COMMITTEES

NATURAL RESOURCES
RANKING DEMOCRAT

ENERGY AND COMMERCE

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836

DISTRICT OFFICES:
5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900

http://markey.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515–2107

May 2, 2012

Mr. Randall F. Stephenson
Chairman, President and Chief Executive Officer
AT&T
208 S. Akard St.
Dallas, TX 75202

Dear Mr. Stephenson:

According to a recent article in The New York Times ("Police Are Using Phone Tracking as a Routine Tool", April 1, 2012), law enforcement departments routinely track mobile telephones, often with little or no judicial oversight. The article also describes how wireless carriers, while responding to law enforcement requests for consumer information, sometimes charge police departments for such services, from providing the location of mobile phones to full-scale wiretapping.

The practice of cell phone tracking raises a number of legal, constitutional, and privacy questions. According to 5,500 pages of internal records obtained by the American Civil Liberties Union from 205 police departments nationwide, a number of departments "claim broad discretion to get the records on their own" without any judicial orders, as described in the report above. Furthermore, a recent Supreme Court ruling that found the warrantless use of GPS devices to track suspects unconstitutional brings to light questions about the standards for cell phone tracking explained in The New York Times story. I am deeply concerned about possible privacy intrusions, particularly in the absence of consumer knowledge or consent, or judicial oversight.

The Times report also explores how mobile phone companies may profit from selling their customers' personal information to law enforcement. The article explains, "The practice has become big business for cell phone companies, too, with a handful of carriers marketing a catalog of 'surveillance fees' to police departments to determine a suspect's location, trace phone calls and texts or provide other services."

As a Co-Chair of the Congressional Bi-partisan Privacy Caucus, I ask that you provide answers to the follow questions:

1. Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text messages, and full-scale wiretapping?

a. How many of these requests did your company fulfill and how many did it deny?

b. If it denied any requests, for what reasons did it issue those denials?

2. What protocol or procedure does your company employ when receiving these requests?

    a. Do you consider whether law enforcement has obtained a warrant to obtain this information?

    b. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?

3. Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?

4. How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?

5. The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?

6. Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping)?

    a. Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?

    b. Please include any written schedule of any fees that your company charges law enforcement for these services.

7. Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.

Thank you for your attention to this important matter. Please provide responses to these questions no later than May 23, 2012. If you have any questions, please have a member of your staff contact Joseph Wender at 202-225-2836.

Sincerely,

Edward J. Markey
Co-Chairman
Congressional Bi-partisan Privacy Caucus

at&t

Timothy P. McKone
Executive Vice President
Federal Relations

AT&T Services, Inc.
1133 21st Street, NW
Suite 900
Washington, DC 20036

T: 202.463.4144
F: 202.463.4183
tm3703@att.com

May 29, 2012

The Honorable Edward J. Markey
United States House of Representatives
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Congressman Markey:

I am responding to your letter to Randall Stephenson, dated May 2, 2012, related to a recent article in the New York Times raising concerns about law enforcement tracking of mobile telephones.

AT&T takes seriously its responsibilities to simultaneously protect our customer's privacy while cooperating with law enforcement. As we have stated many times in filed testimony, in letters to you and other legislative offices, and in communicating with our own customers, the protection of customer privacy is fundamental to the way we do business everyday. Simply put, we do not sell our customers' personal information to law enforcement. As explained in more detail below, we are required by state and federal laws to respond to appropriate law enforcement subpoenas, warrants, court orders and other legal processes. In addition, we are authorized by law to provide location and other information to public safety personnel for purposes of responding to 911 calls and other emergency circumstances when warranted.

AT&T makes every effort to explain these requirements to our customers. Our Privacy Policy makes very clear that we will provide personal information to governmental agencies:

- To comply with court orders, subpoenas, lawful discovery requests and legal and regulatory requirements;

- To provide information regarding the caller's location to a public safety entity when a call is made to 911; and

- To notify or respond to a responsible governmental entity if we reasonably believe, based on information provided by law enforcement personnel, that an emergency involving immediate danger of death or serious physical injury to any person requires or justifies disclosure without delay.

AT&T does not respond to law enforcement without receipt of appropriate legal process. When the law requires a warrant for disclosure of customer phone usage information, AT&T requires that a warrant be provided – as is also the case for court orders, subpoenas or any other form of legal process.

AT&T also plays a vital role in assisting 911 operators to quickly dispatch law enforcement and emergency services in response to customer calls. AT&T responds to approximately 230 emergency requests (also referred to as "exigent requests") per day, including calls from more than 8300 Public Safety Answering Point 911 centers (PSAPs) around the country and from law enforcement agencies working on kidnappings, missing persons, attempted suicides and similar emergencies. Information is provided to PSAPs immediately upon verification that we are, in fact, dealing with a legitimate PSAP. All other requests for exigent information require law enforcement to sign a certification form confirming that the information is required to deal with an emergency involving immediate danger of death or serious physical injury to a person. The certification form must be signed and returned to AT&T before any information is provided to the law enforcement officer.

AT&T does not "market" the provision of its customer's phone usage information to law enforcement. AT&T employs more than 100 full time workers and operates on a 24x7 basis for the purpose of meeting law enforcement demands. AT&T's charges are intended to recoup at least a portion of our costs incurred in providing these required responses, and we believe we fall far short of our actual costs. For example, the scope of providing CALEA compliance alone is broad, and touches so many different areas within our company, which makes it virtually impossible to capture those costs. And, AT&T imposes no charges for handling exigent requests, from either PSAPs or law enforcement.

While your letter focuses on wireless carriers, it is important to note that wireless carriers are only one of many potential sources of location information. As explained in our April 22, 2011 response letter to you and Rep. Barton, there are situations in which AT&T has no role in the provision of location-based service to the customer. For example, AT&T customers may utilize location-based services from third-party sources that are not in any way affiliated with AT&T. Those providers may derive the location of the customer's device directly from the handset, or may obtain it by partnering with location providers who, in turn, obtain location from use of GPS, Wi-Fi hotspot mapping, reverse-engineered cell tower ID information, and other available mechanisms. In addition, many mobile applications capture information (like text messaging and call detail information) that once was in the sole purview of telecommunications services providers. The information available through these sources is not obtained from or available to AT&T (or any other carrier), but can be every bit as detailed and comprehensive as any carrier information.

Against this backdrop, AT&T responds as follows to your letter seeking information-related to AT&T's responses to law enforcement requests for individual AT&T customer wireless phone usage information, responses to your questions are provided below.

1. **Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text messages, and full-scale wiretapping?**

   a. **How many of these requests did your company fulfill and how many did it deny?**

   ANSWER: Approximate request numbers are provided in the table below.

TYPES OF REQUEST	2007	2008	2009	2010	2011
Subpoenas (Criminal)	63,100	76,300	75,400	98,500	131,400
Orders/Warrants	36,900	39,500	40,300	37,300	49,700
Rejected Surveillance Orders	425	560	630	740	965
Exigent Requests (PSAPs)	23,200	31,600	39,600	45,600	65,500
Exigent Requests (Non-PSAPs)	1,800	3,500	5,500	8,100	13,800

   To keep these numbers in perspective, AT&T serves over 103,200,000 wireless customers (in 2007, by contrast AT&T served just over 70,000,000 wireless customers). In 2011, assuming each request was for a different individual subscriber, the total number of law enforcement requests for individual wireless phone usage information impacted approximately 0.25% (or, stated differently, one quarter of one percent) of AT&T's wireless customer base. We also provide wireless services throughout the 50 states and Puerto Rico, which means our service footprint falls within the jurisdiction of tens of thousands of federal, state, county and local law enforcement agencies, as well as more than 8300 PSAPs.

   b. **If it denied any request, for what reasons did it issue those denials?**

   ANSWER: AT&T rejects requests for information about customer phone usage when the form of process received is not appropriate for the type of information requested, or when there is some form of procedural defect sufficient to cause the request to not meet legal requirements.

   For example, law enforcement may attempt to obtain information using a subpoena when a court order is required – such a request would be rejected. A request also may be rejected because it is defective in form – i.e., the order does not contain a signature, fails to include the subject of the request, includes a number or name that does not match AT&T's records, etc. AT&T, however, only keeps records on the numbers of rejected surveillance (i.e., pen register or wiretap) orders. Accordingly,

the number of rejected surveillance orders provided in response to Question 1(a) above understates the total number of rejected law enforcement requests.

Based on the total number of rejected surveillance requests reflected in our response to Questions 1 (a) above, AT&T rejected approximately 18 law enforcement surveillance (pen register/wiretap) requests a week in 2011.

