

Comcast Cable

Law Enforcement Handbook



internet

tv

voice

Table of Contents

Introduction.....	3
Xfinity® Voice Service	4
Xfinity Internet™	
Xfinity Cable™	
Xfinity Wi-Fi	
Xfinity Text Messaging	5
Contact Information	6
Internet, Voice & Cable TV Compliance	
Subscriber Account Identification and Related Records	8
Retention Policies	10
Types of Legal Requests.....	14
Quick Reference	19
Fees.....	21
Appendix.....	22
Attachment #1 Emergency Situation Disclosure Request	23
Attachment #2 CALEA Worksheet.....	25
Attachment #3 VPN Request Form.....	26
Attachment #4 Cable Communications Policy Act of 1984.....	28
Telecommunications Act of 1996	31

Introduction

Comcast Corporation (through its operating company subsidiaries) is the nation's leading provider of cable, entertainment, and communications products and services, currently with nearly 22.8 million cable customers, nearly 17.6 million high-speed Internet customers and over 9 million voice customers as of January 2012. More information about Comcast and its products and services is available at <http://www.comcast.com>.

Comcast assists law enforcement agencies in their investigations while protecting subscriber privacy as required by law and applicable privacy policies. The main federal statutes that Comcast must conform to when releasing subscriber information are: The Cable Communications Policy Act of 1984 ([47 U.S.C. § 551](#)); The Electronic Communications Privacy Act ([18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127](#)); Communications Assistance for Law Enforcement Act ([47 U.S.C. §§ 1001-1010](#)); and the Telecommunications Act of 1996 (particularly, [47 U.S.C. § 222](#) pertaining to customer proprietary network information or CPNI). Copies of [47 U.S.C. § 551](#) and [47 U.S.C. § 222](#) current as of the date of this handbook are included in Attachment #4 for reference. Comcast also complies with other applicable state and federal laws.

Comcast's primary goal is to provide *timely* and *accurate* responses to all law enforcement and legal requests. Comcast has highly qualified personnel who are responsible for complying with legal requests made of Comcast. Unless otherwise required by the request, Comcast's goal is to provide a response within eight to ten working days of each request. If necessary, Comcast employees can offer testimony in support of subscriber identifications at reasonable costs. However, Comcast encourages the use of affidavits in order to avoid personal court appearances and costs wherever possible.

Note: This Handbook is provided for informational purposes only. Comcast expressly reserves the right to add, change, or delete any information contained in this Handbook at any time and without notice. Furthermore, Comcast reserves the right to respond or object to, or seek clarification of, any legal requests and treat legal requests for subscriber information in any manner consistent with applicable law.

Xfinity® Voice Telephone Service



voice

Comcast's IP-enabled phone service, branded Xfinity Voice, is a residential, primary line service that offers digital quality and includes all of the features that customers expect from their phone service in addition to new, enhanced features such as the ability to check voice mail online. Comcast also offers commercial telephone services, branded Comcast Business Class (formerly Workplace Digital Voice), and has a very small number of switched-circuit (non-IP enabled) commercial Comcast Digital Phone customers.



internet

Xfinity Internet™

Xfinity Internet provides a constant connection to the Internet and offers download speeds up to 50 Mbps and upload speeds up to 10 Mbps depending on the location of the Comcast market. In addition, Comcast gives subscribers up to seven unique email accounts accessible from any Internet-connected computer. Note: If law enforcement needs data regarding a wireless connection that appears to be Comcast related, please contact the LRC for further instructions.



tv

Xfinity TV

Xfinity TV television service provides customers with the best programming and broadcast networks, as well as movies, sports, and other events. On Demand and Digital Video Recorder options further enhance customers' ability to experience all of the programming provided over this service.

Xfinity Wi-Fi

Xfinity Wi-Fi is provided to all Xfinity Internet subscribers as a value added service and may be accessed by a subscriber using any device that is Wi-Fi capable. Also, limited Wi-Fi service is provided to non-subscribers through a sponsored access program with other internet service providers for limited periods of time. Comcast can provide historic Internet Protocol assignment and session information for a period of 180 days for Xfinity internet users.

Xfinity Text Messaging

Xfinity text messaging is a service offered to all unlimited Xfinity Voice subscribers, leveraging the Comcast network to send and receive text messages from a home computer or smart phone with an installed Xfinity text messaging application. Comcast can provide historic text message sessions by the originating and terminating device identification and telephone number for a period of 30 days.

