Digium Cloud Services L.L.C. Customer Proprietary Network Information Policy

January 26, 2015

Table of Contents

CPNI: Definition and Background

Digium Cloud Services LLC, a wholly owned subsidiary of Digium Inc., ("DCS") is committed to protecting the privacy and security of our customers' personal information as set forth in the Digium Inc. privacy policy and also in any product or service specific agreements http://www.digium.com/en/company/policies . We strive to be transparent about how we use and protect the information we collect from our customers. **This policy applies to all DCS services except for Respoke as Respoke is not an Interconnected VoIP service.**

As an interconnected VoIP service provider, DCS has access to a highly regulated form of customer personal information known as Customer Proprietary Network Information or "CPNI". Due to an April 2007 order which requires that interconnected VoIP providers abide by CPNI regulations previously only imposed on telecommunications carriers, DCS has a duty to protect the confidentiality of CPNI and use for marketing purposes subject to the guidelines provided in federal law and so DCS has created this CPNI policy to insure compliance with federal requirements.

Setting your CPNI Password and Security Questions

As detailed further in this policy, there are some circumstances under which we must ask DCS customers for the CPNI call-in password or security questions. Before reading further please take a moment to set up or reset your CPNI call-in password and security questions by signing into my.digium.com/en/user, clicking "My Account", and clicking on the managing CPNI link.

Definition of CPNI:
"(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes some highly-sensitive personal information."

DCS also receives access from customers to subscriber list information.

Definition of Subscriber List Information:
"Subscriber list information includes customer names, addresses, telephone numbers, and for business customers, the headings under which they are listed in the yellow pages. This information remains subscriber list information even if it appears on an invoice as it does not pertain to the telephone exchange service or telephone toll service received by a customer of DCS. This information is used as appears in the Digium Inc. Privacy Policy and any product or service specific agreements and is not governed by this CPNI specific policy."

For most DCS customers the most sensitive CPNI is the detailed call records of whom the customer called or from whom they received calls. This information may be of interest to people who attempt to engage in a practice known as pretexting. Broadly speaking, pretexting is when a person pretends to be customer or a law enforcement official in order to obtain CPNI. In some cases the purpose of pretexting is to offer calling records for sale on the Internet. Pretexting is a crime punishable by fine or imprisonment of up to 10 years.

Examples of DCS Customer Specific CPNI
Jenny Smith of Alabama whose telephone number is 867-5309 licenses a single seat of Switchvox Cloud on a month to month contract at $35.00 per user. Jenny Smith also calls her friend Tommy T in Oregon every Tuesday night at 8 pm.

Of the above, the following is CPNI: (1) Jenny Smith licenses Switchvox Cloud, (2) Jenny Smith licenses a single seat, (3) Jenny Smith is on a month to month contract, (4) Jenny Smith calls Oregon, (5) Jenny Smith calls Tommy T, (6) Jenny Smith calls on Tuesday nights, (7) Jenny Smith calls on Tuesday nights at 8 pm, and (8) Jenny Smith pays $35.00 per user.

What is NOT CPNI is the fact that Jenny Smith lives in Alabama and that Jenny Smith's phone number is 867-5309. Only the detailed information pertaining to Digium Cloud Services products and services (excluding Respoke) is CPNI.

Any published directory information or information that is in the public domain, such as customer's name, address, and telephone number is not CPNI.

DCS and its parent company Digium, Inc. occasionally publish on their public websites case studies of their customers. If DCS or Digium Inc. wishes to publish a case study regarding the customer then DCS or Digium, Inc. will first make it clear to the customer any information in the study that may be CPNI under the FCC rules and obtain customer's permission to disclose the CPNI as part of the case study, which shall put the CPNI in the public domain.

Additional definitions and links to the CPNI Regulation and the Communications Act of 1934 can be found in the back of this policy.

Use of Customer CPNI which does not require Customer approval

Regulation: Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.*, local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

Regulation: If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

Regulation: Telecommunications carriers 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.

