

Please Do Not Reply To This Email.

Public Comments on Privacy and Security of Information Stored on Mobile
Communications Devices:=====

Title: Privacy and Security of Information Stored on Mobile Communications Devices
FR Document Number: 2012-14496
Legacy Document ID:
RIN:
Publish Date: 6/13/2012 12:00:00 AM

Submitter Info:

First Name: sean

Last Name: kelly

Mailing Address: 1103 22nd street

City: Bellingham

Country: United States

State or Province: WA

Postal Code: 98225

Comment: Since the previous amendment of the Communications Act of 1934 in 2007, the information capacity of wireless communications devices has increased significantly. With this increase came an increase in the amount of information service providers have access to. It is vital that an update be made on the regulation of carrier's use of that information, specifically with regards to consumer proprietary network information (CPNI). CPNI includes information relating to "the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" as well as billing information, with all information being provided to the carrier "solely by virtue of the carrier-customer relationship" (47 U.S.C. section 222 FCA). In the 2007 amendment, the FCC required an annual CPNI certification to be filled out by service providers, but as early as 2011, the FCC noted that some carriers had failed to complete this certification (FCC Enforcement Advisory No. 2011-02). In a 2011 enforcement advisory sent to carriers by the Enforcement Bureau, it was stated that "failure to file a timely and complete certification calls into question whether a company has properly complied with the rules requiring it to protect its customers' sensitive information" (FCC Enforcement Advisory No. 2011-02). Carrier IQ makes this issue even more severe, as the software has the ability to record customer activity information and forward that information to phone companies unbeknownst to the customer (Tsukayama, Hayley. The Washington Post. December 1, 2011). Software such as these could harm the carrier-customer relationship and presents a new dilemma for CPNI regulation, as customer-specific information is being transferred without the customer's knowledge.

Since the previous amendment of the Communications Act of 1934 in 2007, the information capacity of wireless communications devices has increased significantly.

With this increase came an increase in the amount of information service providers have access to. It is vital that an update be made on the regulation of carrier's use of that information, specifically with regards to consumer proprietary network information (CPNI). CPNI includes information relating to "the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" as well as billing information, with all information being provided to the carrier "solely by virtue of the carrier-customer relationship" (47 U.S.C. section 222 FCA). In the 2007 amendment, the FCC required an annual CPNI certification to be filled out by service providers, but as early as 2011, the FCC noted that some carriers had failed to complete this certification (FCC Enforcement Advisory No. 2011-02). In a 2011 enforcement advisory sent to carriers by the Enforcement Bureau, it was stated that "failure to file a timely and complete certification calls into question whether a company has properly complied with the rules requiring it to protect its customers' sensitive information" (FCC Enforcement Advisory No. 2011-02). Carrier IQ makes this issue even more severe, as the software has the ability to record customer activity information and forward that information to phone companies unbeknownst to the customer (Tsukayama, Hayley. The Washington Post. December 1, 2011). Software such as these could harm the carrier-customer relationship and presents a new dilemma for CPNI regulation, as customer-specific information is being transferred without the customer's knowledge.