

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

REBECCA COUSINEAU, individually on her
own behalf and on behalf of all others
similarly situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a Delaware
corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT

PLAINTIFF’S CLASS ACTION COMPLAINT

Plaintiff Rebecca Cousineau (“Plaintiff”) brings this Class Action Complaint against Defendant Microsoft Corporation (“Microsoft” or “Defendant”) based upon its practice of unlawfully tracking its users’ geolocation information through their mobile devices. Plaintiff, for her Class Action Complaint, alleges as follows upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys:

NATURE OF THE ACTION

1. Microsoft intentionally tracks the movements of its users’ mobile devices in direct contravention of their privacy settings and the law. While Microsoft claims that users

1 may opt-out of its location-tracking program, Microsoft has designed its mobile operating
2 software to track its users locations deceptively even after they *affirmatively deny* such
3 consent. As discussed more fully herein, Microsoft effectuates this scheme through its
4 popular mobile operating system (“OS”), Windows Phone 7 (“Windows Phone”), which is
5 used by a variety of manufacturers of mobile devices, such as HTC, Samsung, and LG.
6 Regardless of the device model, Microsoft consciously designed its OS to siphon geographic
7 location information from users and transmit their specific whereabouts to Microsoft’s
8 servers.

9 2. Over the past decade, mobile telephony use among United States consumers
10 has grown exponentially. Seeking to capitalize on this new medium of communication,
11 Microsoft is racing to develop a system that facilitates targeted advertisements to consumers
12 based upon their geographic locations. Before Microsoft is able to effectuate such a
13 marketing campaign, however, it must first compile a digital map by collecting geographic
14 information and unique identifiers from cellular towers, wireless network routers, cellular
15 telephones, and computer systems.

16 3. Faced with the expensive and laborious task of collecting this information,
17 Microsoft has elected to gather instead, the necessary geolocation information through its
18 customers’ mobile devices. In this way, Microsoft uses its customers as a virtual army of
19 surveyors who constantly gather and transmit the geolocation information necessary to build
20 its digital map.

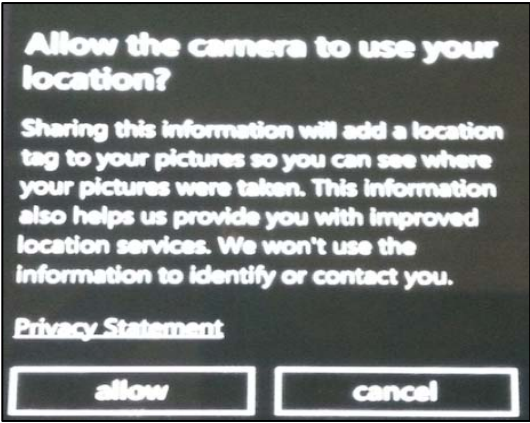
21 4. Microsoft’s scheme is executed through its camera application, which comes
22 standard with a mobile device running the Windows Phone OS. The first time a user opens
23 the camera application, a display screen prompts the user to allow or deny Microsoft access
24 to his or her geolocation:

25 ///

26 ///

27 ///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27



(The above depiction is a true and accurate copy of the Windows Phone OS display screen (“Display Screen”).)

5. Users clicking “cancel” explicitly deny Microsoft access to their geolocations. Unfortunately for its users, however, Microsoft brazenly continues to collect users’ location information, regardless of whether or not the individual chooses “cancel” so as to not allow such information to be tracked. Thus, Microsoft surreptitiously forces even unwilling users into its non-stop geo-tracking program in the interest of developing its digital marketing grid.

6. Still, Microsoft publicly maintains that it only collects geolocation data “with the express consent of the user.” (A true and accurate copy of Microsoft’s Letter to Congress, dated May 9, 2011, is attached hereto as Exhibit A). Nevertheless, and in clear contradiction to its assertions, Microsoft designed its camera application to transmit its users’ geolocation information regularly to Microsoft’s servers—even when the user expressly denies Microsoft access to such information.

7. By and through these actions, Microsoft has refused and continues to refuse to honor its users’ desire to refrain from being tracked.