2. **What protocol or procedure does your company employ when receiving these requests?**

ANSWER: AT&T processes requests that satisfy applicable requirements for response. Those that do not satisfy applicable requirements are rejected. AT&T provides a written explanation for the rejection to the submitting law enforcement agency. The law enforcement agency may then file a corrected request or pursue resolution through the court system.

a. **Do you consider whether law enforcement has obtained a warrant to obtain this information?**

ANSWER: Yes. AT&T will not respond to a request for information that requires a warrant unless a warrant is provided.

b. **Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking request? If yes, what are the distinctions?**

ANSWER: Yes. Non-emergency tracking requests require a search warrant or probable cause order. Before responding to emergency requests, AT&T requires law enforcement to provide a written description of the emergency, to certify the facts are true, and that they constitute an emergency involving danger of death or serious physical injury to a person, requiring disclosure without delay.

The certification must be signed and submitted to AT&T before AT&T will provide the requested information. If AT&T determines that a particular request does not fit the criteria for an emergency response, the requesting law enforcement agency is advised that the information cannot be provided without legal process.

3. **Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?**

   ANSWER: AT&T has not encountered any misuse of cell phone tracking by police departments. As described above, emergency requests require certification from law enforcement personnel; non-emergency requests require a warrant or court order. AT&T responds to the requests for information as described above. AT&T has no information on how law enforcement uses the data.

4. **How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?**

   ANSWER: AT&T has more than 100 full time employees specifically devoted to receiving, reviewing and responding to law enforcement requests submitted by federal, state, county and local law enforcement agencies, departments and organizations, including PSAPs and special districts (transit police, park police, etc.), throughout the 50 states and Puerto Rico.

5. **The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?**

   ANSWER: AT&T is required by law to cooperate with police departments that make lawful requests for information. AT&T does not know whether the police departments to which it has lawfully provided information own their own tracking equipment.

6. **Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping)?**

   ANSWER: In some cases, AT&T is compensated for the cost of collecting and submitting customer phone usage information to law enforcement in response to lawful law enforcement requests for that information. Approximate totals for the amount of money received by AT&T in each of the last five years are provided in the table below. As noted in the introduction to this letter, we do not believe our revenues in this area cover our actual costs. AT&T's price list for providing information in response to court orders and warrants is included as Attachment A to this letter. In addition, AT&T charges $40 an hour to respond to criminal subpoenas, with a minimum 1 hour assessment.

	2007	2008	2009	2010	2011
Collections	$2,813,000	$3,482,000	$4,239,000	$5,382,000	$8,253,000

a. Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking request from police departments?

ANSWER: AT&T does not charge for emergency requests.

b. Please include any written schedule of any fees that your company charges law enforcement for these services.

ANSWER: *See* Attachment A.

7. Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.

ANSWER: AT&T does not market the provision of its customer's phone usage information to law enforcement. Rather, AT&T responds to lawful requests from law for information and in some circumstances, we are compensated for the process of collecting and providing that data to law enforcement personnel.

Sincerely,

Tim McKone

AT&T PRICING STRUCTURE
Effective February 25, 2010

Type of Fee	Cost Per Number For Court Orders, Extensions or Amended Orders
DATA ORDERS	
Activation Fee: Includes activation costs per number associated with supporting CALEA compliance and responding to court orders in a timely manner.	**$325.00**
Daily Fee: Applied to each number per day the order is active to support CALEA compliance and delivery of CALEA data over the AT&T network.	**$5.00/Day**
CONTENT ORDERS	
Activation Fee: Includes activation costs per number associated with supporting CALEA compliance and responding to court orders in a timely manner.	**$325.00**
Daily Fee: Applied to each number per day the order is active to support CALEA compliance and delivery of CALEA voice/data over the AT&T network.	**$10.00/Day**
DATA WITH CONTENT ORDERS	
Activation Fee: Includes activation costs per number associated with supporting CALEA compliance and responding to court orders in a timely manner.	**$325.00**
Daily Fee: Applied to each number per day the order is active to support CALEA compliance and delivery of CALEA voice/data over the AT&T network.	**$10.00/Day**
AMENDED CONTENT OR DATA ORDERS	
Activation Fee: Includes activation costs per number associated with supporting changes to existing orders, CALEA compliance and responding to court orders in a timely manner.	**$325.00**
PACKET DATA	
Activation Fee: Includes activation costs per number associated with supporting CALEA compliance and responding to court orders in a timely manner.	**$325.00**
Daily Fee: Applied to each number per day the order is active to support CALEA compliance and deliver of CALEA packet data over the AT&T network.	**$10.00/Day**
PACKET DATA (In Conjunction with Voice Charges)	
Activation Fee: Includes activation costs per number associated with supporting CALEA compliance and responding to court orders in a timely manner.	**$100.00**
Daily Fee: Applied to each number per day the order is active to support CALEA compliance and deliver of CALEA packet data over the AT&T network.	**$10.00/Day**
BILLING ADDRESS CHANGE	
Change Fee: Invoice sent to a different billing contact other than what was previously provided.	**50.00**
MOBILE LOCATE	
Activation Fee: Includes activation costs and email delivery per number.	**$100.00**
Daily Fee: Applied to each number per day.	**$25.00**
Change Fee: Includes changes in the provisioning of the email address or frequency.	**$100.00**
VOICEMAIL PRESERVATION	
Fee/Target Number: Voicemail preservation and password reset on AT&T's legacy voicemail platform.	**$150.00**

AT&T PRICING STRUCTURE
Effective February 25, 2010

Type of Request	Fee
PERSONNEL RECORDS	
Requests for payroll, personnel, and other AT&T employee-related records.	$100.00
BILLING RECORDS	
Requests for subscribers' invoices and billed usage.	$35.00 processing Fee + $10.00/Month
CALLS TO DESTINATION	
Requests for incoming call detail (including blocked calls) per subscriber. Note: These searches may only include calls from other AT&T subscribers.	$25.00
ACCOUNT NOTES	
Requests for account notes per subscriber.	$35.00 processing Fee + $25.00
CELL SITE SEARCHES	
Requests for all calls processed during a specific time period on a specific cell site.	$75.00/tower
MAPS	
Requests for detailed cell site coverage maps.	$75.00/Hour

C Spire Wireless
1018 Highland Colony Parkway, Ste 300
Ridgeland, MS 39157

May 23, 2012

VIA ELECTRONIC MAIL AND U.S. MAIL
The Honorable Edward J. Markey
Co-Chairman
Congressional Bi-partisan Privacy Caucus
2108 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Markey:

Thank you for your May 2, 2012, letter requesting information regarding how C Spire Wireless deals with requests for consumer information from law enforcement agencies.

Please find our responses to your inquiries below. We trust you will find this information helpful as you examine policies to promote the interests of wireless consumers.

Q1: Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text message, and full-scale wire-tapping?

RESPONSE: Approximately 12,500.

Q1a: How many of these requests did your company fulfill and how many did it deny?

RESPONSE: Because many of the approximately 12,500 requests we have received seek multiple and various types of information, it is difficult to identify a specific number of requests fulfilled or denied over the given period. However, we estimate that approximately 15% of all law enforcement requests for customer information are denied either in whole or in part.

Q1b: If it denied any requests, for what reasons did it issue those denials?

RESPONSE: Law enforcement requests for consumer information are denied for various reasons. However, the most common basis for a denial is that the given request seeks information that is no longer retained by the company. Other requests are denied for procedural defects. For example, agencies may incorrectly pursue information via subpoena when a court order is required. Additionally, requests are denied due to a facial defect, such as the lack of a valid signature on the given subpoena or court order.

Q2. What protocol or procedure does your company employ when receiving these requests?

RESPONSE: All requests from law enforcement agencies seeking customer information are submitted to our Subpoena Compliance Department, where the requests are logged and reviewed by an attorney. The assigned attorney then evaluates the validity of the request and prepares an appropriate written response to the relevant law enforcement agency.

Q2a. Do you consider whether law enforcement has obtained a warrant to obtain this information?

RESPONSE: Yes.

Q2b. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?

RESPONSE: Yes. A one-time "current location" can be provided to law enforcement agencies if we detect a 911 call or if the law enforcement agency certifies that there is an emergency involving immediate danger of death or serious physical injury to any person. Requests for this one-time "current location" information are received via an Exigent Circumstances Form or, occasionally, on law enforcement agency letterhead. All other requests require a court order or warrant before information is provided.

Q3. Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?

RESPONSE: We have received and denied emergency requests for customer information in which no true "exigent" circumstances exist. We are not aware of any instance in which customer data has been improperly released by the company.

Q4. How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function?)

RESPONSE: We maintain a dedicated Subpoena Compliance Department comprised of two full-time attorneys and two full-time administrative assistants. Approximately 90-95% of the Subpoena Compliance Department's workload is comprised of reviewing and responding to law enforcement requests.

Q5. The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?

RESPONSE: To the extent compliance with a valid court order or warrant requires, we will provide customer or network-related information to law enforcement agencies which operate their own tracking equipment.

Q6. Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much

does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping?)

