United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510–6275

November 30, 2011

Mr. Larry Lenhart, President and CEO
Carrier IQ, Inc.
1200 Villa Street, Suite 200
Mountain View, CA 94041

Dear Mr. Lenhart,

I am very concerned by recent reports that your company's software—pre-installed on smartphones used by millions of Americans—is logging and may be transmitting extraordinarily sensitive information from consumers' phones, 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 smartphone—even when the customer has *expressly denied* permission for an app that is currently running to access his or her location.

It appears that this software runs automatically every time you turn your phone on. It also appears that an average user would have no way to know that this software is running—and that when that user finds out, he or she will have no reasonable means to remove or stop it.

These revelations are especially concerning in light of Carrier IQ's public assertions that it is "not recording keystrokes or providing tracking tools" (November 16), "[d]oes not record your keystrokes," and "[d]oes not inspect or report on the content of your communications, such as the content of emails and SMSs" (November 23).

I understand the need to provide usage and diagnostic information to carriers. I also understand that carriers can modify Carrier IQ's software. But it appears that Carrier IQ's software captures a broad swath of extremely sensitive information from users that would appear to have nothing to do with diagnostics—including who they are calling, the *contents* of the texts they are receiving, the *contents* of their searches, and the websites they visit.

These actions may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. This is potentially a very serious matter.

I ask that you provide answers to the following questions by December 14, 2011.

(1) Does Carrier IQ software log users' location?

(2) What other data does Carrier IQ software log? Does it log:

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?

(3) What if any of this data is transmitted off of a users' phone? When? In what form?

(4) Is that data transmitted to Carrier IQ? Is it transmitted to smartphone manufacturers, operating system providers, or carriers? Is it transmitted to any other third parties?

(5) If Carrier IQ receives this data, does it subsequently share it with third parties? With whom does it share this data? What data is shared?

(6) Will Carrier IQ allow users to stop any logging and transmission of this data?

(7) How long does Carrier IQ store this data?

(8) Has Carrier IQ disclosed this data to federal or state law enforcement?

(9) How does Carrier IQ protect this data against hackers and other security threats?

(10) Does Carrier IQ believe that its actions comply with the Electronic Communications Privacy Act, including the federal wiretap statute (18 U.S.C. § 2511 et seq.), the pen register statute (18 USC § 3121 et seq.), and the Stored Communications Act (18 U.S.C. § 2701 et seq.)?

(11) Does Carrier IQ believe that its actions comply with the Computer Fraud and Abuse Act (18 U.S.C. § 1030)? Why?

I appreciate your prompt attention to this matter.

Sincerely,

AL FRANKEN
Chairman, Subcommittee on Privacy
Technology and the Law