8. By designing the Windows Phone camera application to thwart users’ attempts to prohibit the collection of their geolocations, Microsoft blatantly disregards its users’ privacy rights, and willfully violates numerous state and federal laws.

///
///

1 **PARTIES**

2 9. Plaintiff Rebecca Cousineau is a natural person and citizen of the state of
3 Michigan.

4 10. Defendant Microsoft Corporation is a Delaware corporation with its principal
5 place of business located at 1 Microsoft Way, in the city of Redmond, state of Washington.

6 **JURISDICTION AND VENUE**

7 11. This Court has jurisdiction over the subject matter of this action pursuant to
8 28 U.S.C. § 1331. This Court has personal jurisdiction over Defendant because it resides in
9 this District, conducts business in this District, and the improper conduct alleged in the
10 Complaint occurred in this District.

11 12. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant
12 resides in this District, conducts business in this District, the improper conduct alleged in the
13 Complaint occurred in this District, and the injury arose in this District. Venue is additionally
14 proper because Defendant transacts significant business in this District.

15 **FACTUAL BACKGROUND**

16 **I. Microsoft Profits from Collecting its Users' Location Data**

17 13. Mobile advertising is projected to become a \$2.5 billion dollar industry by
18 2015.¹ To gain a competitive advantage, Microsoft is using mobile devices running the
19 Windows Phone OS to build a digital map, comprised of cell tower and wireless network
20 ("WiFi") access point information. (Ex. A, p 4.) In turn, this map can be used to help
21 pinpoint the location of users' mobile phones and other devices.

22 14. In the future, Microsoft can use its proprietary database of cell tower and WiFi
23 to deploy targeted advertisements to mobile phone users based upon their geolocations.

24
25
26
27 ¹ See, <http://www.nytimes.com/2011/04/26/technology/26locate.html> (last visited August 30, 2011).

1 15. In order to gather the information for the database described above, Microsoft
2 designed the Windows Phone OS to collect and send geolocation data to its servers when “a
3 user-authorized application has made a request for location.” (Ex. A, p. 4.)

4 16. However, when consumers use certain Windows Phone OS mobile
5 applications, they—regardless of their privacy restrictions—unwittingly transmit specific
6 geolocation data to Microsoft.

7 17. Previously, Microsoft had allowed public access to its database containing the
8 approximate locations of millions of mobile phones, laptop computers, and other devices
9 with WiFi connections.

10 18. Strikingly, researchers were able to show that it is possible to track the
11 approximate whereabouts of individual consumers using information gleaned from
12 Microsoft’s database.² Facing increased scrutiny over privacy concerns raised by the
13 researchers’ discovery, Microsoft recently ceased publication of the contents of its
14 geolocation database.

15 **II. Microsoft Promises Not to Collect Geolocation Data Without User Consent**

16 19. In April of 2011, leaders of the United States House of Representatives
17 Committee on Energy and Commerce sent letters to a number of developers of mobile device
18 operating systems, including Microsoft, requesting information about how their software was
19 designed to track and store users’ locations. In its response to Congress’s inquiry, Microsoft
20 unequivocally stated that the Windows Phone OS never collects geolocation data without the
21 express consent of its users. (Ex. A, pp. 1, 2, 4, 5, 9.)

22 20. Specifically, Microsoft asserted that its OS will “collect data *only* if ... the
23 user has allowed an application to access and use location data.” (Ex. A, p. 4.)

24 21. Microsoft’s representations to Congress were false.

25 **III. Microsoft Intentionally Breaks its Promise to Consumers**

26 _____
27 ² See, Microsoft Curbs Wi-Fi Location Database, http://news.cnet.com/8301-31921_3-20086489-281/microsoft-curbs-wi-fi-location-database/ (last visited August 30, 2011).

1 All persons in the United States that denied their Windows Phone 7 camera
2 application access to their location information, and unwittingly had their geolocation
3 data transmitted to Microsoft's servers.