Contact Information

Legal Compliance (Subpoena, Search Warrant, Court Order):

Comcast's Legal Response Center is located in Moorestown, New Jersey and is responsible for matters involving subscriber information for Xfinity Internet services, telephone services (Xfinity Voice) and television services (Xfinity TV). The Legal Response Center is also responsible for matters involving Comcast's Business Class commercial Internet, voice, and cable services.

Comcast uses CT Corporation (866-925-9916) as a registered agent which can accept the submission of legal requests *for civil matters*. If, as a law enforcement officer, your legal request *must* be served in your state of origin you may contact CT Corporation's local office for submission or the Legal Response Center for a list of CT Corporation's offices. If you may serve legal process outside of your state of origin, Comcast prefers service of legal requests via facsimile directly to the LRC (see contact information below).

Routine Requests and Information 866-947-8LRC

- Option 1. Law Enforcement
- Option 2. Subscriber Requests Annoyance / Harassment
- Option 3. Civil Process

Please listen to the voice mail prompt and provide a detailed message. All calls will normally be returned within one business day.

E911- ANI / ALI Failures (Only) 800-839-6707

Imminent Loss of Life or Serious Bodily Injury 877-249-7306

Emergency disclosure form will be required for the release of any subscriber information

Fax Number 866-947-5587

Fax for Service of Process and Other Documents

Mailing Address
650 Centerton Road
Moorestown, NJ 08057
Attn: Custodian of Records

Subscriber Account Identification

Subscriber Account Identification and Related Records

Upon receipt of a properly executed, valid and statutorily authorized legal request that is timely submitted (within 6 months from the date of the incident), under Comcast's current data retention policies for residential dynamic IP addresses, Comcast can usually supply the subscriber's name, address, telephone number, account number, account balance, and payment information and, depending on the Comcast service(s), to which services they subscribe.

For identification based upon telephone number:

- Comcast can only provide account information on telephone numbers for which we currently or have historically provided service. The current company which provides service to a specific telephone number can be obtained by contacting Neustar. Neustar is the company which serves as the FCC-appointed administrator of the North American Numbering Plan (NANP). To obtain provider information from Neustar, you must first have an account active at Neustar. Neustar's website is www.neustar.biz and the NANP website is <http://www.nanpa.com/>.

For identification of Internet Protocol Addresses

-Before sending a request, please confirm that the IP address is assigned to Comcast. This can be accomplished by visiting <http://ws.arin.net/whois> or <http://www.ip2location.com/free.asp> and inputting the IP address.

- Because Comcast's system of allocating IP addresses uses Dynamic Host Configuration Protocol (DHCP), its residential subscribers are not assigned a single, constant or static IP address. Instead, a dynamic IP address is assigned and has the potential to change several times throughout the course of service. As a result, it is necessary in all requests for subscriber information linked to a specific IP address that you supply the **specific date and time of the incident when an IP address is involved.**
- Comcast currently maintains its dynamic IP address log files for a period of 180 days. If asked to make an identification based upon a dynamic IP address that was used more than 180 days prior to receipt of the request, Comcast will not have information to provide. (Note: Comcast can process preservation requests received within 180 days after the alleged date of usage as outlined in this Handbook.)
- **For identification based upon an email address:**

All residential email address accounts issued through Comcast High Speed Internet will end in *comcast.net* (i.e. JohnDoe@comcast.net). If the residential email account ends in any other domain (i.e. @hotmail.com or @yahoo.com), Comcast will not have

information responsive to the request.

For identification based upon a person's name:

- Comcast cannot identify a subscriber based upon a name alone. It is necessary to include the street address, account number, phone number or other identifiable information where it is believed the individual receives service. It may be possible in some cases to identify a subscriber based on name and a city and state (with no street address).
- Comcast will only respond to a request for identification based on the name exactly as it is written on the request. For example: if the request asks for information relating to *James Doe* in Springfield and Comcast's records reveal a *J. Doe* and/or a *Jim Doe* in Springfield, Comcast will not have information responsive to the request or may require additional legal process to determine if it has responsive information. If initials or nickname are used you should add a request for those variations of the name in your legal request.

