they are and are not authorized to access CPNI, and iTalk has an express disciplinary process in place.

iTalk does not use CPNI for marketing purposes and does not share CPNI with any third parties.

4. *Section 64.2010; Safeguards on the disclosure of CPNI*

Safeguarding CPNI. iTalk has undertaken technical, operational and policy measures to discover and protect against attempts to gain unauthorized access to CPNI. Specifically, iTalk has taken steps to ensure that all access to CPNI is guarded by a password and those accesses granted by passwords are constrained so as to protect against breach and abuse. These protections are discussed in more detail below.

iTalk has undertaken development to provide tracking and auditing systems that record any access to CPNI attempted by an agent or customer and will store the data for a minimum of one year.

Telephone access to CPNI. iTalk has undertaken policy and training measures for customer care representatives regarding the proper handling of CPNI information over the telephone. Customer care representative are trained to identify a customer without the use of readily available biographical information. For example:

The customer care representative is able to call the customer back using a telephone number from the iTalk database that has been issued to the customer by iTalk, or previously registered with iTalk, by the customer, using their password.

The customer care representative may accept the customer's password as authentication. The customer care representative is permitted to initiate a password reset as described below, and is not permitted to divulge the password directly.

The customer is able to provide, without assistance from iTalk personnel, all of the call detail information necessary to address the customer care issue (*i.e.* the telephone number called, when it is called, and if applicable the amount charged for the call), then iTalk personnel are permitted to address that customer care issue.

Online access to CPNI. iTalk customers must provide a password to access CPNI online. For customers that purchase service online, establishment of a password for online access is part of the subscription process. For customers that subscribe over the telephone, a random password is generated and emailed to the customer.

In-Store access to CPNI. iTalk may disclose CPNI to a customer who, at a retail location, first presents to iTalk or its agent a valid photo ID matching the customer's account information or satisfies criteria defined for "Telephone access to CPNI" above.

Password selection and reset. During the initial subscription phase the customer is prompted to register a password. The same password is used for all future iTalk phone and online access. When a customer requests a password reset online, or on the phone with a customer care representative, the password reset is handled using the email address registered by the customer at the time of subscription. The email message may contain the password or an html link that walks the customer through the reset process.

Notification of account Changes. iTalk sends email notification of account changes to customers at their email address of record. Customers receive notice for changes to their password, PIN, security questions and address of record.

Training/Discipline. iTalk trains its employees and personnel as to when they are and are not authorized to use or access CPNI, and the company has an express disciplinary process in place in the event CPNI policies and procedures are not followed. Employees are subject up to and including termination of employment for access to CPNI if they conduct the access in a way that is not in compliance with FCC rules.

5. Section 64.2011; Security Breaches.

iTalk fraud detection personnel are responsible to monitor the tracking and auditing data for possible breaches in CPNI data. iTalk trains its employees and personnel to report all suspected breaches of CPNI data to iTalk general counsel, chief engineer and CEO in order to ensure that security breaches may be handled in accordance with the FCC's regulations.

iTalk shall notify law enforcement of a breach of its customers' CPNI. iTalk shall not notify its customers or disclose the breach publicly, whether voluntary or under state or local law or these rules, until it has completed the process of notifying law enforcement.

As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, iTalk shall electronically notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") through a central reporting facility. Notwithstanding any state law to the contrary, iTalk shall not notify customers or disclose the breach to the public until seven (7) full business days have passed after notification to the law enforcement agencies except in the following cases: (i) if iTalk believes that there is an extraordinarily urgent need to notify any class

of affected customers sooner than otherwise allowed in order to avoid immediate and irreparable harm; or (ii) in the event that the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct iTalk not to so disclose or notify for an initial period of up to 30 days, plus any extensions reasonably necessary in the judgment of the agency.

After iTalk has completed the process of notifying law enforcement as described above, it shall notify its customers of a breach of those customers' CPNI.

iTalk maintains a record of any breaches discovered, notifications made to the USSS or FBI and notifications made to customers. The record shall include, if available, dates of discovery and notification, a detailed description of CPNI that was the subject of the breach, and the circumstances of the breach. iTalk shall retain the record for a minimum of two (2) years.