4 Excluded from the Class are (1) Defendant, Defendant's agents, subsidiaries, parents,
5 successors, predecessors, and any entity in which the Defendant or their parents have
6 a controlling interest and their current and former employees, officers, and directors,
7 (2) the Judge or Magistrate Judge to whom this case is assigned and the Judge's or
8 Magistrate Judge's immediate family, (3) persons who execute and file a timely
9 request for exclusion, (4) the legal representatives, successors, or assigns of any such
10 excluded person, and (5) all persons who had claims similar to those alleged herein
11 finally adjudicated or who have released their claims against Defendant.

12 29. **Numerosity:** The exact number of the members of the Class is unknown and
13 is not available to Plaintiff at this time, but individual joinder in this case is impracticable.
14 The Class consists of tens of thousands of individuals and other entities. Class members can
15 be easily identified through Defendant's records and public records.

16 30. **Commonality:** There are many questions of law and fact common to the
17 claims of Plaintiff and the other members of the Class, and those questions predominate over
18 any questions that may affect individual members of the Class. Common questions for the
19 Class include but are not limited to the following:

- 20 (a) Whether Microsoft continues to collect geolocation data through the
21 camera application included in the Windows Phone 7 operating system
22 when the user denies Microsoft access to that information;
- 23 (b) Whether Microsoft profits, or intends to profit from, the collection of
24 geolocation data obtained as a result of the unlawful practices
25 described more fully herein;
- 26 (c) Whether Microsoft's conduct described herein violates the Stored
27 Communications Act, 18 U.S.C. §§ 2701, *et seq.*;

- 1 (d) Whether Microsoft's conduct described herein violates the Electronic
2 Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*;
- 3 (e) Whether Microsoft's conduct described herein violates the
4 Washington Consumer Protection Act, RCW § 19.86, *et seq.*;
- 5 (f) Whether Microsoft has been unjustly enriched by Plaintiff and the
6 Class; and
- 7 (g) Whether Microsoft has breached its fiduciary duty to Plaintiff and the
8 Class.

9 31. **Typicality:** The factual and legal bases of Microsoft's liability to Plaintiff and
10 to the other members of the Class are the same and resulted in injury to Plaintiff and all of
11 the other members of the Class. Plaintiff and the other members of the Class have all suffered
12 harm as a result of Microsoft's wrongful conduct.

13 32. **Adequate Representation:** Plaintiff will fairly and adequately represent and
14 protect the interests of the Class members, and have retained counsel competent and
15 experienced in complex class actions. Plaintiff has no interest antagonistic to those of the
16 Class and Defendant has no defenses unique to Plaintiff.

17 33. **Predominance and Superiority:** This class action is appropriate for
18 certification because class proceedings are superior to all other available methods for the fair
19 and efficient adjudication of this controversy, since joinder of all members is impracticable.
20 The damages suffered by the individual members of the Class will likely be relatively small,
21 especially given the burden and expense of individual prosecution of the complex litigation
22 necessitated by the actions of Defendant. It would be virtually impossible for the individual
23 members of the Class to obtain effective relief from the misconduct of Defendant. Even if
24 members of the Class themselves could sustain such individual litigation, it would still not be
25 preferable to a class action, because individual litigation would increase the delay and
26 expense to all parties due to the complex legal and factual controversies presented in this
27 Complaint. By contrast, a class action presents far fewer management difficulties and

1 38. The SCA mandates, among other things, that it is unlawful for a person to
2 obtain access to stored communications on another’s computer system without authorization.
3 18 U.S.C. § 2701.

4 39. Congress expressly included provisions in the SCA to address this issue so as
5 to prevent “unauthorized persons deliberately gaining access to, and sometimes tampering
6 with, electronic or wire communications that are not intended to be available to the public.”
7 Senate Report No. 99–541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

8 40. Microsoft has programmed its Windows Phone 7 operating system to store the
9 location information (“the stored file”) of its users. Microsoft has violated 18 U.S.C. §
10 2701(a)(1) because it intentionally accessed consumers’ communications without
11 authorization and obtained, altered, or prevented authorized access to a wire or electronic
12 communication while in electronic storage by collecting location data from the stored file on
13 Plaintiff and the Class’s mobile devices while using the camera application, despite the fact
14 that the user expressly denied Defendant access to that information. At all relevant times,
15 Defendant had actual knowledge of, and benefited from, this practice.