RESPONSE: Consistent with 18 U.S.C. §§ 2518(4), 2706(c), and 3124(c), we charge law enforcement agencies an administrative fee for responding to certain types of requests. Through April of this year, fees collected from law enforcement agencies related to requests for information total less than $18,000.00. A copy of our fee schedule is attached.

Q6a. Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?

RESPONSE: No.

Q6b. Please include any written schedule of any fees that your company charges law enforcement for these services.

RESPONSE: Please see response to Q6, above.

Q7. Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.

RESPONSE: No.

Sincerely,

Benjamin M. Moncrief
Director, Government Relations
C Spire Wireless

Fee Schedule*

Type of Request	Fee
Processing Fee (for all subpoenas and court orders)	$30.00
Call Detail	$15.00 up to 1 month; $10 each additional month
Subscriber Information	$5 per number
Electronic Surveillance - new order	$200.00 initial set up, $15.00 daily
Electronic Surveillance - renewal order	$15.00 daily (if the initial order has expired before the renewal order is received, it is billed as a new order)

* Fee Schedule effective as of October 1, 2002. Rates are subject to change.

May 23, 2012

The Honorable Edward J. Markey
Congressional Bi-partisan Privacy Caucus
7th District, Massachusetts
Congress of the United States
House of Representatives
Washington, DC 20515-2107

Dear Representative Markey:

I write in response to your May 2, 2012 letter, to our CEO Douglas Hutcheson requesting information about Cricket's responses to legal process issued by law enforcement. I am happy to answer the specific questions you raised and I would welcome the opportunity to discuss these matters further if you believe it would be helpful.

By way of background, Cricket takes its obligations to balance subscriber privacy with compliance with law enforcement requests quite seriously. Except in emergency circumstances, as defined by statute, Cricket does not release subscriber information to law enforcement without formal legal process, and Cricket examines all legal process to verify that the correct types of process are being used for the type of subscriber data being requested, even where it requires Cricket to refuse to comply with a law enforcement demand.

Below, I have set forth the specific questions in your letter and Cricket's response.

1. *Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing of phone calls and text messages, and full-scale wiretapping?*

Cricket receives thousands of forms of compulsory legal process each year from law enforcement for information related to phone usage, including subpoenas, court orders, search warrants, pen register, trap and trace orders, and intercept orders. Each form of legal process may seek multiple types of information, or information about multiple subscribers. Cricket also receives requests for disclosures of information under emergency circumstances. For the five year period from 2007– 2011, Cricket received a steadily increasing number of requests, from a low of approximately 24,000 in 2007 to a high of approximately 42,500 in 2011. This growth is in line with the growth in the number of Cricket subscribers over the same time period.

a. *How many of these requests did your company fulfill and how many did it deny?*

Cricket does not keep records of law enforcement requests that were not fulfilled. Anecdotally, however, I can inform you that Cricket does deny some requests based on insufficient law enforcement process.

b. *If it denied any requests, for what reasons did it issue those denials?*

The primary reasons that Cricket may have not implemented a law enforcement request are:

- The language of the order is insufficient to allow production of the requested content
- The level of legal process is insufficient for the type of data requested. For example, a subpoena is used to request transactional records that require a Court Order under 18 U.S.C. § 2703(d).
- Cricket may have no responsive information if data is requested with respect to time periods during which an identified user is not on our network but is roaming on a partner carrier's network
- The identified user is not a customer during the period for which data is requested, either because they have disconnected or because they are now with another carrier
- Law enforcement provided incorrect information, making it impossible to provision the request

2. What protocol or procedure does your company employ when receiving these requests?

Until April 2012, Cricket had an in-house Subpoena Compliance Group that was responsible for receiving, logging and reviewing all legal process seeking subscriber information. That group was managed by an attorney in Cricket's legal department and was trained to evaluate subpoenas, court orders and search warrants to determine if they are facially valid and are the appropriate form of process for the information requested. Such training was conducted by a former Department of Justice Computer Crime prosecutor who specializes in issues related to proper methods of obtaining electronic evidence. Each piece of legal process received by Cricket was also individually evaluated for compliance with Cricket's policies and procedures. Cricket will reject and has rejected legal process where the incorrect process is used to seek subscriber data. Where Cricket's policies caused a disagreement between the in-house compliance staff and the requesting law enforcement agency, such disputes were generally elevated to in-house legal counsel, and occasionally to outside counsel to resolve.

Since April 2012, Cricket has turned the law enforcement compliance function over to a third-party provider, Neustar, who regularly provides outsourced subpoena compliance functionality to telecommunications providers and performs the screening and production function on Cricket's behalf, with the same escalation path to in-house and outside counsel. Cricket understands that Neustar has over 400 provider clients in the WiFi, Voice, IP Broadband, wireline and wireless

industry for whom it provides these same legal compliance services. More information on Neustar's services can be found at the link below.[1]

a. *Do you consider whether law enforcement has obtained a warrant to obtain this information?*

Yes. Cricket requires law enforcement to procure a warrant, or in some cases, a Title III intercept Order for certain types of subscriber information.

b. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency requests? If yes, what are the distinctions?

Yes, Cricket follows a process to provide disclosures without legal process in emergency circumstances where Cricket, in good faith, relying on certifications by law enforcement, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency. Cricket requires that law enforcement fill out an emergency disclosure form in order to screen for bona fide emergencies.

3. Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?

Cricket is unaware of any misuse of cell phone tracking data by police departments. It also does not conduct such tracking on law enforcement's behalf without judicial process. Also, Cricket Communications does not currently have the ability to 'ping' or geo-locate a handset upon request by law enforcement.

4. How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?

As indicated above, Cricket recently outsourced these services to a third-party vendor, Neustar, Inc. Neustar provides compliance and intercept services for Cricket. Cricket has one vendor manager on staff to monitor the activities and performance of Neustar to ensure that compliance and intercept services are being performed per Cricket's policies and applicable law. Prior to outsourcing this service to Neustar, Cricket Communications had 10 dedicated employees trained to review and process law enforcement requests.

5. *The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?*

Cricket is not aware of what types of equipment can be purchased for this functionality, nor would Cricket have any reason to coordinate with police departments in the use of their equipment. Cricket controls all access to its equipment, which is not available for law enforcement use.

---

[1] http://www.neustar.biz/solutions/communication-service-providers/numbering/comply-with-regulations

6. Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping)?

Pursuant to 18 U.S.C. § 2706 Cricket is entitled to reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing information in request to legal process received from law enforcement. For real-time requests for surveillance, Cricket is also entitled to reasonable reimbursement pursuant to 18 U.S.C 2518(4) for "reasonable expenses incurred in providing such facilities or assistance" in implementing Title III orders. Cricket is not entitled to, and does not make any profit on services rendered to law enforcement. Further, Cricket is frequently not paid on the invoices it submits to law enforcement. From January 1, 2010 through the present, Cricket has requested reimbursement according to the schedule attached as Exhibit A.

a. Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?

Cricket does not charge for disclosures to law enforcement in emergency circumstances involving immediate danger of serious bodily injury or loss of life.

b. Please include any written schedule of any fees that your company charges law enforcement for these services.

Cricket's current reimbursement schedule is attached as Exhibit A to this letter.

7. Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.

Cricket does not actively advertise or market this functionality to law enforcement. Cricket primarily distributes its reimbursement schedule in response to receiving a request from law enforcement, as well as making it available to law enforcement at various law enforcement training conferences when requested.

Sincerely,

Robert J. Irving, Jr.
Senior Vice President and General Counsel

Exhibit A

COSTS FOR PRODUCTION OF RECORDS OR SERVICE RENDERED:

1. Subscriber Information:
   Over 25 requests: $5 per name/number lookup

2. Call Detail Records:
   $64 per name/number

4. Pen Register/Trap and Trace or Wire Tap/Title III/Title 50:
   $235 per name/number, per order
   $100 per name/number per extension or renewal order

5. SMS, Voicemail:
   $5.50 per name/number

metroPCS Communications, Inc.

2250 Lakeside Boulevard
Richardson, TX 75082

May 23, 2012

The Honorable Edward J. Markey
U.S. House of Representatives
Washington, DC 20515-2107

Dear Congressman Markey:

Thank you for your letter of May 2, 2012 inquiring into MetroPCS Communications, Inc.'s ("MetroPCS") policies regarding the provision of mobile phone tracking information to law enforcement agencies. MetroPCS is pleased to respond to your letter on this important topic.

MetroPCS provides mobile wireless voice and broadband data service in selected major metropolitan areas in the United States and serves more than 9.3 million subscribers,[1] making it the fifth-largest facilities based mobile broadband wireless carrier in the United States based on number of subscribers served. MetroPCS targets a mass market largely underserved by the larger national mobile broadband wireless providers. MetroPCS' service plans are differentiated from the more complex long-term plans offered by many of its competitors by being more affordable, predictable and flexible. MetroPCS' service plans currently begin at $25 per month for unlimited voice and text on a nationwide basis and $40 per month for voice, text and data on a nationwide basis, including all applicable taxes and regulatory fees. MetroPCS customers can use their unlimited wireless service in MetroPCS' coverage areas, as well as in their extended service areas through various roaming arrangements, under its flat-rate monthly service plans. Customers pay for service in advance, without a credit check.