For identification based upon a street address:

- It is necessary to provide an entire street address. In the request, please supply the house or apartment number, the street name, the city, state, and the zip code of the location you have targeted.
- Over a length of time it is possible that Comcast has supplied service to multiple customers at the same address. Therefore, it is necessary to narrow a search for customer identity to a specific period of time.

For identification based upon a Comcast account number:

- Please provide a complete account number. Legal requests with incomplete account numbers will not result in successful identifications.

For Identification based upon a specific payment method:

- For bank account search provide the DDA and Routing number
- For credit card, complete credit card number and the approximate date the payment was applied to the card, provide the dollar value and institution which issued the card.

Retention Policies

Retention Policies – Xfinity Internet

IP Address Information

- Comcast currently maintains dynamic IP address log files for a period of 180 days. If Comcast is asked to respond for information relating to an incident that occurred beyond this period, we will not have responsive information and cannot fulfill a legal request. (Comcast can process and respond to preservation requests received within 180 days after the alleged date of usage as outlined in this Handbook.)

Web mail Account Information for email contents and attachments

- Xfinity Internet customer accounts are currently provided the option of having up to seven separate email accounts. Customers may choose to not use Comcast email at all, instead using another provider's email such as Gmail or Yahoo Mail, or use those email services in addition to a Comcast email account. In cases involving another entity's email service or account, Comcast would not have any access to or ability to access those other customer email accounts in response to a legal request. Legal requests seeking the contents of emails or attachments to emails should also be aware of the following:

- When customers use Comcast email, they may use the Comcast Webmail service. This permits customers to access their email from any Internet connected computer. In this case, the contents of emails are stored on Comcast's email servers where they may be produced in response to a legal request if they have not been deleted by the customer.

- Customers may also use an email client program like Outlook Express, Outlook, Vista mail or Eudora to move or "pop" email from Comcast's email servers to their own personal computers. In those cases, emails may be deleted from Comcast's email servers and if so, they are not accessible to Comcast.

- Customers may also use Webmail and an email client program and leave emails on Comcast's email servers as well as copy, not move, them to their personal computers. In these cases, emails that remain on Comcast's email servers may be produced in response to a proper legal request if they have not been deleted by the customer.

Comcast's Webmail service permits customers to change their email deletion policies, but the current default settings are described below.

- Inbox *(Read Mail – No automatic deletion policy)*
(Unread Mail – 45 day retention period)

- Trash *(Read Mail – 1 day retention period)*
(Unread Mail – 1 day retention period)

- Sent Mail *(Read Mail – 30 day retention period)*
(Unread Mail – 30 day retention period)

- Screened Mail *(Read Mail – 3 day retention period)*
(Unread Mail – 3 day retention period)

- Personal Folders *(Read/Unread – No deletion policy)*

- Popped Mail *(Deleted immediately from web mail servers)*

Note: Xfinity Internet customers can set their own preferences for certain web mail deletion or retention; thus, individual customer accounts may have settings that differ from those above. For more information about Comcast Webmail settings, see:

<http://customer.comcast.com/Pages/FAQViewer.aspx?Guid=e9278638-56c6-4010-a24a-767e1b9caee5>.

Retention Policies – Xfinity Voice

Accessing Call Detail Records

- Comcast maintains historical call detail records for our Xfinity Voice telephone service for no less than two years. This includes local, local toll, and long distance records. In limited instances, older records may be available but will require additional time and resources to retrieve.

Accessing Account Records

- Account records are generally stored for approximately two years. If the account has an outstanding balance due, records may be retained for a longer period of time.

NOTE: In situations where a Comcast subscriber is cooperating with law enforcement on an investigation or case, subscribers have direct access themselves to their own records as follows. Xfinity Voice is an un-metered service and we currently provide to subscribers 90 days of call detail records going back from the current date as a customer convenience through the Xfinity Connect Center, accessible via Comcast.net. This includes all detail, including local calls. To obtain these records, the subscriber simply logs into the website www.digitalvoice.comcast.net. Subscribers can also access one year's worth of records that would be considered traditional toll records through the Xfinity Voice Details in the View My Bill section of Comcast.com. These records would only include outbound calls terminating outside the customers local rate center, international calls and directory assistance calls.

All requests to Comcast for call detail records require legal process such as a subpoena (law enforcement) or court order (civil) to obtain. There is a fee for the research and processing of civil legal demands requesting call detail records.