DCS Policy: Most of DCS's services fall within the VoIP services category or adjunct to basic category. With respect to products and services that fall outside of these categories, any marketing sent to those customers only uses the customer's name and e-mail address (subscriber list information) to send the communication. Therefore DCS may market all of the DCS services to customer without opt in or opt out consent having first been received. However, Customer may always elect to opt out of receiving these communications at any time by responding to the email with the communication and stating Customer wishes to opt out, calling at 1 (844) 894-1314, or by completing the opt out form available at, or by completing the opt out form available at http://www.digium.com/en/company/subscribe/mailing-list. If Customer wishes to unsubscribe from a particular marketing list Customer may do so by clicking the unsubscribe link at the bottom of the marketing email.

Regulation: A telecommunications carrier may use, disclose, or permit access to CPNI obtained from its customers, either directly or indirectly through its agents to do the following: (1) to initiate, render, bill and collect for telecommunications services or (2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

DCS Policy: DCS uses agents authorized under contract to assist DCS in initiating, rendering, billing, and collecting for telecommunications services. The agents are contractually bound with DCS to only utilize CPNI for these purposes and may use without having first received customer opt in or opt out consent. If DCS believes Customer has violated the DCS Acceptable Use Policy (a copy of which is available for viewing at http://www.digium.com/en/company/policies/dcs-acceptable-use-policy) or any other DCS terms regarding prevention of fraudulent, abusive, or unlawful use of, or subscription to the DCS services or any law regarding such then DCS will use, disclose, and permit access to CPNI to the extent necessary to protect itself, other users of DCS services, and other carriers from further fraudulent, abusive, or unlawful actions. DCS agents do market to the customers, however the marketing does not use CPNI disclosed by DCS. The DCS agents use information disclosed directly by the customer to the DCS agent and as the DCS agents are not themselves telecommunications carriers they are not restricted in using information disclosed directly to them by the customer for marketing purposes.

Additionally, DCS may disclose CPNI without customer approval if required by a Public Safety Answering Point (PSAP), i.e. emergency call takers.

When DCS is required to disclose CPNI

DCS must provide CPNI to any person designated by customer, upon receipt of an affirmative written request from customer. DCS may not encourage a customer to freeze third party access to CPNI.

DCS must provide CPNI when required by law such as through a subpoena or other request from law enforcement. If you believe DCS is required by law to disclose CPNI notify the below contact immediately.

Digium Cloud Services LLC attn.: Legal
445 Jan Davis Drive, Huntsville, Alabama 35806
legal@digium.com
256-428-6000

Federal Requirements DCS follows to protect CPNI

Establishing Password and Back- up Authentication

Regulation: Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords. To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

DCS Policy: DCS requires that the Customer create a password and select security questions which do not rely on readily available biographical or account information. The Customer may set up or reset the CPNI call-in password and security questions by signing into my.digium.com/en/user, clicking "My Account", and clicking on the managing CPNI link.

Providing CPNI over the Telephone in Response to Customer Initiated Telephone Contact

Regulation: Telecommunications carriers are prohibited from releasing CPNI to customers during customer initiated telephone contacts, except when the customer has previously established a password for their account. Otherwise, telecommunications carriers may not release CPNI except by sending it to an address of record or calling the telephone number of record.

DCS Policy: DCS only discloses CPNI over the telephone, based on customer-initiated contact, if the Customer first provides DCS with a password that is not prompted by asking Customer for readily available biographical information or account information. If the customer does not provide a password DCS will only disclose CPNI by mailing to the customer's physical or electronic address of record or by calling the customer at the telephone number of record. If the customer is able to provide CPNI to DCS during a customer initiated call without DCS's assistance only then may DCS discuss the CPNI provided by the customer.

Providing CPNI in Person

Regulation: Telecommunications carriers may provide CPNI to customers in a retail location with a valid government issued photo ID.