In summary, MetroPCS only supplies information to law enforcement agencies in response to valid subpoenas, court orders, state and federal law, exigent circumstances as defined by Title 18 USC, and the Communications Assistance Act for Law Enforcement Agencies ("CALEA").

MetroPCS is pleased to respond to the questions you posed in your May 2, 2012 letter as follows:

1. *Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text messages, and full-scale wiretapping?*

From January 2006 through May 2012, MetroPCS responded to an average of fewer than 12,000 requests per month from law enforcement to provide information about MetroPCS' customers' phone usage. This figure, however, does not include requests that were not valid or were rejected because MetroPCS does not track information or requests that are not fulfilled or

[1] As of December 31, 2011.

are rejected. In addition, a single subpoena or wiretap could contain multiple requests, so the number of discrete subpoenas, court orders, and other valid processes would have been less than the amount provided above.

a. *How many requests did your company fulfill and how many did it deny?*

MetroPCS fulfilled an average of fewer than 12,000 per month from January 2006 through May 2012. MetroPCS does not have any information on how many requests it has denied because MetroPCS does not track requests that are denied or rejected.

b. *If it denied any requests, for what reasons did it issue those denials?*

MetroPCS will deny a request, among other things, if: (1) the request is not directed to MetroPCS; (2) the request is not valid; (3) the request is in the wrong form (e.g., trying to use a subpoena to get information for which a warrant is required); or (4) the phone number for which information is being requested is not a MetroPCS number.

2. *What protocol or procedure does your company employ when receiving these requests?*

MetroPCS Subpoena Compliance analysts follow a written Company procedure, which requires that each subpoena or court order is valid and complies with applicable law.

a. *Do you consider whether law enforcement has obtained a warrant to obtain this information?*

Yes.

b. *Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?*

MetroPCS distinguishes between exigent and non-exigent tracking requests. An exigent circumstance is defined by federal law as a request that the time delay to obtain a subpoena or court order may pose imminent danger of death or serious bodily injury to a person(s). If a law enforcement agency declares that a situation is "exigent," the agency is required to fill out and return to MetroPCS an Exigent Request Form, which must be signed/approved by a supervisory level police officer or federal agent. The agency must also agree to obtain the proper legal process (subpoena, warrant or court order as dictated by the nature of the request) as soon as it is reasonably possible to do so (usually 48 to 72 hours). All other circumstances are considered non-exigent and a valid court order, warrant or subpoena is required prior to fulfilling such request.

3. *Has your company every encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?*

MetroPCS is unaware that any cell phone tracking information provided by MetroPCS has been misused.

4. *How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?*

MetroPCS has a Subpoena Compliance group that is specifically trained and dedicated to responding to requests from law enforcement agencies. The group totals 16 employees and is comprised of one director, one manager, two supervisors, and 12 compliance analysts.

5. *The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?*

MetroPCS is unaware of which police departments may have their own mobile phone tracking equipment. MetroPCS only provides information to police departments pursuant to lawful process.

6. *Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping)?*

Yes. Federal law provides that telecommunications carriers may recover the cost of some of the services provided to law enforcement agencies. MetroPCS may incur different costs for providing different kinds of information. Accordingly, MetroPCS recovers the permissible cost of supplying these services based on the information sought. The schedule of cost recovery amounts is attached as **Attachment A** to this letter.

a. *Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charges fees for emergency cell phone tracking requests from police departments?*

MetroPCS does not charge a fee for providing exigent information.

b. *Please include any written schedule of any fees that your company charges law enforcement for these services.*

MetroPCS' cost recovery schedule is included with this letter as **Attachment A**.

7. *Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.*

   No.

Sincerely,

Steve Cochran
Vice President, Audit & Compliance
MetroPCS Communications, Inc.

Attachment A

metroPCS MetroPCS Subpoena Compliance

Law Enforcement Agencies/Attorneys:
Welcome to MetroPCS! Please read the updated information. Thank you!

What is Needed from Law Enforcement/Attorneys to Process Requests
The following information will assist our team of analysts to process your records:

- Please include the requesting agent's first and last name, phone number, fax number, email and mailing address with each request. **Email is our preferred method of returning records.**
- Please include specific agency billing instructions.
- Please use 1-800-571-1265 when calling the Compliance Department. Please listen to the options and choose appropriately.
- For general questions and status checks, please use our leaquestions@metropcs.com email.
- Be prepared with the tracking number, target number, or invoicing number if calling or emailing for information.

All requests received by fax or email will generate an automatic receipt when accepted into the system. The records will be returned via email, fax, or mail. **Email is the fastest method of receiving results.**

How to Contact MetroPCS

Phone 24x7: **(800) 571-1265**
Office Hours: **8:00-5:00 CST**
Please listen to the options and choose appropriately.

Mailing address:
MetroPCS Subpoena Compliance
2250 Lakeside Blvd.
Richardson, TX 75082

To fax subpoenas/court orders:
972-860-2635

To E-mail subpoenas/court orders:
subpoenas@metropcs.com

For questions and status checks:
leaquestions@metropcs.com

For pen/wire issues or questions:
esu@metropcs.com

For invoicing issues or questions:
leainvoicing@metropcs.com

What is Available
The following cites what information is available, specific documentation required, and the associated reasonable and customary fees.

- **Subscriber**: Subscriber information may be obtained with a subpoena. Current subscriber data is provided unless a specific time frame is requested.
- **Call Detail Records**: Call detail records are retained approximately **6** months from the current date after which they are overwritten and cannot be recovered. Call detail records may be obtained with a subpoena. Call detail records with *cell sites* require a court order or a search warrant. Since subscribers change often, it is advised to narrow the timeframe to the time of the event.
  $50 per number for call detail records for more than 30 days
- **Text messages**: Text messages are stored for approximately 60 days and require a court order, search warrant, or grand jury subpoena.
  $50 per number for text messages with content or without content for any date range
- **Voicemail Password Reset**: Voicemail is stored on the server for 7 days unless the subscriber saves the message. Once the message is deleted, it is permanently deleted and cannot be restored. A court order or search warrant is required in order for the voicemail to be reset.
  $50 per number for a voicemail password reset
- **Calls to Destination Search**: Requires a court order or a search warrant.
  $50 per number for calls to destination search
- **Cell Tower/Area Dumps**: Requires a court order or a search warrant.
  $50 for a Cell Tower Dump per tower number for a 2 hour period
  $100 for an Area Dump (if you know the location but do not know the cell towers that affect the area) for a maximum of 2 cell towers for a 2 hour period per cell tower search
- **Pen Registers**: Requires a court order.
  $200 set-up fee and $20 per day maintenance with a minimum fee of $500
- **Wire Taps**: Requires a court order.
  $400 set-up fee and $40 per day maintenance

What is not Available
The following information is not available:

- Subscriber information based on an IP Address
- Picture messages or Multi-Media Messages (MMS)
- Caller ID blocked from Non-MetroPCS customers
- Triangulation and Pinging (GPS) and Cell Site Location on numbers that have been turned off or are out of range

Rev. 11-2-2011 dml

601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004

May 23, 2012

The Honorable Edward J. Markey
US House of Representatives
2108 Rayburn House Office Building
Washington, DC 20515

Dear Representative Markey:

We write in reply to your letter of May 2, 2012, regarding law enforcement practices with respect to mobile phones. T-Mobile USA, Inc. ("T-Mobile USA") provides customer information to law enforcement agencies only where legally permitted or required to do so. T-Mobile USA maintains a dedicated law enforcement relations team (referred to as "LER") which handles lawful requests from law enforcement and other governmental agencies and the courts for customer information. This team is trained in legal requirements and follows strict internal policies and procedures. LER works closely with our Chief Privacy Officer and reports into the VP of Legal Affairs and Compliance in the Legal Department.

We require law enforcement agencies to follow established legal processes when they make a request for customer information. We examine each such request to ensure it meets legal requirements. We seek clarification if a request appears overbroad, unauthorized or omits important details. If a request is beyond the scope of the law, requests information outside of the company's control, is facially defective or otherwise has a legal impairment it is rejected. We would note that when lawful request for customer information is presented to us we are obliged to comply.

As permitted by law, we seek to recover our costs incurred in responding to lawful requests. We do not, however, market services to law enforcement.

In response to your specific questions, please find our answers below:

1. Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text messages, and full-scale wiretapping?