16 41. Additionally, Defendant has violated 18 U.S.C. § 2701(a)(2) because it
17 intentionally exceeded the authorization of consumers to access consumers’ communications
18 and obtained, altered, or prevented authorized access to a wire or electronic communication
19 while in electronic storage by collecting location data from the stored file on Plaintiff and the
20 Class’s mobile devices while using the camera application, despite the fact that the user
21 expressly denied Defendant access to that information. At all relevant times, Defendant had
22 actual knowledge of, and benefited from, this practice.

23 42. As a result of Defendant’s conduct described herein and its violation of §
24 2701, Plaintiff and the Class have suffered injuries. Plaintiff, on his own behalf and on behalf
25 of the Class, seeks an order enjoining Defendant’s conduct described herein and awarding
26 himself and the Class the maximum statutory and punitive damages available under 18
27 U.S.C. § 2707.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

SECOND CAUSE OF ACTION
Violations of the Electronic Communications Privacy Act
18 U.S.C. §§ 2510, *et seq.*
(On behalf of Plaintiff and the Class)

43. Plaintiff incorporates the forgoing allegations as if fully set forth herein.

44. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* (the “ECPA”) broadly defines an “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...” 18 U.S.C. § 2510(12).

45. The ECPA defines an “electronic communications system” as “any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(14).

46. The ECPA broadly defines the contents of a communication. Pursuant to the ECPA, “contents” of a communication, when used with respect to any wire, oral, or electronic communications, include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). “Contents,” when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication. The definition thus includes all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.

47. Defendant’s conduct violated 18 U.S.C. § 2511(1)(a) because Defendant endeavored to intercept and intentionally intercepted Plaintiff’s and Class Members’ electronic communications to, from, and within their mobile devices without consent.

1 48. Defendant's conduct violated 18 U.S.C. § 2511(1)(d) because Defendant
2 endeavored to use and used the contents of Plaintiff's and Class Members' electronic
3 communications to profit from its unauthorized collection and sale, knowing and having
4 reason to know that the information was obtained through interception in violation of 18
5 U.S.C. § 2511(1).

6 49. Defendant intentionally obtained and/or intercepted, by device or otherwise,
7 these electronic communications, without the knowledge, consent or authorization of
8 Plaintiff or the Class.

9 50. Plaintiff and the Class suffered harm as a result of Defendant's violations of
10 the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be
11 appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant
12 as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. §
13 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and
14 attorneys' fees.

15 **THIRD CAUSE OF ACTION**
16 **Violations of the Washington Consumer Protection Act**
17 **RCW 19.86, *et seq.***
(On behalf of Plaintiff and the Class)

18 51. Plaintiff incorporates by reference the foregoing allegations.

19 52. Washington's Consumer Protection Act, RCW § 19.86, *et seq.* ("CPA")
20 protects both consumers and competitors by promoting fair competition in commercial
21 markets for goods and services.

22 53. The CPA prohibits any unlawful, unfair or fraudulent business acts or
23 practices including the employment of any deception, fraud, false pretense, false promise,
24 misrepresentation, or the concealment, suppression, or omission of any material fact.

25 54. As described herein, Microsoft's continued unlawful and unconscionable
26 conduct of transmitting geolocation data after the user has expressly denied Microsoft access
27

1 to such information constitutes an unlawful business practice in violation of RCW § 19.86, *et*
2 *seq.*

3 55. By doing so, Microsoft engaged, and continues to engage, in a deceptive and
4 misleading course of conduct intended to deceive and significantly confuse consumers into
5 purchasing its software (via purchasing any Windows Phone) and using its applications (*i.e.*,
6 its Windows Phone camera application) which constitutes unconscionable commercial
7 practices, deception, fraud, false promises, false pretenses and/or misrepresentations in its
8 interactions with Plaintiff and the Class.