DCS Policy: DCS agents and DCS may disclose CPNI to a customer who at either the DCS office, any Digium Inc. location, or at the agent's or customer's premises first presents to DCS or Digium a valid photo ID matching customer's account information.

One Time Use of CPNI Requirements

Regulation: Telecommunications carriers may use oral notice to obtain limited, one time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt out or opt in approval based on the nature of the contact. The contents of the oral notice must meet all of the requirements detailed in section requirements of content of customer notices regarding CPNI except that carrier may omit the following if not relevant to the limited use for which carrier seeks CPNI: (a) need not advise customers that if they have opt out previously no action is needed to maintain opt out election, ned not advise customers they may share CPNI with their affiliates or third parties or name the entities if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party, (b) need not disclose the means by which a customer can deny or withdraw further access to CPNI as long as carriers explain to customers that the scope of approval the carrier seeks is limited to one-time use, and (c) carrier may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to CPNI for the call.

DCS Policy: DCS only discloses CPNI over the telephone, based on customer-initiated contact, if the Customer first provides DCS with a password that is not prompted by asking Customer for readily available biographical information or account information. If the customer does not provide a password DCS will only disclose CPNI by mailing to the customer's physical or electronic address of record or by calling the customer at the telephone number of record. If the customer is able to provide CPNI to DCS during a customer initiated call without DCS's assistance only then may DCS discuss the CPNI provided by the customer.

Marketing specific federal requirements DCS follows to protect CPNI

When Opt In Is Required

Regulation: Telecommunications providers must obtain opt in approval prior to disclosing CPNI to a joint venture partner or independent contractor for the purposes of marketing communications related services to the customer. A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) content of notice of this section.

DCS Policy: As of February 27, 2014 DCS current practice is not to disclose customer CPNI to joint venture partners or independent contractors for purposes of marketing communications related services to the customer, though DCS does disclose CPNI to agents as detailed in the section listing out when we may disclose CPNI without customer permission. If this policy changes prior to disclosing Customer CPNI DCS will first request opt in consent from customer to disclose CPNI which meets the notice requirements contained herein. Customer's decision to deny approval to use CPNI to market in this way will not affect the provision of services to which customer subscribes.

When either Opt In or Opt Out is required

Regulation: In order to use CPNI to market a service or product in a category of which customer does not already subscribe to or purchase telecommunications carriers must first obtain either opt in or opt out approval. If opt out is used the telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except with regard to one time use of CPNI as detailed under in the section titled One Time Use of CPNI Requirements). The contents of any such notification must comply with the requirements in the section titled Requirements of content of customer notice regarding CPNI. Telecommunications carriers must wait a 30 day minimum period of time after giving customer notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may in its discretion provide for a longer period. Carriers must notify customers as to the applicable waiting period before approval is assumed. In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification is sent. In the case of notification by postal mail the waiting period shall begin to run on the third day following the date on that the notification was mailed. Carriers which elect to use opt out mechanisms must provide notices to their customers every two years.

DCS Policy: As of 02/26/2014 DCS current practice is not to use CPNI to market a service or product in a category of which customer does not already subscribe to or purchase as all of DCS's services are categorized in a single category, VoIP services. If this policy changes before using your CPNI for the first time for this purpose, we will notify you by e—mail or regular mail. You will then have 30 days to tell us, by responding to the email with the notice, calling us at 1 (844) 894-1314 , or by completing the opt out form available at http://www.digium.com/en/company/subscribe/mailing-list , if you do not want us to use your information to offer those services. After the 30-day period has expired, DCS may use your CPNI to offer services different from those you currently receive from DCS unless you have notified us within the 30 day window that we may not use it for this purpose. Your decision to deny approval to use your CPNI to market in this way will not affect the provision of services to which you subscribe. At any time, you can change your decision by contacting via the above processes. Your decision will remain in effect unless you change it. DCS does not sell your CPNI to unaffiliated third parties.