Legal Requests

Types of Requests

Generally, the following information, when available to Comcast, can be supplied in response to the types of requests listed below. Each request is evaluated and reviewed on a case by case basis in light of any special procedural or legal requirements and applicable laws. The following examples are for illustration only.

Special Note related to our cable television service only: the Cable Act requires Comcast, as a cable operator, to only disclose personally identifiable information to a governmental entity *solely* in response to a court order (and not, for example, a subpoena) in a criminal proceeding or with the subscriber's express written consent. When the request is related to an account that has cable TV service only the Cable Act requires that the cable subscriber be afforded the opportunity to appear and contest in a court hearing relevant to the court order any claims made in support of the probable cause court order. At the proceeding, the Cable Act requires the governmental entity to offer clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case. See 47 U.S.C. § 551(h). Once this opportunity has been afforded the subscriber, and the court enters an appropriate order, then Comcast may respond.

If, however, your investigation includes the fraudulent use of a credit card or identity theft, please contact the Legal Response Center and we will discuss options for obtaining basic cable television account information in response to a subpoena or court order without a hearing. If you do not have legal process but need information preserved, please refer to the Preservation section.

Important Note on Email Communications (Contents): In most instances, the contents of email communications in storage for 180 days or less may *only* be produced in response to a state or federal warrant (unless it can be demonstrated that the email has been opened *and* is not being kept for purposes of backup protection) and in such situations may be done so without notice to the subscriber. For email communications in storage for over 180 days, a warrant may also be used, as well as court orders and valid statutorily authorized administrative subpoenas may be used, but use of these two alternative methods generally requires notice to the subscriber by law enforcement.

Child Exploitation

Comcast will make information available to the National Center for Missing and Exploited Children as required by 18 U.S.C. § 2258A.

Court Order or Search Warrant (both signed by a Judge)

Law enforcement agencies are eligible to obtain subscriber identification including:

- 1) Subscriber's name
- 2) Subscriber's address
- 3) Length of service including start date
- 4) Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address.
- 5) Subscriber's email account names
- 6) Call Detail (records of local and long distance calling connections)
- 7) Means and source of payment for such service (including any credit card or bank account number).
- 8) The content of certain of the subscriber's email communications can be provided if stated within the order and with notice (refer to Preservation Request section).

Emergency Disclosure

18 U.S.C. § 2702(b)(8) and § 2702(c)(4) contain provisions for the expedited release of subscriber information in situations where there is an immediate danger of death or an immediate risk of serious bodily injury. Law enforcement agencies need only complete Comcast's Emergency Situation Disclosure Request form (Reference Attachment #1) and they will receive accelerated subscriber identification. Proper legal process must be submitted after the emergency has subsided. The emergency number to contact LRC to initiate this process is **877-249-7306**. *This number is only for emergencies.*

Foreign Intelligence Surveillance Act of 1978

Title 50 U.S.C. §§ 1801-1862 and new §§ 105 A and B submissions to Comcast should be coordinated with the FBI field office in Trenton, NJ or Philadelphia, PA. A Special Agent will be tasked to hand deliver the request to Comcast. Upon receipt, Comcast will handle all documents with the appropriate care and security as required by law.

Grand Jury, Trial, or Statutorily Authorized Administrative Subpoena

Law enforcement agencies are eligible to receive subscriber identification (except cable TV only subscribers) including items (1-7) without notice to the subscriber:

- 1) Subscriber's name
- 2) Subscriber's address
- 3) Length of service including start date
- 4) Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address
- 5) Subscriber's email account names;
- 6) Call Detail (records or local and long distance calling connections)
- 7) Means and source of payment for such service (including any credit card or bank account number); and
- 8) In certain instances, email communications older than 180 days *with advance notice to subscriber by law enforcement.*

(preservation)

Judicial Summons

Law enforcement agencies are eligible to receive subscriber identification including:

- 1) Subscriber's name
- 2) Subscriber's address
- 3) Length of service including start date and end date.
- 4) Subscriber's telephone number, instrument (model or serial) number or other subscriber number or identity, including a temporarily assigned network address.
- 5) Subscriber's email account names;
- 6) Call Detail (records of local and long distance calling connections)
- 7) Means and source of payment for such service (including any credit card or bank account number).

National Security Letter

All National Security Letters should be coordinated with the FBI field office in Trenton, NJ.