9 56. The ability to control the privacy settings of a consumer product (*i.e.*, access
10 to geolocation information) is material to any transaction because it is likely to affect a
11 consumer's choice of, or conduct regarding, whether to purchase a product. Any deception
12 related to the privacy settings of a consumer product is materially misleading.

13 57. The misrepresentation of the privacy settings of Microsoft's products is likely
14 to mislead a reasonable consumer who is acting reasonably under the circumstances.

15 58. Microsoft has violated the "unfair" prong of the CPA in that their actions
16 caused substantial injury to consumers by failing to disclose that it was accessing consumers'
17 geolocation information after the user has expressly denied Microsoft access to such
18 information. The injury caused by Microsoft's conduct is not outweighed by any
19 countervailing benefits to consumers or competition, and the injury is one that consumers
20 themselves could not reasonably have avoided.

21 59. The act and practice of Microsoft is injurious to the public interest because
22 Microsoft has injured numerous people beyond just Plaintiff. Microsoft has the ongoing
23 capacity to injure members of the public through the conduct alleged in this Complaint.

24 60. Microsoft also violated the CPA by engaging in fraudulent and/or deceptive
25 conduct by representing that it would honor its users' decisions not to have location data
26 recorded and sent to its servers.

27

1 from Microsoft, Microsoft receives a monetary benefit for each and every Windows Phone
2 sold by its partners. Accordingly, Microsoft received and retained money from every
3 Windows Phone transaction.

4 69. Additionally, Microsoft received and retained a monetary benefit from its
5 unlawful conduct described herein by developing a database of geolocation data that will be
6 used in mobile marketing campaigns.

7 70. Defendant appreciates or has knowledge of these benefits.

8 71. Under principles of equity and good conscience, Defendant should not be
9 permitted to retain the money that Defendant has unjustly received as a result of its unlawful
10 actions.

11 72. Accordingly, Plaintiff and the Class seek full disgorgement and restitution of
12 any amounts Microsoft has retained as a result of the unlawful and/or wrongful conduct
13 alleged herein.

14 **PRAYER FOR RELIEF**

15 WHEREFORE, Plaintiff Rebecca Cousineau, individually and on behalf of the Class,
16 prays for the following relief:

17 A. Certify this case as a class action on behalf of the Class defined above,
18 appoint Rebecca Cousineau as class representative, and appoint her counsel as class counsel;

19 B. Declare that Microsoft's actions, as described herein, violate the Stored
20 Communications Act, 18 U.S.C. §§ 2701, *et seq.*, Electronic Communications Privacy Act,
21 18 U.S.C. §§ 2510, *et seq.*, and the Washington's Consumer Protection Act, RCW § 19.86, *et*
22 *seq.*;

23 C. Award injunctive and other equitable relief as is necessary to protect the
24 interests of the Plaintiff and the Class, including, *inter alia*: (i) an order prohibiting Microsoft
25 from engaging in the wrongful and unlawful acts described herein; and (ii) requiring
26 Microsoft to stop collecting geolocation data through the camera application from its users'
27 mobile devices after the user has expressly denied access to that information;

1 D. Award damages, including statutory damages of \$1,000 per violation under
2 the Stored Communications Act, 18 U.S.C. § 2707(c) and the Electronic Communications
3 Privacy Act, 18 U.S.C. § 2520, and punitive damages where applicable, to Plaintiff and the
4 Class in an amount to be determined at trial;

5 E. Award Plaintiff and the Class their reasonable litigation expenses and
6 attorneys' fees;

7 F. Award Plaintiff and the Class pre- and post-judgment interest, to the extent
8 allowable; and

9 G. Award such other and further relief as equity and justice may require.

10 **JURY TRIAL**

11 Plaintiff demands a trial by jury for all issues so triable.

12
13
14 Dated: August 31, 2011

Respectfully submitted,

15 **TOUSLEY BRAIN STEPHENS PLLC**

16 By: /s/ Kim D. Stephens
17 Kim D. Stephens, WSBA #11984
18 1700 Seventh Avenue, Suite 2200
19 Seattle, Washington 98101
20 Telephone: (206) 682-5600
21 Facsimile: (206) 682-2992
22 kstephens@tousley.com