Notification to Customer of Certain Account Changes

Regulation: Telecommunications providers must notify customers when a password, address, or other certain other account changes occur. Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

DCS Policy: DCS mails a notice to Customer's electronic or physical address of record whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, changes to customer's user profile in the online account such as name or e-mail address, or address of record is changed. The mailed notice is sent only to an address that has been associated with the customer's account for at least 30 days (except for accounts activated within the last 30 days in which case

the notice is sent to the address provided at account activation). Any such notice will not include or reveal the changed information.

Notification to Customer and Public in the event of a CPNI breach

Regulation: Telecommunications carriers must establish a notification process for both law enforcement officials and customers in the event of a CPNI breach as detailed below.

A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily 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, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at *http://www.fcc.gov/eb/cpni.*

Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below.

If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

If 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 the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

After a telecommunications carrier has completed the process of notifying law enforcement, it shall notify its customers of a breach of those customers' CPNI.

As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

DCS Policy: DCS's policy is to notify the United States Secret Service ("USSS") and Federal Bureau of Investigation ("FBI") as soon as practical, but in no event later than seven (7) business days after a reasonable determination has been made that a breach of its customer's CPNI has occurred. Notwithstanding state law to the contrary, DCS shall not notify customers of the breach until 7 full business days have passed after notification to the USSS and the FBI except if DCS 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, it will so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigation agency. DCS will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification. DCS will provide customer notifications to either the electronic or physical address of record.

However, if the relevant investigating agency determines that public disclosure or notice to customer would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct us not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify DCS when it appears that the public disclosure or notice to

affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to DCS, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by DCS.

Annual Certification

Regulation: Telecommunications carriers must file an annual certification with the FCC including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNI.

DCS Policy: DCS files the annual certification by March 1st.

Alternative Authentication regimes

Regulation: Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

DCS Policy: If DCS enters into any such contracts which fall within the above regulation which allows for an alternative customer authentication regime DCS will ensure the contract address's DCS's protection of CPNI and that the business customer has a dedicated account representative to assist with protection of CPNI.

Definitions

Account information is any information that is specifically connected to the customer's service relationship with the telecommunications carrier, including such things as an account number or any component thereof, the telephone number associated with the account or the bill's amount.

Address of record whether postal or electronic, is an address that the telecommunications carrier has associated with the customer's account for at least 30 days.

Affiliate means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with another person. For purposes of this paragraph, the term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent.

Information services means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing but does not include any use of any such capability for the management, control or operation of a telecommunications system or the management of a telecommunications service.

Interconnected VoIP providers" are companies that provide a service that: 1) enables real-time, two-way voice communications; (2)requires a broadband connection from the user's location; (3) requires Internet protocol-compatible customer premises equipment (CPE); and(4) permits users generally to receive calls that originate on the public switched telephone network and terminate calls to the public switched network.
Opt-in approval refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

Opt-out approval refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in §64.2008(d)(1) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

Readily available biographical information is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

Solicitation means the initiation of a call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods or services, which is transmitted to any person, but such term does not include a call or message (A) to any person with that person's prior express invitation or permission, (B) to any person with whom the caller has an established business relationship, or (C) by a tax exempt non-profit organization

Subscriber list information means any information— (A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format

Valid photo ID is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

Telecommunications carrier, for purposes of CPNI only, includes an entity that provides interconnected VoIP Service.

Contact information for questions and concerns regarding the policy
DCS is committed to the protection of its customers' CPNI and full compliance with the FCC's CPNI rules. Questions and/or concerns regarding this policy should be directed to DCS's CPNI Compliance Manager who may be reached by emailing legal@digium.com .

Links to Rules
The CPNI rules can be found in Title 47 Telecommunication http://www.ecfr.gov/cgi-bin/text-idx?SID=d46a98909ec54c67fde054aa9a8f4011&node=47:3.0.1.1.11.21&rgn=div6

Additional definitions from the CPNI rules can be found in the Communications Act of 1934 amended April 24, 2013 http://www.house.gov/legcoun/Comps/FCC_CMD.PDF