The requests for customer information from law enforcement agencies may relate to a variety of matters including national security, drug activities, murders, thefts, kidnappings and terrorism, to name a few. When presented with a lawful request for customer information, T-Mobile USA is legally obligated to provide the information. Approximately 50% of all requests received by LER are grand jury or administrative subpoenas requesting basic subscriber information and/or tolls as defined by 18 USC § 2703. While T-Mobile does not disclose the number of requests we receive from law enforcement annually, the number of requests has risen dramatically in the last decade with an annual increase of approximately 12-16%.

We understand that information on use of cell phone location data in criminal prosecutions may be available through Freedom of Information Act requests made to specific agencies. This may be a potential source of information to Congress. With regard to wiretaps, T-Mobile has not publicly disclosed this information. However, there is an annual wiretap report produced by the federal judiciary which may be of assistance.[1]

a. How many of these requests did your company fulfill and how many did it deny?

While T-Mobile maintains records on each individual request and whether it has been fulfilled or denied, T-Mobile currently does not track this information in the aggregate. Requests may be denied in whole or in part, or denied and resubmitted if the defect has been remedied.

b. If it denied any requests, for what reasons did it issue those denials?

T-Mobile USA has denied requests on a variety of grounds, including but not limited to: requests that cannot be verified as coming from an authorized law enforcement agency; requests which fail to fulfill legal requirements, and requests for information which T-Mobile USA does not possess.

2. What protocol or procedure does your company employ when receiving these requests?

We provide law enforcement agencies with dedicated contact information for our LER team as well as guidance on how to submit requests to us. This helps ensure that requests come to the appropriate staff for handling. Requests are reviewed to determine that they are valid on their face (for example, the request contains the appropriate signatures and the issuing body has the authority to make the request). Applying applicable state and Federal law, a determination is made whether the proper legal process (subpoena, court order, search warrant) has been used based upon the type of information requested. The LER team will also determine that the demand is not beyond the scope of

[1] http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/2010WireTapReport.pdf

the law, is sufficiently specific and that it clearly describes the specific subscriber whose information is sought.

a. Do you consider whether law enforcement has obtained a warrant to obtain this information?

Yes, as required by law. We require a warrant (which requires the government to show probable cause) to provide real-time tracking of mobile device location. In other cases, the law allows the government to compel production of information without a showing of probable cause and information may be obtained by court order or subpoena.

Under the Electronic Communications Privacy Act ("ECPA") we are obliged to provide information "pertaining to a customer" when presented with a lawful court order for which the government must provide "specific and articulable facts" which are presented to the court.[2] We are obliged to provide "basic subscriber information" – data which merely identifies a customer but does not reveal the customer's transactions or activity - under a broader variety of government authorizations, including administrative subpoenas.[3]

Our LER staff is trained to recognize the proper type of legal demand that is required for specific types of customer information.

b. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?

We do distinguish between emergency requests and non-emergency requests. The distinction we apply is based on federal law. ECPA allows for disclosure of communications content or information pertaining to a subscriber if we believe in good faith that an emergency involving danger of death or serious physical injury to any person requires disclosure of the information without delay.[4] This process requires law enforcement to make a written request and answer certain specific authenticating questions. Also, under federal law governing Customer Proprietary Network Information ("CPNI"), we are authorized to provide call location information to law enforcement in order to respond to a user's call for emergency services.[5]

3. Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?

---

[2] See 18 USC § 2703(d).

[3] See, e.g., 21 U.S.C. § 876 (Drug Enforcement Agency authority to issue subpoenas); Internal Revenue Code § 7602(2) (a) (authorizing IRS to issue subpoenas).

[4] 18 U.S.C. § 2702(b)(6)(c), *as amended* (communications content; 18 USC § 2702(c)(4) (customer records or content pertaining to a subscriber).

[5] 47 USC § 222 (d)(4)(A).

In the last three years we have identified inappropriate requests for cell phone tracking from law enforcement on two occasions. In both cases we referred the matters to the FBI and no information was released to law enforcement. We have also identified several instances in which persons posed as law enforcement officers to obtain this information and in such cases the requests were denied. Once a properly issued lawful warrant for cell phone tracking has been received, reviewed and implemented, we have no visibility into what use (or misuse) is made of the data by law enforcement.

4. How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?

T-Mobile maintains a dedicated LER team assigned specifically to this function. This team is a part of our Legal Department and works closely with our Privacy team.

5. The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?

We are not aware of any police department asking T-Mobile USA for assistance with their own tracking equipment. Any requests for assistance would be handled pursuant to legal requirements and we would require a proper showing of sufficient legal authority before providing such assistance.

6. Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping)?

T-Mobile may seek compensation for the recovery of costs incurred in providing information to law enforcement agencies where we are entitled to do so by law. For example, federal law provides that carriers are entitled to be compensated for the reasonable costs of providing technical assistance for lawful surveillance activities, and for costs incurred in providing stored electronic communications or backup copies to the government.[6] This includes the cost of software, infrastructure, personnel and other costs incurred in providing such services.

a. Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?

[6] See 18 U.S.C. § 2518(4) (wiretaps); 18 U.S.C. § 3124 (c) (pen register, trap and trace); 18 U.S.C. § 2706(a) (stored electronic communications).

Generally, T-Mobile does not charge law enforcement agencies for the costs incurred in responding to exigent requests such as kidnappings, imminent terrorist acts, specific threats to law enforcement agents and other crimes which may fall under 18 U.S.C. 2702. However, that depends on the type of production or service required and the volume of the production. 18 USC § 2706 precludes us from cost recovery for producing toll records and subscriber information except in cases of undue burden.

b. Please include any written schedule of any fees that your company charges law enforcement for these services.

The fees attributable to the costs are considered confidential and proprietary information.

7. Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.

T-Mobile USA does not market the provision of this information to law enforcement. We do provide law enforcement agencies with copies of our policies and procedures and with other information to assist them in understanding the requirements that must be met for the handling specific types of requests for customer information .

Respectfully Submitted,

Tony Russo
Vice President, Federal Legislative Affairs

Legal Department
Maria C. Montenegro, SVP – Litigation Counsel
9700 NW 112th Avenue | Miami, FL 33178
Direct Dial: 305-715-3690
E-Mail: mmontenegro@tracfone.com

May 23, 2012

VIA FEDERAL EXPRESS

The Honorable Edward J. Markey
Co-Chairman, Congressional Bi-Partisan Privacy Caucus
2108 Rayburn House Office Building
Washington, DC 20515-2107

Re: Cell Phone Tracking by Law Enforcement Departments

Dear Representative Markey:

Thank you for your letter of May 2, 2012, directed to Mr. F. J. Pollak, President and Chief Executive Officer of TracFone Wireless, Inc. ("TracFone"). I am responding to your letter on Mr. Pollak's behalf.

First, I would like to emphasize that TracFone shares your concerns regarding the unauthorized tracking of wireless phones by law enforcement with little or no judicial oversight and I assure you that TracFone does not participate in or condone such unauthorized tracking. TracFone's responses to the questions set forth in your letter appear below:

1. TracFone is a reseller of wireless service. It purchases wireless service on a wholesale basis from network based providers such as AT&T, T-Mobile, Verizon Wireless and other carriers and resells that wireless service on a prepaid basis. As a reseller, TracFone does not have access to and cannot provide information regarding the location of a wireless phone. TracFone cannot trace calls or text messages on a real-time basis or facilitate full-scale wire-tapping. This type of information and functionality is available at the underlying carrier level. TracFone is able to provide historical information in the form of customer call detail records (including the date, time, length and number called or calling) for voice calls and text messages. We do not have access to and cannot provide the actual text messages. Any law enforcement requests we receive for phone call or text tracing and/or wire-tapping are redirected to the underlying carrier.

a. TracFone does not have access to its underlying carriers' networks and is unable to fulfill law enforcement requests for customer device location, real-time tracing of phone calls and text messages, or full-scale wiretapping. Any such requests from law enforcement for real-time information are redirected to the underlying carrier. TracFone does provide subscriber information (if any is available) to law enforcement personnel in certain exigent circumstances and historical call records in response to valid search warrants, subpoenas or court orders.

b. TracFone will deny any non-exigent request for subscriber information that is not accompanied by a search warrant, subpoena or court order.

2. Law enforcement calls to TracFone's exigent circumstances line are handled pursuant to company protocol. Essentially, the agent answering the call must verify the identity of the caller and confirm that it is a law enforcement official. If subscriber information is available for release, the TracFone agent must independently confirm the identity and authority of the caller requesting the information, determine if the circumstances are an "emergency" and whether the release of subscriber information is warranted. Non-emergency requests from law enforcement for customer information require a search warrant, subpoena or court order.

a. We require a search warrant, court order or subpoena before we release customer information in non-exigent circumstances.

b. We do not have the capability of providing cell phone tracking information. All such requests are redirected to the underlying carrier.

3. Not applicable as we do not provide cell phone tracking.

4. TracFone has specially trained staff devoted to addressing law enforcement requests for customer information. TracFone employs 20 call center agents who process both exigent circumstances calls and non-exigent requests for information (where a subpoena, search warrant or court order is provided). In addition, TracFone employs six (6) full time subpoena compliance agents who process search warrants, subpoenas and court orders.