23 Jay Edelson (*pro hac admission pending*)
24 Rafey S. Balabanian (*pro hac admission*
25 *pending*)
26 William C. Gray (*pro hac admission pending*)
27 Ari J. Scharg (*pro hac admission pending*)
EDELSON MCGUIRE, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
Facsimile: (312) 589-6378

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

jedelson@edelson.com
rbalabanian@edelson.com
wgray@edelson.com
ascharg@edelson.com
**Pro hac vice* admissions to be sought

*Counsel for Rebecca Cousineau and the
Putative Class*

EXHIBIT A

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
<http://www.microsoft.com/>



May 9, 2011

The Honorable Fred Upton
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Greg Walden
U.S. House of Representatives
2182 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Mary Bono Mack
U.S. House of Representatives
104 Cannon House Office Building
Washington, D.C. 20515

The Honorable Lee Terry
U.S. House of Representatives
2331 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Marsha Blackburn
U.S. House of Representatives
217 Cannon House Office Building
Washington, D.C. 20515

Dear Chairman Upton, Chairman Walden, Chairwoman Bono Mack, Vice Chair Terry, and Vice Chair Blackburn:

Thank you for the opportunity to respond to your letter of April 25, 2011, in which you seek information about the extent to which smart phones running the Microsoft Windows Phone 7 operating system may collect, use, store and share location data.

The explosive growth of smart phones, the applications they use, and the technologies on which they rely has brought with it tremendous social and economic benefits. Indeed, in the span of just a few short years, the smart phone has become an indispensable device for many consumers. An important part of what makes the smart phone so compelling is the availability of feature-rich location services. Put simply, knowing the general location of a smart phone can help deliver more useful and relevant experiences to users. For instance, location data can facilitate more relevant search results, provide information such as local movie options and directions to the nearest coffee shop, and help a user find nearby friends for an impromptu get together.

To provide these rich experiences, Microsoft collects limited information necessary to determine the approximate location of a device. Collection is always with the express consent of the user and the goal of our collection is never to track where a specific device has been or is going. Rather, our goal when providing users -- or, more specifically, the location-based

applications they select -- with this service is to find landmarks (typically nearby WiFi access points and cell towers) that help us determine the approximate location of a device more quickly and accurately. Microsoft recognizes that consumers should have control over the location information they share and that the information collected should be narrowly tailored to support specific experiences on Windows Phone 7 devices. Therefore, Microsoft designed the location based services on Windows Phone 7 with the following principles in mind:

1. **User Choice and Control.** Microsoft does not collect information to determine the approximate location of a device unless a user has expressly allowed an application to collect location information. Users that have allowed an application to access location data always have the option to access to location at an application level or they can disable location collection altogether for all applications by disabling the location service feature on their phone.
2. **Observing Location Only When the User Needs It.** Microsoft only collects information to help determine a phone's approximate location if (a) the user has allowed an application to access and use location data, and (b) that application actually requests the location data. If an application does not request location, Microsoft will not collect location data.
3. **Collecting Information About Landmarks, Not About Users.** Microsoft's collection of location data is focused squarely on finding landmarks that help determine a phone's location more quickly and effectively. In our case, the landmarks we use are nearby WiFi access points and cell towers. The information we collect and store helps us determine where those landmarks are, not where device users are located. In fact, we've recently taken specific steps to eliminate the use and storage of unique device identifiers by our location service when collecting information about these landmarks. Without a unique identifier, or some other significant change to our operating system or practices, we cannot track an individual device.
4. **Transparency About Microsoft's Practices.** Microsoft gives consumers opportunities to learn more about its location data collection practices. When the user makes a decision to allow an application to access and use location data, Microsoft provides a link to the Windows Phone Privacy Statement,¹ which includes its own section on location services with information describing the data Windows Phone 7 collects or stores to determine location, how that data is used, and how consumers can enable or disable location-based features. Additionally, at the time Windows Phone 7 launched last November, Microsoft published a consumer-friendly Q&A in the "Help and How-To" section of its Windows Phone website to

¹ See <http://www.microsoft.com/windowsphone/en-us/privacy.aspx>

address commonly-asked questions about location services and consumer privacy.² This Q&A provides detailed information on how location services work for Windows Phone 7, the data Microsoft collects to provide location services, and step-by-step instructions (as well as diagrams) on how to enable and disable location services on Windows Phone 7 and the methods Microsoft uses to assemble and maintain its location database. Prior to launch of Windows Phone 7, Microsoft proactively engaged with various government and consumer organizations to start constructive dialogues regarding our location data collection and use practices.

