RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:
ARMED SERVICES
JUDICIARY
HEALTH, EDUCATION, LABOR, AND PENSIONS
AGING

United States Senate
WASHINGTON, DC 20510

702 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

30 LEWIS STREET, SUITE 101
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958
http://blumenthal.senate.gov

May 17, 2011

Mr. Steven A. Ballmer
Chief Executive Officer
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Mr. Jim Balsillie
Mr. Mike Lazaridis
Co-Chief Executive Officers
Research In Motion
295 Phillip Street
Waterloo, Ontario
Canada N2L 3W8

Mr. Stephen Elop
Chief Executive Officer
Nokia Head Office
Keilalahdentie 2-4
P.O. Box 226
FIN-00045 Nokia Group
Finland

Mr. Steve Jobs
Chief Executive Officer
Apple
1 Infinite Loop
Cupertino, CA 95014

Mr. Ted Morgan
Chief Executive Officer
Skyhook Wireless
34 Farnsworth Street
5th Floor
Boston, MA 02210

Mr. Larry Page
Chief Executive Officer
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Ballmer, Mr. Balsillie, Mr. Elop, Mr. Jobs, Mr. Lazaridis, Mr. Morgan, and Mr. Page:

The explosive growth of the mobile computing industry has revolutionized the way that individuals access and use the internet. Virtually overnight, Android phones, iPhones, Blackberries, and other smartphones have quickly become an iconic part of American life. These tools help us to read emails, browse websites, locate stores and restaurants, and run businesses, in ways that would have been unimaginable just a few years ago.

The ubiquity of these devices, however, raises serious privacy concerns regarding the ways in which the companies who own and operate them interact with the wider wireless ("WiFi") internet universe to improve their products and gain competitive advantages. As legislators charged with protecting the rights of our constituents, it is vital that we first understand how third party privacy is assessed, valued, and treated by your businesses. It is for that reason that I write to request information regarding the history, practice, and details surrounding the interception by your companies of wireless data traveling over private wireless networks for the purpose of constructing WiFi maps.

On May 10, 2011, at a Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law hearing entitled, "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy," representatives from the Federal Trade Commission and the Department of Justice, as well as Google and Apple, testified regarding a variety of emerging mobile internet privacy concerns. Much of the discussion focused on the responsibility of companies to respect the privacy of their own consumers when it comes to personal content or location data that might be collected and shared during normal smartphone use. This is an important area of inquiry, and one where I have called for new rules to hold companies accountable for the personal consumer data that they hold.

Another area explored during the May 10 hearing involves the responsibility of companies to respect the privacy of third parties with whom they have no business relationship but whose personal internet data they may nonetheless intercept and utilize for their own business purposes. Representatives from both Google and Apple were asked about their collection of wireless network data for the purpose of building WiFi maps. Maps pinpointing the locations of wireless networks across the world can be extraordinarily valuable to smartphones that use location-based services, since determining the location of a given phone by sensing nearby wireless networks and consulting a WiFi map is quicker and more efficient than constantly consulting GPS satellites.

The construction of WiFi maps, however, has the potential to raise serious privacy concerns. Attempting to document the locations of personal wireless networks in individuals' homes without their knowledge or consent raises issues regarding what constitutes a reasonable expectation of privacy for an ordinary citizen who installs such a network in their home for personal internet use. Those issues become more acute depending on what steps individuals take to affirmatively safeguard their privacy, the more precisely their networks are pinpointed, and the more personal network traffic that is intercepted to make that determination. Localizing those networks to a particular house, rather than a particular block, may raise additional concerns, as does pinpointing the location of encrypted or "hidden" networks, collecting user-assigned wireless network names (called SSIDs), intercepting non-content data traveling between people's computers and their wireless networks, and finally intercepting content data traveling over these networks.

These concerns are perhaps most acute in the context of the Google Wi-Spy scandal, where Google was revealed to have spent three years using Google Maps "Street View" cars to collect bits of users' emails, passwords, browsing history, and other personal information while driving around taking pictures of streets. Google initially denied it was collecting this personal information. The company subsequently revised its story and has since maintained that the collection of this content data was the unintentional result of a piece of experimental software code written by a single engineer. Many have found this explanation unsatisfying in light of the fact that Google reportedly collected and stored content data from around the world and across multiple continents for three whole years without noticing what was happening.

The Google Wi-Spy scandal may represent the most visible example in recent years of a large technology company unequivocally violating the privacy of third parties, but is surely not the first or last such example. The entire enterprise of WiFi mapping highlights these concerns, and it is but one of many such business endeavors. Until companies have a compelling reason to consider the personal privacy of third parties when developing new technology schemes, the drive to extract every potential advantage over competitors will invariably put the rights of ordinary citizens at risk. It is for that reason that I ask each of you to answer the attached list of questions with as much accuracy and specificity as can be obtained. Only by better explaining the history, practice, and details surrounding WiFi mapping can policymakers hope to devise solutions that will build the trust between the American people and your companies that is vital to sustain the incredible technological revolution of mobile computing.

Thank you for your consideration.

Sincerely,

Richard Blumenthal
United States Senate

QUESTIONS REGARDING WIRELESS SIGNAL INTERCEPTION

1. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points for any purpose? If so:

    A. Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from the interception of wireless data transmissions described above.

    B. Please indicate any and all purpose(s) underlying any such signal interceptions.

    C. Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.

    D. Please describe any and all methods initially contemplated and/or implemented for these purposes.

    E. Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.

    F. Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc). For each category of data, please define the term used to reference that category, including an indication of how it is derived.

    G. Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

    H. Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited data frames, payload data, etc.*

        1) If so, please explain how and why such content data is excluded from interception.

        2) If not, please explain how and why such content data is not excluded from interception.

    I. Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited data frames, payload data, etc.*

J. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.

K. Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?

2. Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.

    A. How many wireless access points exist, or have ever existed, in any database of wireless access point locations?

        1) How many of these wireless access points were unencrypted when identified?

        2) How many of these wireless access points were encrypted when identified?

        3) How many of these wireless access points were "hidden" when identified?

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

    A. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

    B. Indirectly valuable for any other purpose.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

    A. Legal or illegal under current federal law;

    B. Legal or illegal under current state law; and

    C. Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.

Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited data frames, payload data, etc.