5. No, TracFone does not cooperate with police departments that have their own tracking equipment.

6. No, TracFone does not and has not previously accepted money or any other form of compensation in exchange for providing information to law enforcement. TracFone does not charge fees for providing information to law enforcement.

a. TracFone does not charge fees for any type of request from law enforcement.

b. Not applicable. TracFone does not charge fees.

7. TracFone does not market the provision of information to law enforcement.

Please advise should you require any clarification or further information. Thank you.

Respectfully,

Maria C. Montenegro,
Senior Vice President – Legal

MCM/

cc. F.J. Pollak, President and CEO, TracFone
Richard B. Salzman, EVP – General Counsel, TracFone

U.S. Cellular
8410 W. Bryn Mawr Avenue
Chicago, IL 60631
www.uscellular.com

May 23, 2012

Edward J. Markey
Co-Chairman
Congressional Bi-partisan Privacy Caucus
Congress of the United States
House of Representatives
Washington, D.C. 20515-2107

Dear Congressman Markey,

We are in receipt of your letter of May 2, 2012 in which you request information regarding United States Cellular Corporation's ("U.S. Cellular") responses to law enforcement's requests for customers' records, including cell phone usage, location and text messages.

U.S. Cellular's Subpoena Compliance Team ("Compliance Team") responds to all lawful requests from customers, attorneys and members of the law enforcement community which includes prosecutors, local, state, county and federal law enforcement officers. The Compliance Team is a centralized department consisting of 3 Subpoena and Cloning Specialists, 1 Subpoena and Cloning Team Leader and 1 Supervisor of Risk Management. In addition, U.S. Cellular uses its National Roamer Support Team in Knoxville, TN for all exigent requests (referred herein as "E911") that are received after normal business hours with support from a member of the Compliance Team in case issues arise. The Compliance Team and National Roamer Support Team ensure that U.S. Cellular is available 24 hours a day, 7 days a week, 365 days a year to provide law enforcement information as required under the Communications Assistance to Law Enforcement Act. 47 U.S.C. §1002 *et seq.* The Compliance Team also testifies in court to authenticate and interpret U.S. Cellular records. Through this work, U.S. Cellular is committed to serving its customers, law enforcement, and members of the legal community by providing information in a professional and expeditious manner while maintaining the privacy and security of its customers.

U.S. Cellular's responses to the specific questions raised in your letter are contained in Attachment A, enclosed.

Sincerely,

John C. Gockley

Attachment A

1. **Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text messages, and full-scale wiretapping?**

   a. **How many of these requests did your company fulfill and how many did it deny?**

   b. **If it denied any requests, for what reasons did it issue those denials?**

Over the past 5 years, U.S. Cellular has received over 103,000 requests in the form of subpoenas, court orders, search warrants and letters regarding its customers' phone accounts and usage. Specifically, U.S. Cellular has received requests for subscriber names, numbers, billing records, phone location (PING), cell tower records, text message content, pen registers and wiretaps. Pursuant to legal requirements, U.S. Cellular requires search warrants or court orders, which may include grand jury orders, to provide cell tower records and content of text messages. Court orders issued pursuant to Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.* ("Title III"), are required for pen registers and wiretaps. U.S. Cellular also receives a number of exigent requests (hereinafter "E911") from law enforcement each year. These E911 requests most often seek subscriber information or phone location by having U.S. Cellular "ping" (PING) the device to determine which cell tower the device is communicating with at that time.

Attached as Exhibit 1 is a General Information sheet that U.S. Cellular provides to law enforcement and attorneys about its Subpoena Compliance program. It explains how to submit requests, the guidelines for E911 requests, and information regarding the legal documentation needed to procure specific information. The General Information sheet also includes the rates U.S. Cellular charges for services as well as the period of time that U.S. Cellular retains records used to comply with lawful requests. As noted in the General Information sheet, requests can be denied for several reasons, including U.S. Cellular not being the carrier for the phone number provided, the number being ported to a different carrier, or the legal document not being completed properly.

The table below contains more specific information about the requests submitted to the Subpoena Compliance Team for each of the last 5 years. U.S. Cellular uses a database program ("Remedy Program") in order to track and respond to lawful requests. The table includes all requests submitted to the Compliance Team and is not limited to requests by law enforcement. Based on information in the Remedy Program, requests are broken into the follow categories: (i) Court Order; (ii) E911 request; (iii) Grand Jury request; (iv) Letter; (iv) Police Report; (v) Pen Register; (vi) Search Warrant; (vii) Subpoena; and (viii) Wiretap. The resolution is listed as: (i) Complied; (ii) Denied due to information needed; (iii) Denied due to information not available; and (iv) Resolution not

recorded. Exhibit 2 and Exhibit 3 are the form letters for "denial because information is needed" and "denial because information is not available."

Year	Method of Request	Complied	Need Information	Information Not Available	Resolution Not Recorded	Total
2007	Court Order	2665	1	0	64	2730
	E911	2494	3	1	470	2968
	Grand Jury	0	0	0	0	0
	Letter	391	8	0	14	413
	Police Report	246	1	0	9	256
	Pen Register	6	0	0	1	7
	Search Warrant	117	0	0	11	128
	Subpoena	9239	9	2	365	9615
	Wiretap	5	0	0	1	6
2008	Court Order	2462	2	4	180	2640
	E911	3125	3	1	845	3974
	Grand Jury	30	0	0	0	30
	Letter	657	18	1	172	848
	Pen Register	119	0	0	7	126
	Police Report	159	2	0	21	182
	Search Warrant	222	2	1	25	230
	Subpoena	11646	28	23	837	12,534
	Wiretap	6	0	0	0	6
2009	Court Order	2064	3	6	23	2096
	E911	3598	3	7	634	4242
	Grand Jury	1236	2	4	29	1271
	Letter	969	3	8	194	1174
	Pen Register	134	5	0	40	179
	Police Report	194	5	1	3	203
	Search Warrant	349	3	1	12	365
	Subpoena	10486	14	34	322	10,856
	Wiretap	4	4	0	0	8
2010	Court Order	1879	7	15	15	1916
	E911	4201	5	26	99	4331
	Grand Jury	1216	3	16	4	1259
	Letter	1219	17	12	324	1572
	Pen Register	200	0	2	11	213
	Police Report	180	2	1	0	183
	Search Warrant	417	5	6	4	432
	Subpoena	9905	42	93	341	10,381
	Wiretap	3	0	0	0	3

Year	Method of Request	Complied	Need Information	Information Not Available	Resolution Not Recorded	Total
2011	Court Order	1590	4	15	19	1628
	E911	3473	10	184	357	4024
	Grand Jury	714	2	7	5	728
	Letter	1522	11	16	522	2071
	Pen Register	284	1	5	22	312
	Police Report	85	1	0	4	90
	Search Warrant	350	4	6	7	367
	Subpoena	10,058	41	96	316	10,511
	Wiretap	3	0	0	0	3
2012	Court Order	566	4	2	11	583
	E911	1486	6	92	20	1604
	Grand Jury	262	1	7	4	274
	Letter	623	9	9	212	853
	Pen Register	126	1	1	9	137
	Police Report	12	1	0	1	14
	Search Warrant	197	2	7	6	212
	Subpoena	4243	21	40	140	4444
	Wiretap	1	0	0	0	1
Total						103,655

E911 is an exigent request by law enforcement in life or death situations. Law enforcement is required to complete an Exigent Form at which time the information is provided immediately. E911 requests are often subscriber information or phone location (PING). Exigent Forms are attached as Exhibit 4.

Letters are either from: (i) customers requesting their own records accompanied by their picture identification card; or (ii) law enforcement requesting preservation of documents pursuant to Section 2703 of the Stored Communications Act, 18 U.S.C. §2703.

Police Report is a request by law enforcement for a customer's bill or subscriber information in order to complete a police report. The request is accompanied by a letter from the customer and customer identification, and the response is sent to law enforcement.

2. What protocol or procedure does your company employ when receiving these requests?

a. Do you consider whether law enforcement has obtained a warrant to obtain this information?

b. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?

As noted in the response to Question #1, U.S. Cellular's Compliance Team provides a General Information sheet to law enforcement and attorneys about its processes. The Compliance Team will record each request in the Remedy Program as it is received. Subpoena requests and court orders are handled on a first-come, first-serve basis. And, E911 requests are handled on as needed basis. The Compliance Team provides content of text messages and cell tower records pursuant to search warrants and court orders. Pen registers and wiretaps require Title III Court Orders. The Compliance Team works with law enforcement on the Title III Orders in order to ensure timely setup and monitoring as required.

