

HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TOM COBURN, OKLAHOMA

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

December 1, 2011

Mr. Randall L. Stephenson
Chairman, CEO, and President
AT&T, Inc.
One AT&T Plaza
208 South Akard Street
Dallas, TX, 75202

Mr. Peter Chou
President and CEO
HTC Corporation
13920 SE Eastgate Way, Suite 400
Bellevue, Washington 98005

Mr. Geesung Choi
Vice Chairman and CEO
Samsung Electronics Co., Ltd.
85 Challenger Rd.
Ridgefield Park, NJ 07660-0511

Mr. Dan Hesse, CEO
Sprint Nextel Corporation
6391 Sprint Parkway
Overland Park, KS, 66251

Dear Mr. Stephenson, Mr. Chou, Mr. Choi and Mr. Hesse:

Attached please find my letter to Mr. Larry Lenhart, President and CEO of Carrier IQ, Inc. It describes my concerns regarding that company's software, pre-installed on countless Americans' smartphones, that appears to log and potentially transmit highly sensitive information regarding consumers' use of smartphones, including:

- when they turn their phones on;
- when they turn their phones off;
- the phone numbers they dial;
- the contents of text messages they receive;
- the URLs of the websites they visit;
- the contents of their online search queries—even when those searches are encrypted; and
- the location of the customer using the phone—even when the customer has *expressly denied* permission for an app that is currently running to access his or her location.

This information appears to be logged in a manner undetectable by the average consumer. It also appears that, when a consumer does become aware of this activity, he or she has no reasonable means to stop it.

Carrier IQ's representatives have informed my office that while it develops the diagnostics software that has come into question, that software is subsequently modified and actually installed by other companies. Each of your companies has publicly acknowledged integrating Carrier IQ software into the handsets you either manufacture or service through a wireless service contract. *See* ComputerWorld, "AT&T, Sprint confirm use of Carrier IQ software on handsets," December 1, 2011.

While I understand and acknowledge the legitimate need for diagnostics software, the data that it appears can be logged through this software appears to go beyond technical diagnostic information. Given this information, I request that you answer the following questions regarding what information your companies receive as a result of the operation of Carrier IQ software on your devices, how you protect and share that information, and what you believe the legal implications of these activities to be:

- (1) On what devices does your company use or install Carrier IQ software?
- (2) As of what date has your company used or installed this software on these devices?
- (3) To the best of your knowledge, how many American consumers use these devices?
- (4) Does your company receive customer location data collected by Carrier IQ software or by Carrier IQ?
- (5) What other data does your company receive that has been collected by Carrier IQ software or by Carrier IQ?
 - a. The telephone numbers users dial?
 - b. The telephone numbers of individuals calling a user?
 - c. The contents of the text messages users receive?
 - d. The contents of the text messages users send?
 - e. The contents of the emails they receive?
 - f. The contents of the emails users send?
 - g. The URLs of the websites that users visit?
 - h. The contents of users' online search queries?
 - i. The names or contact information from users' address books?
 - j. Any other keystroke data?
- (6) If your company receives this data, does it subsequently share it with third parties? With whom does it share this data? What data is shared?
- (7) Has your company disclosed this data to federal or state law enforcement?
- (8) How long does your company store this data?
- (9) How does your company protect this data against hackers and other security threats?
- (10) Does your company believe that its actions comply with the Electronic Communications Privacy Act, including the pen register statute (18 USC § 3121 et seq.), the federal wiretap statute (18 U.S.C. § 2511 et seq.), and the Stored Communications Act (18 U.S.C. § 2701 et seq.)?

- (11) Does your company believe that its actions comply with the Computer Fraud and Abuse Act (18 U.S.C. § 1030)?
- (12) Does your company believe that its actions comply with your privacy policy?
- (13) Does it believe that consumers are aware that this activity is actually occurring on their devices?

I believe that if these reports are verified—and if these activities do not meet specific statutory safe harbors—it is possible that some of these activities may violate federal privacy laws. I am eager to obtain a complete factual record from each of your companies to better evaluate this situation.

I appreciate your prompt attention to this matter, and would appreciate a response by December 14, 2011.

Sincerely,



AL FRANKEN
Chairman, Subcommittee on Privacy,
Technology and the Law