Pen Register / Trap and Trace Device

Title 18 U.S.C. § 3123 provides a mechanism for authorizing and approving the installation and use of a pen register or a trap and trace device pursuant to court order. All orders must be coordinated with the LRC prior to submission to Comcast. Law enforcement will be asked to agree to reimburse Comcast's reasonable costs incurred to purchase and/or install and monitor necessary equipment as defined in section labeled "Reimbursement Fees".

Preservation Request/ Backup Preservation Request

Title 18 U.S.C. §§ 2703(f) and 2704 provide a mechanism for law enforcement agencies to require Comcast to preserve subscriber data *already in its possession as a "snapshot" at a specific time, and not on an ongoing, continual basis*, until an appropriate legal order is obtained. No information can be released until Comcast receives a formal and valid legal request. The information will be retained for ninety days upon which, if no valid legal request is made, or no authorized ninety day extension is sought, the information will be permanently purged. If an extension is sought, the information will be retained for an additional ninety days upon which, if no valid legal request is made, the information will be permanently purged. If law enforcement desires to capture ongoing real-time data during the period of time between the preservation request and the obtaining of legal process, a valid Order for wiretap or pen register must

be presented.

Wiretaps and Interception of Communications

Title 18 U.S.C. § 2510 provides a mechanism for authorizing and approving the interception of a wire, oral, or electronic communication pursuant to court order. All orders must be coordinated with the LRC prior to submission to Comcast. Law enforcement will be asked to agree to reimburse Comcast's reasonable costs incurred to purchase and/or install and monitor necessary equipment. Please refer to section entitled "Reimbursement Fees".

Quick Reference

The checklist below is a quick reference guide for producing a valid legal submission to Comcast and will help reduce processing time associated with overly broad or erroneous submissions.

- ✓ Verify that the phone number, IP address or e-mail address is registered to Comcast. For phone numbers, follow the instructions referenced earlier in Guide. For IP addresses, go to www.ARIN.net or <http://www.ip2location.com/free.asp>. Comcast residential e-mail addresses end in *@comcast.net*.
- ✓ Limit your request to no more than five telephone numbers, IP addresses or email address elements per individual legal document. This will allow us to manage your request more effectively and provide a quicker response.
- ✓ Include the IP address, email address, street address, phone number and all other pertinent information that will allow Comcast to adequately respond to your request.
- ✓ Your request should specifically state what you require Comcast to provide; we do not make assumptions about the information being sought and will not provide “extra” information.
- ✓ Do not use language which is specific to one company. Use general terms such as “call detail records” rather than an acronym for call detail records that one company might use and another may not.
- ✓ Include date and time of all incidents including seconds and time zone, i.e. 12 December 2011 @ 06:13:21 EST. State on your request specifically what you require Comcast to provide and be sure it conforms to what Electronic Communications Privacy Act permits; overly broad requests often require additional follow up and may slow response time.
- ✓ Ensure that you have made the required certifications and complied with all applicable substantive and procedural requirements under the particular statutes or regulations authorizing your request. If your email address is provided on the initial legal submission, Comcast will email you a confirmation number and tracking information for your convenience.

- ✓ Ensure that you completely explain the nature and circumstances of any potential serious injury or death to justify an emergency disclosure.

Ensure that all of your contact information is correct. Comcast will return legal requests via fax unless otherwise requested in the subpoena or order. We can provide CD, USPS, or overnight mail but we will not provide data via email due to lack of security/privacy.

Reimbursement Fees

The Legal Response Center does not charge for responses to legal process served by a government entity involving child exploitation. In all other situations, Comcast reserves the right to seek reimbursement for processing and responding to all legal process as permitted by law. Our policy is to discuss reimbursement with the requesting party before we incur any costs. However, in time-sensitive situations we may have to discuss costs after the fact.

Costs for the implementation of a Court Ordered Pen Register/Trap and Trace complaint/FISA requiring deployment of an intercept device are as follows:

- Intercept: \$1,100.00 initial Comcast start-up fee (including the first month of intercept service or any part thereof) and \$850.00 per month for each subsequent month or any part thereof in which the original order or any extensions of the original order are active.
- Requesting Law Enforcement Agencies must complete a CALEA Worksheet (See Attachment 2) providing detailed billing information and point of contact.
- Billing will occur at the completion of the interception period. If this period exceeds ninety (90 days) billing will occur in 90 day intervals.
- Call Detail records released in response to an ongoing Court order: \$150.00 per week for one time per week delivery of incoming and outgoing call detail records for the duration of the original order and any extension of the original order. More frequent delivery of call detail records is an additional \$50.00 per delivery.
- For all requests that necessitate Comcast employee travel for installation, Comcast asks the requesting agency to reimburse Comcast for all reasonable, documented travel and related expenses.