The Compliance Team distinguishes between E911 requests and non-emergency tracking requests both in the time period in which it responds and the method for obtaining information. With an emergency request, law enforcement must complete the Exigent Form prior to receiving either the requested information, usually subscriber information or the location of the device through the PING. With a non-emergency request, law enforcement must submit a court order to receive the cell tower data which will provide information regarding calls made by the devices that communicated with the cell tower during a specific period.

3. Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, how has your company responded?

U.S. Cellular has not encountered misuse of phone tracking by law enforcement.

4. How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?

U.S. Cellular has a staff of 5, the Compliance Team consisting of 1 Supervisor, 1 Team Lead and 3 Specialists, devoted to responding to requests by law enforcement and attorneys. The Compliance Team also has access to U.S. Cellular attorneys as well as outside legal counsel in the event that questions arise regarding the sufficiency of any subpoena, court order, search warrant or other document submitted.

5. The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?

U.S. Cellular is unaware of police departments purchasing their own mobile phone tracking equipment. As noted in its General Information sheet, the Compliance

Team does provide the information for pen registers and wiretaps to law enforcement's own equipment pursuant to a Title III Court Order.

6. **Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does you company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping?**

   a. **Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?**

   b. **Please include any written schedule of any fees that your company charges law enforcement for these services.**

In order to cover its costs of providing this service, U.S. Cellular began charging law enforcement and attorneys for complying with lawful requests in 2009. U.S. Cellular has collected the following amounts since it has implemented its fee schedule: (i) $162,720 in 2009; (ii) $413,535 in 2010; (iii) $460,692 in 2011; and (iv) $140,125 in 2012 year-to-date. In regard to an emergency request, U.S. Cellular does not charge different fees for the services, but U.S. Cellular does charge an additional fee to expedited processing a request. The expedited fees are: (i) $100 for processing an order in 1 day; (ii) $50 for processing an order in 2-3 days; and (iii) $25 for processing an order in 3-4 days. With regard to emergency tracking requests, U.S. Cellular does not charge law enforcement for its first 3 PING requests; however U.S. Cellular charges $25 per PING for every request thereafter. Nevertheless, before receiving any GPS locator information, law enforcement must complete an Exigent Form. A written schedule of fees is provided as part of the General Information sheet (Exhibit 1) which details U.S. Cellular's charges for services.

7. **Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.**

U.S. Cellular does not market the provision of these services to law enforcement. U.S. Cellular strives to respond to these requests in a professional and expeditious manner.

United States Cellular Corporation

General Information

Contact Information and Hours of Operation:

- Monday – Friday 8:00 a.m. – 5:00 p.m. CST
- Telephone Number – **(630) 875-8270**
- Fax Number – **(866-669-0894)**
- Mailing Address: **U.S. Cellular**
  Subpoena Compliance
  One Pierce Place
  Suite 800
  Itasca, IL 60143
- Email address – legal.compliance@uscellular.com
- Staffing 1 Supervisor and 4 Specialists.

All Subpoena and court order requests are processed in the order that they are received. Our normal turn around time is 2 weeks from the date of receipt unless it is an Exigent Circumstance. Exigent requests take precedence over all other requests.

Exigent Requests

1. From time to time, calls are received from law enforcement regarding emergency situations. USCC defines an emergency situation as *"(i) an emergency situation requiring swift action to prevent imminent danger to life or serious damage to a person, property, or to forestall the imminent escape of a suspect, or destruction of evidence. (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered to authorize such interception."*
2. If you have an emergency situation after normal business hours, please call our after hours department for assistance at **(630) 875-8270**. This department ONLY handles exigent circumstances and only works with Law Enforcement Agencies or E911 centers that are required to complete the attached Exigent Form before any information is released.

Subpoena

Administrative Subpoena – is required to release Call Detail Records, Subscriber Information, and reprint of a customer's bill.

Search Warrant or Court Orders

Search Warrant or Court Orders are required to release:

- content of text messages
- cell tower location data which show what cell towers were used to connect a call. This provides a general location of the phone during a specific call.

Title III Orders

Title III court orders are required to release the following to LEA's that have their own equipment:

- The set up of pen register (electronic transmittal of all phone numbers called on a specific target number to law enforcement agents).
- Title III surveillance (electronic transmittal of all oral voice conversation on a specific target number to law enforcement agents).

Denial of Subpoena, Search Warrant, Court or Title III Orders

On occasion requests have been denied for the following reasons:

- The records are not available for the time frame requested.
- Cellular telephone number does not belong to U.S. Cellular
- U.S. Cellular is not the carrier listed in the request.
- The time frame requested has exceeded our retention period (see attached).
- Subpoena or court order is not signed or contains incomplete information.
- Cellular phone number is not in the name of the person listed on the request.
- Cellular telephone number ported out to another carrier.

COSTS FOR PRODUCTION OF RECORDS OR SERVICE RENDERED

- Subscriber Information
  - $5 per CTN

- Bill Reprints:
- Bill reprints - 5 months or less $5 per month per CTN
- 6 months or greater $10 per month per CTN

- Call Detail Records:
  - $50 per CTN per month

- Text Messaging Detail Records:
  - $40 per CTN per month

- Pen Register/Trap and Trace or Wire Tap/Title III
  - $250 set up fee.
  - $25 per day per CTN

- GPS Locator (PINGS)
  - First 3 requests free - $25.00 each subsequent request
  - $25.00 per request on nonexigent circumstances

- Content of Text Messages
  - $25.00 flat fee per CTN/per request

- Cell Tower Dumps
  - $50.00 per staff hour/per cell tower for requests greater than 0.5 hours

- Expert Testimony
  - $50.00 per hour per court case. (This fee includes the time it takes to prepare the witness along with travel to and from the appearance).

- Expedited Services
  - $100.00 1 business day
  - $50.00 2-3 business days
  - $25.00 3-4 business days

Retention of records

Type of Information	Description	Retention Period
Call Detail Records	Details the outgoing and incoming phone numbers, captures date and time of calls.	1 rolling calendar year
Text Messaging Records	Details the outgoing and incoming phone numbers, captures date and time of text messages.	1 rolling calendar year
Content of Text Messages	Captures the content of information sent via text.	3-5 days
Bill Reprints	Reprint of customers billing statement.	estimated 7 years
Cell Tower Information	Tower information that call was processed through.	1 rolling calendar year
Subscriber Information	Name, address, social security number, equipment type, activation date and location of service activation.	estimated 7 years
Payment History	Payment amounts, date payment made and source type (i.e. credit card, check, IVR or cash).	1 rolling calendar year
Account Memos	Record of customer interaction with U.S. Cellular® front line associates.	estimated 7 years

U.S. Cellular
believe in something better™

May 22, 2012

Requestor Name
Requestor Agency
Street Address 1
Street Address 2
City State Zip

Re: Info Requested

Dear Agent Name,

Your discovery request dated Date, directed to *U.S. Cellular* was recently received. At this time *U.S. Cellular* does not have the information you have requested on file for telephone number CTN, however this information may be obtained from Carrier Name.

If you have any questions, please contact a Subpoena Specialist at the number listed below. Thank you.

Sincerely,

Your Name Here

Your Name Here
Subpoena Specialist
630-875-8270

File: Remedy Number

Exhibit 3

8410 West Bryn Mawr, Ste 700
Chicago, Illinois 60631-3486

[insert date]

[insert entity]

Dear [insert name],

Your discovery dated directed at *U.S. Cellular* was recently received. Based on the information you submitted, we require a time frame for the records in question
You may resubmit your requests with the required information and it will be processed accordingly. Should you have any questions regarding this letter, please contact a Subpoena Specialist at the number listed below. Thank you.

Please consider this letter as our response to the discovery request.

Sincerely,

Lauren Murdock
Supervisor Risk Management
630-875-8270

File:

Exhibit 4

U.S. Cellular
believe in something better

911 EXIGENT CIRCUMSTANCES FORM

FAX TO: U.S. Cellular Subpoena Department

Monday–Friday 8:00 a.m. to 5:00 p.m. CST		**After hours, weekends and holidays**	
Business Hours Phone:	630-875-8270 Option 1	After Hours Phone:	630-875-8270 Option 1,2
Business Hours Fax:	866-669-0894	After Hours Fax:	865-777-8333

1. REQUESTOR INFORMATION

Law Enforcement Agency: _____

Address: _____

City, State, Zip _____

Requested By (Printed Name): _____

Contact #: _____ Fax #: _____

2. U.S. CELLULAR SUBSCRIBER INFORMATION

Emergency Request for Wireless #: __ __ __ - __ __ __ - __ __ __ __

Name of Wireless Subscriber: _____

Information Requested: _____

_____

3. FOR 911 EXIGENT CIRCUMSTANCES (SUBSCRIBER INFO) COMPLETE THE FOLLOWING:

This office received a 911-distress call for assistance for the above-listed U.S. wireless telephone number on _____, 20__ at _____A.M./P.M. Based upon that call, I believe that one or more people face immediate danger of death or serious physical injury. I request that you promptly provide me with the current subscriber name and billing address for the above-referenced wireless number so that we may render assistance to this individual(s).

