



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?

²See 18 USC § 2703(d).

³See, 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).

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

⁵47 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?

⁶See 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,

A handwritten signature in cursive script that reads "Tony Russo".

Tony Russo
Vice President, Federal Legislative Affairs