Appendix

Attachment #1

Emergency Situation Disclosure Request by Law Enforcement

Please complete this form to assist the Comcast Legal Response Center in exercising its discretion to disclose information to your law enforcement agency or governmental entity pursuant to 18 U.S.C. § 2702(b) or § 2702(c). If you are unable to answer a specific question in writing, please call 877-249-7306. Failure to provide complete answers to any question may result in a delay of the disclosure of the requested information or Comcast choosing not to make any disclosure.

1. What is the nature of the emergency involving immediate danger of death or serious physical injury to any person?

2. Whose death or serious physical injury is threatened?

3. What is the pending nature of the threat? Do you have information that suggests that there is a specific deadline before the act indicated in Question 1 will occur? (For example, tonight, tomorrow, at noon.)

4. Why is the required disclosure process pursuant to 18 U.S.C. § 2703 or another applicable law insufficient or untimely as set forth by the deadline indicated in Question 3?

5. What specific information in Comcast's possession are you seeking to receive on an emergency basis? (Please be specific such as name, street address, telephone, or e-mail contents; do not respond by asking for everything or all account information as that will likely delay processing of the request.)
 - **Address Identification** – You must provide the IP address and a specific date & time on this form
 - **Email Identification** – You must provide the Comcast email address on this form
 - **Telephone # Identification** – You must provide the telephone number and a specific date & time on this form
 - **Physical Address Identification** – You must provide the complete physical address on this form

If Comcast makes an emergency disclosure to your law enforcement agency or governmental entity pursuant to 18 U.S.C. § 2702(b) or § 2702(c), you agree to provide Comcast with a formal order to provide your agency with the information provided pursuant to this request within 72 hours. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Printed Name

Signature

Title

Signature of Supervisor

Name of Agency/Governmental Entity

Printed name of Supervisor

Address

Address

Telephone number

Fax number

Please return this form to fax # 856-638-4531

Attachment #2

National IP Engineering & Operations



**Legal Response Center
CALEA Worksheet**

Please complete with all relevant information and fax with each court order to 866-947-5587

Surveillance Order: (Attach)

Date of Order _____
 Date Served _____
 Termination Date _____
 Case/Docket# _____
 New or Extension? _____
 Deactivation? _____

Target Information:

Name(s) _____
 Phone _____
 IP Address _____
 Email Address _____
 Physical Address _____
 MAC Address _____
 Other _____

LEA Information:

Case Agent/Officer _____
 Agency/Department _____
 Case Agent _____
 Contact Info. _____
 Technical Contact _____
 Contact Info w/email _____
 Agency _____
 Billing Contact _____
 Billing Name/Address _____

Billing Ref. No. _____

Surveillance Type:	Comcast Digital Phone <input type="checkbox"/>	Pen Register/Trap Trace <input type="checkbox"/>
		Wiretap/Title III <input type="checkbox"/>
		FISA/Title 50 <input type="checkbox"/>
	Comcast HSI <input type="checkbox"/>	Header Information <input type="checkbox"/>
		Full Content <input type="checkbox"/>
	Email (@comcast.net) <input type="checkbox"/>	Header Information <input type="checkbox"/>
		Full Content <input type="checkbox"/>

LEA Technical Requests:

Attachment #3

National IP Engineering & Operations



**Legal Response Center
VPN Request Form**

Use this form to request the establishment of a LEA Interconnect VPN for CALEA requirements. Upon completion, please fax to 866-947-5587 along with court order.

Requests typically take between 10 and 15 business days to complete. Requests requiring complex engineering or other unforeseen circumstances may require additional time to complete. Please plan accordingly.

Please provide as much detail as possible. Answers that are incomplete or ambiguous may delay your request.

Provide the name and address of the Law Enforcement Agency where the VPN will be terminated:

LEA	
Address	
City, State, Zip	

Provide the information for the contact at the LEA to coordinate the VPN setup:

Name	
Telephone	
Email	

Specify the type of VPN gateway that will be used at the LEA to terminate the VPN:

Make	
Model	
Software Ver.	