We believe that our careful and deliberate approach to user privacy in the development of the Windows Phone 7 operating system reflects Microsoft's commitment to give users informed choice about the collection and use of location information and to facilitate the delivery of device location information solely at the user's request and solely for the user's benefit. We believe that, when designed, deployed and managed responsibly, the location-based feature of a mobile operating system should function as a tool for the user and the applications he or she elects to use, and not as a means to generate a database of sensitive information that can enable a party to surreptitiously "track" a user.

With this information as background, Microsoft responds below to your specific questions.

1. What location data do devices running your operating system track, use, store, or share?

The collection and use of location data by smart phones can serve a variety of purposes. It therefore is worth clarifying at the outset that the term "location data" can refer to two related but conceptually distinct categories of data: (1) data that is used to determine the approximate location of a device for use by an application; and (2) data that identifies specifically where a device is or has been. The Windows Phone 7 operating system is designed to focus squarely on the first category, and we have taken steps to avoid collecting the type of data described in the second category, which can facilitate user tracking.

When an application on a Windows Phone requests the device's location data to provide a service, the Windows Phone is capable of determining its approximate location based on its proximity to nearby WiFi access points or cell towers, or based on Global Positioning System (GPS) coordinates. The location data that is observed and collected by the Windows Phone 7 operating system to determine the approximate location of the device can depend on a variety of factors, including the device's settings, battery power, signal detection capability (e.g., whether in an "urban canyon" or a more open area), and the level of location precision

² See <http://www.microsoft.com/windowsphone/en-us/howto/wp7/web/location-and-my-privacy.aspx>.

that the application requests. If the Windows Phone is WiFi-enabled, the Media Access Control (MAC) addresses and signal strength of the WiFi access points detected by the phone may be collected by the Windows Phone 7 operating system to determine the phone's approximate location. If a Windows Phone is connected to a cellular network, then identifiers of the cell towers available to the phone may be collected to determine the phone's location. And if GPS is the only location data that is available or is specifically sought by the requesting application, then the latitude, longitude, speed, and direction of the phone, as provided by the GPS, will be collected to determine the phone's location.

The Windows Phone 7 location service typically relies on WiFi access point or cell tower information to determine a phone's approximate location. Generally, location determined by WiFi access points and cell towers will be less precise than GPS. Windows Phone 7 generally relies upon WiFi access point or cell tower information to determine a phone's approximate location because GPS location data is not always available, and when it is, it can draw more heavily on battery power and may take longer to respond to a request for location. Because the Windows Phone 7 operating system is designed to help the user effectuate his or her immediate objectives quickly and efficiently, GPS data is collected only when available WiFi access point or cell towers are not able to resolve a request or a user-authorized requesting application demands it.

To determine the approximate location of a Windows Phone based on the WiFi access point or cell tower information detected by the device, that data must be compared against a database that Microsoft maintains that correlates such information to latitude and longitude data. We may store a portion of our WiFi access point and cell tower database on the phone in order to resolve location requests without making a request to our database, which resides in the cloud and thus can take more time and result in data usage. This snippet of our database is only stored on a user's phone if a user-authorized application has made a request for location and benefits the user by allowing subsequent requests for location in the same general area to be resolved quickly. This database snippet contains information about nearby WiFi access points and cell towers in the area (on average a 5-6 square kilometer area) where the user made the request. It does not show where a user is or has been within that area.