4. ATTESTATION

I hereby attest that the information provided above is, to the best of my knowledge, truthful and accurate and that: (a) an emergency situation exists that involves (i) immediate danger of death or serious physical injury to a person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered to authorize such interception.

_____ _____

Signature **Printed Name**

_____

Date

Exhibit 4

U.S. Cellular
We connect with you:

EMERGENCY PEN REGISTER / TRAP AND TRACE
EMERGENCY WIRETAP FORM

FAX TO: **U.S. Cellular Subpoena & Cloning Department**
Monday-Friday 8:00 a.m. – 5:00 p.m. CST
Business Hours Phone: 630-875-8270
Business Hours Fax: 866-669-0894

After Hours, Weekends and Holidays
After Hours Phone: 630-875-8270
After Hours Fax: 865-777-8333

1. REQUESTOR INFORMATION

Law Enforcement Agency: _____

Address: _____

City, State, and Zip: _____

Requested By (Printed Name): _____

Contact #: _____ Fax #: _____ Date: _____

2. U.S. CELLULAR SUBSCRIBER INFORMATION

Emergency Request for Wireless #: _____ - _____ - _____

Name of Wireless Subscriber: _____

Other Relevant Information: _____

_____

3. REQUESTED ACTION

☐ Emergency Pen Register and Trap and Trace (Complete Sections 4 and 5)

☐ Emergency Wiretap (Complete Sections 4 and 5)

4. **For Emergency Pen Register, Trap and Trace and Wiretap Intercept, Complete the Following:**

Describe the situation and request: _____

_____

_____

_____

_____

_____

_____

If U.S. Cellular is not provided with an Order approving this interception within forty-eight (48) hours after the installation of the Pen Register, Trap and Trace, and/or Wiretap, U.S. Cellular will, without notice, immediately terminate this interception.

5. **ATTESTATION**

I hereby attest that the information provided above is, to the best of my knowledge, truthful and accurate and that: (a) an emergency situation exists that involves (i) immediate danger of death or serious physical injury to a person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered to authorize such interception.

_____ _____

Signature Printed Name

William B. Petersen
General Counsel

Verizon Wireless
One Verizon Way
VC43E024
Basking Ridge, NJ 07920-1097

Phone 908 559-5695
Fax 908 559-7397
william.petersen@verizonwireless.com

Tuesday, May 22, 2012

The Honorable Edward J. Markey
United States House of Representatives
2108 Rayburn House Office Building
Washington, DC 20515

Dear Representative Markey:

I am writing in response to your May 2, 2012 letter to Lowell C. McAdam, President and Chief Executive Officer of Verizon Communications Inc., inquiring about Verizon Wireless' practices when responding to requests for customer information from law enforcement.

Protecting our 93 million customers' privacy is one of Verizon Wireless' highest priorities. Yet we also have a legal obligation to provide customer information to law enforcement in certain situations. Law enforcement demands for customer information are typically accompanied by a warrant, a court order, or a subpoena. Verizon Wireless carefully reviews each of these legal demands and has in place a process to ensure that we fulfill our legal obligations to provide information, but only when authorized by law.

Unless a customer consents to the release of the information or law enforcement certifies that there is an emergency involving danger of death or serious physical injury, we do not release location information to law enforcement without a signed warrant or order from a judge.

Moreover, we do not "sell [our] customers' personal information to law enforcement." Rather, we comply with legal process requiring us to provide specific information. In most instances, as explained below, we do not even charge a fee for responding to legal process. In those circumstances where we do charge law enforcement, we do so in accordance with law and seek reimbursement for only a portion of our reasonable expenses.

1. ***Over the past five years, how many requests has your company received from law enforcement to provide information about your customers' phone usage, including but not limited to location of device, tracing phone calls and text messages, and full-scale wiretapping?***

    a. ***How many of these requests did your company fulfill and how many did it deny?***

b. If denied any requests, for what reasons did it issue those denials?

In 2011, Verizon Wireless received approximately 260,000 requests for customer information from law enforcement. About half of these requests were subpoenas; generally speaking, law enforcement can only seek subscriber or call detail records (the type of information on a phone bill) through a subpoena. See 18 U.S.C. § 2703(c)(2)(A-F). The other half were warrants and orders (generally for phone bill information, wiretaps, pen registers, traps and traces, text message information and location information) or emergency requests. Over the past five years, the number of requests has grown an average of about 15% each year.

Verizon Wireless has a dedicated team that reviews every request from law enforcement and does not release customer information unless authorized by law. We will not release information if the legal process from law enforcement facially fails to comply with the law (e.g., is not signed or a subpoena is used when different legal process is required). In some instances, law enforcement seeks information that Verizon Wireless does not have. Verizon Wireless does not in the ordinary course of business track the number of law enforcement requests to which information is provided, or is not provided for any of the reasons above.

2. What protocol or procedure does your company employ when receiving these requests?

As explained in response to question 1, we have a team of trained employees and managers that reviews and, if appropriate, responds to these demands. We have a group dedicated only to subpoenas and have team members that specialize in responding to warrants and orders.

a. Do you consider whether law enforcement has obtained a warrant to obtain this information?

As explained in response to question 1, Verizon Wireless reviews every request from law enforcement and does not release customer information unless authorized by law. As part of that review, we will consider the specific form of legal process at issue and the directives therein. Again, we have a group dedicated to reviewing only subpoenas and team members that specialize in responding to warrants and orders.

b. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?

Yes. A non-emergency request for location information must be accompanied by a warrant or an order. Consistent with federal law, (e.g., 18 U.S.C. §2702(c)(4)), Verizon Wireless will release information regarding the location of a device without a warrant or order in an emergency involving danger of death or serious physical injury.

3. ***Has your company encountered misuse of cell phone tracking by police departments? If yes, in what ways has tracking been misused? And if yes, has your company responded?***

Verizon Wireless is unaware of any misuse of cell phone tracking by police departments.

4. ***How much of your staff is devoted to providing this type of information to law enforcement (i.e., does your company have staff assigned specifically to this function)?***

As explained in response to question 1, Verizon Wireless has a dedicated team of approximately seventy that works 24 hours a day, seven days a week. The team is trained to respond to lawful demands for customer information in accordance with applicable law.

5. ***The New York Times article mentions police departments purchasing their own mobile phone tracking equipment. Does your company cooperate with police departments that have their own tracking equipment? If yes, how?***

We do not cooperate with police departments in the use of their own tracking equipment. We do comply, however, with valid warrants or court orders or in an emergency involving danger of death or serious physical injury (as described on page 1).

6. ***Has your company ever accepted money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money has your company received? And if yes, how much does your company typically charge for specific services (i.e., phone location, trace phone calls or text messages, full-scale wiretapping)?***

Federal law authorizes carriers to charge a "reimbursement" fee for responding to legal demands for records (see 18 U.S.C. § 2706(a)) or to recoup "reasonable expenses" in complying with a wiretap order or a pen register or trap and trace order (see 18 U.S.C. §§ 2518(4), 3124(c)).

In the majority of instances, however, Verizon Wireless does not seek reimbursement for responding to law enforcement requests. We do not charge for responding to subpoenas or emergency situations.

When we do charge for complying with demands from law enforcement, our fees are permitted by law or court order and seek to recoup only some of our costs. In the past few years, we have charged only to retrieve text message content or for the services we provide in response to wiretap orders, pen register orders or trap and trace orders. We charge $50 to retrieve up to five days of stored text message content. For a wiretap order we charge $775 (or cap our charge at $1,825 if multiple switches are involved) for a new 30 day order and pro-rate the charges for orders that last fewer than 30 days. There is an additional monthly charge of $500 (or $1,250 if multiple switches are involved) when we receive an order to renew a wiretap. For a pen register or trap and trace order, we charge approximately $470 (or cap our charge at $1,100 if multiple switches are involved) for a new 30 day order and, again, pro-rate the charges for orders that last fewer than 30 days. There is an additional monthly charge of $300 (or $750 if multiple switches are involved) when we receive an order to renew a pen register or trap and trace. We have been reimbursed between approximately three and five million dollars in each of the last five years for complying with the many court orders we receive for wiretaps, pen registers, traps and traces and text message content.

a. ***Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests from police departments?***

   Verizon Wireless does not seek reimbursement when we provide information to law enforcement in emergencies as described in response to question 2b.

b. ***Please include any written schedule of any fees that your company charges law enforcement for these services.***

   The last fee schedule we created was in August 2009; we have not updated it to reflect our new practices and have not distributed it for some time. Our current fees are stated in the response to question 6.

7. ***Does your company actively market the provision of this information to law enforcement? If yes, please describe the nature of these marketing activities.***

   No.

Sincerely,

William B. Petersen