Are there requirements from the LEA on the type of VPN gateway to be used at Comcast?

--



National IP Engineering & Operations

**Legal Response Center
VPN Request Form**

Provide the following technical information from the LEA:

IP Address of VPN Gateway	
Encryption Domain (ie. local network)	
IP Address of Collection Server	

These are the Comcast recommended VPN settings:

Phase 1 SA		Phase 2 SA	
Authentication	Preshared Key	PFS	None
DH Group	Group 2	Encapsulation	ESP
Encryption	AES (128 bits)	Encryption	AES (128bits)
Hash	SHA-1	Hash	SHA-1
Lifetime	86400 seconds	Lifetime	3600 seconds

If the LEA requirements differ, please specify their requirements (*subject to approval from Comcast Security Engineering*):

Phase 1 SA		Phase 2 SA	
Authentication		PFS	
DH Group		Encapsulation	
Encryption		Encryption	
Hash		Hash	
Lifetime		Lifetime	

Please provide Communications Path for LEA traffic:

Note: The following destination ports are preferred: CCC/UDP 9000; CDC/TCP Port 43000

Traffic Source		Traffic Destination		
Description	Source IP Address	Description	Destination IP Address	Port and Protocol

Attachment #4

Statutory Authority

Cable Communications Policy Act of 1984, 47 U.S.C. § 551

- (a) Notice to subscriber regarding personally identifiable information; definitions
- (1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of--
- (A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;
 - (B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;
 - (C) the period during which such information will be maintained by the cable operator;
 - (D) the times and place at which the subscriber may have access to such information in accordance with subsection (d) of this section; and
 - (E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

- (2) For purposes of this section, other than subsection (h) of this section--
- (A) the term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons;
 - (B) the term "other service" includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and
 - (C) the term "cable operator" includes, in addition to persons within the definition of cable operator in section 522 of this title, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.
- (D) Collection of personally identifiable information using cable system
- (1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.
- (2) A cable operator may use the cable system to collect such information in order to--
- (A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or
 - (B) detect unauthorized reception of cable communications.

(C) Disclosure of personally identifiable information

- (1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.
- (2) A cable operator may disclose such information if the disclosure is--
 - (A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;
 - (B) subject to subsection (h) of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed;
 - (C) a disclosure of the names and addresses of subscribers to any cable service or other service, if--
 - (i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and
 - (ii) the disclosure does not reveal, directly or indirectly, the—
 - (iii) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or
 - (iv) the nature of any transaction made by the subscriber over the cable system of the cable operator; or
 - (D) to a government entity as authorized under chapters 119, 121, or 206 of Title 18, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.

(d) Subscriber access to information

A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.

(e) Destruction of information

A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) of this section or pursuant to a court order.

(f) Civil action in United States district court; damages; attorney's fees and costs; nonexclusive nature of remedy

- (1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.

- (2) The court may award--
 - (A) actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;
 - (B) punitive damages; and
 - (C) reasonable attorneys' fees and other litigation costs reasonably incurred.
- (3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

(g) Regulation by States or franchising authorities

Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.

(h) Disclosure of information to governmental entity pursuant to court order

Except as provided in subsection (c)(2)(D) of this section, a governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order--

- (1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and**
- (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.**

Telecommunications Act of 1996, 47 U.S.C. § 222

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents--

- (1) to initiate, render, bill, and collect for telecommunications services;
- (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;
- (3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

- (4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title)--
 - (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
 - (B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
 - (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use wireless location information

For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to--

- (1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title), other than in accordance with subsection (d)(4) of this section; or
- (2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (i)(3)(A) [\[FN1\]](#) of this section (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) Definitions

As used in this section:

- (1) Customer proprietary network information

The term "customer proprietary network information" means--

- (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;

except that such term does not include subscriber list information.

(2) Aggregate information

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term "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.

(4) Public safety answering point

The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) Emergency services

The term "emergency services" means 9-1-1 emergency services and emergency notification services.

(6) Emergency notification services

The term "emergency notification services" means services that notify the public of an emergency.

(7) Emergency support services

The term "emergency support services" means information or data base management services used in support of emergency services.

[\[FN1\]](#) So in original. Probably should be "(h)(3)(A)".