

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396-2900188 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

July 11, 2012

The Honorable Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Holder:

I wrote to nine wireless carriers in May seeking detailed information about the policies and procedures employed during law enforcement requests for consumers' mobile phone records. The data I received from the carriers was startling both in volume and scope. Law enforcement at all levels of government made approximately 1.3 million requests for wireless device records during 2011. These requests sought an expansive range of information, including geolocation, call records, content of text messages, and wiretaps. The responses from the carriers raise a number of important questions about how this sensitive data is handled, administered, and disposed of.

According to the responses I received from the wireless carriers, the number of requests received from law enforcement continues to grow each year, with one carrier citing a 15 percent annual increase, and another carrier a 12-16 percent annual jump. The replies from the carriers also reveal that the records of far more than 1.3 million individuals have been turned over to law enforcement, particularly due to the practice of requesting "cell tower dumps". In these data dumps, carriers provide all the phone numbers of mobile phone users who connect with a cell phone tower – often within a small geographic area – during a certain period of time.

The expansive nature of these information requests likely results in the collection of sensitive records of innocent consumers by law enforcement. The practices of law enforcement agencies, along with the enormous amount of requests, range of information provided, and large numbers of consumers involved, raise a number of important privacy concerns. It is important to know how law enforcement is handling the records of consumers, especially those who are innocent, which may be collected as part of these information requests.

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

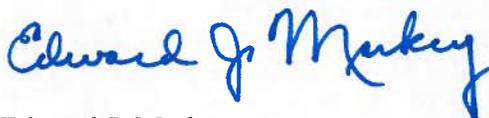
1. How many requests for mobile phone records has the Department of Justice (DOJ) filed with wireless carriers during each of the last five years? Please provide a breakdown of requests (i.e., geolocation, content of text messages, call records, customer information, wiretapping, etc.).

2. For each of these types of requests (i.e., geolocation, content of text messages, call records, customer information, wiretapping, etc.), what legal standard and type of order does DOJ believe applies? Before the Supreme Court decision in U.S. v. Jones, DOJ differentiated between historical and “real-time” location information, and between GPS and cell site location information. In light of the Court’s ruling in Jones, how does DOJ now treat those different types of information?
3. Of the records received by DOJ, how many individuals’ phone records were provided by carriers for each of the past five years?
4. How much in funding was provided to wireless carriers in order to respond to DOJ information requests during each of the past five years?
5. How are mobile phone records transmitted between wireless carriers and DOJ?
 - a. Does DOJ require carriers to take steps to ensure the information is secure during transmission? If yes, what steps (e.g., encryption) are used? If not, why not?
6. What protocol or procedure does DOJ employ after the Department receives these phone records? How and where does DOJ handle, administer, and store this information?
 - a. How does DOJ ensure the security of this information?
 - b. For what purposes is this information used?
 - c. Is this information shared with any entities outside of DOJ? If yes, what entities?
 - d. How long does DOJ store this information? (i.e., what does DOJ do with the information once an investigation concludes?)
 - e. Does DOJ delete this information? If yes, after what period of time does DOJ delete this information? If yes, what procedures does DOJ employ to ensure destruction of these records? If not, why not?
7. Does DOJ segregate the records of individuals who are not subjects of an investigation from individuals who are being targeted for investigation by law enforcement? If yes, how does DOJ handle the records of innocent individuals (e.g., immediate deletion)? If not, why not? For example, if law enforcement requests a cell tower dump, it will receive hundreds or even thousands of records of every mobile phone that connects with a cell tower during a certain period of time.
 - a. Does the length of time DOJ keeps this information depend on whether the records are of innocent individuals or those subject to an inquiry? If yes, please explain. If not, why not?
 - b. What does DOJ do with information that it deems unnecessary for an investigation (i.e., deletion, storage, provide to other entities, etc.)?
8. Is there any notice given to individuals whose information was transmitted to DOJ by their wireless carrier?

9. In cases of emergency or exigent circumstances, what procedures does DOJ use to request mobile phone records?
 - a. If information is provided by carriers on a continuing basis (i.e., the real time location of an individual's device), at what point does DOJ seek a court order for this information?
 - b. Is there a procedure in place for DOJ to later certify, after the phone records are provided, that there was in fact an emergency?
10. Please provide reports on pen registers and trap and trace device orders for each of the last five years, as described in 18 U.S.C. § 3126.
11. Does DOJ require any reporting by local or state law enforcement on the number or types of requests they make each year of wireless carriers for mobile phone records? If not, why not?
12. Does DOJ require any reporting by wireless carriers on the number or types of requests they receive from local or state law enforcement, including how many requests law enforcement fulfills and denies? If not, why not?
13. Has DOJ issued best practices or guidelines for local or state law enforcement about how to best handle, administer, and dispose of this sensitive personal information provided by the wireless carriers? If yes, please provide a copy. If not, why not?

Thank you for your attention to this important matter. Please provide responses to these questions no later than August 1, 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