Regardless of the types of location data that *can* be collected, the Windows Phone 7 operating system will collect location data *only* if (1) the phone's location service capability is enabled, (2) the user has allowed an application to access and use location data; and (3) the user-authorized application actually requests location data.³ If these three elements are satisfied, the approximate location of the device is provided to the application, so the application can provide its location aware features.

³ The only exception to this general rule is when a user makes a request to find their phone using the "Find My Phone" service from their online account. In that instance, the location of the device will be determined regardless of the state of the location service control on the device because we are attempting to honor the user's request to find their phone.

If a user has allowed an application to access location, only the approximate LAT/LONG, speed, direction and altitude of the phone are provided to the requesting application by Microsoft's location service. Information about the available cell towers, WiFi access points and device identifiers are not sent to applications by our location service. Because application providers have some discretion as to how they use location data once they receive it, Microsoft specifically recommends in the Windows Phone 7 Privacy Statement that users review the privacy policies and practices of the applications that they permit to access their phones' location information. Additionally, we require third party application developers who create applications that utilize our location services to, among other things: (1) provide an in-application control to disable use of location by the application; (2) obtain a user's opt-in consent before sharing location data with a third party; (3) use location data only as necessary to provide the location aware features of the application; and (4) make a privacy policy available to users describing the collection and use of location by the application.⁴

Similar to other operating systems, when Microsoft first designed and implemented location services for Windows Phone 7, it programmed its system to collect device identifiers and store them for a limited time. While collecting device identifiers can help assemble and refine a database of available WiFi access points and cell towers more quickly and effectively than without them, these identifiers have diminishing value over time. Given the declining utility of device identifiers, Microsoft recently discontinued its storage and use of device identifiers. Further, as part of its next scheduled update to existing Windows Phone 7 devices, updated devices will no longer send device identifiers to the location service and new phones arriving this fall will not send device identifiers to the location service.

2. Why does the device track, use, store, or share that data?

Microsoft believes that the ability of a mobile operating system to provide location data to user-authorized applications can result in substantial user benefits, so long as the provision of such data is undertaken responsibly, is adequately protected, and is the result of user choice, including sufficient user awareness, consent, and controls.

Windows Phone 7 collects, stores and uses location data so that it can meet the demands of users to provide location to user-authorized applications that offer location aware features. Applications rely on location data for many reasons. Mapping applications, for example, use location data to identify and provide turn-by-turn directions to a particular location. Other applications may use location data to help identify the nearest retail store, restaurant or coffee shop. Still other applications may use location data to locate friends who

⁴ See <http://download.microsoft.com/download/A/B/A/ABA09BC7-8338-4C04-9DA9-1224CD575636/Windows%20Phone%207%20Application%20Certification%20Requirements.p>

df.

may be traveling in the vicinity. For example, a user may download an application that provides movie reviews, trailers and helps the user find the closest cinema to buy tickets.

3. *Where on the device is the data stored; how is it used, stored, or shared; how is it protected?*

There are three instances in which location data may be stored on the phone. The first instance is when a user has expressly enabled the "Find My Phone" feature on the phone or made a request to find the phone from the user's online account. This feature allows a user to remotely find the current location of the phone in the event it is lost. To provide this feature, only the last observed location of the device is stored on the phone, which is updated approximately every six hours.

The second instance is when we download a portion of our database of known WiFi access points and cell towers to the phone. We do this so that we can quickly respond to a user-authorized application request for location. It is impractical to store the entire database locally on the phone, but small portions of the database that show nearby WiFi access points and cell towers can resolve requests for location more quickly because the request would not need to be made to our cloud based database. This information on the phone is protected so that only the location service can access it. No other applications or phone functions have access to this data and this data is not transferred to a user's personal computer when a user tethers or connects their device. The only time this data would be transferred to a user's personal computer is when the user creates an encrypted backup as part of the process of updating the phone. Again, this temporary storage of a portion of our location database occurs only if location services are enabled and a user-authorized application makes a request for location. Further, it only shows nearby WiFi access points and cell towers over a roughly 5-6 square kilometer area. It does not show where a user is or has been within that area. We also limit the amount of data that can be stored from this database on the phone.

The third instance in which location data may be stored on the phone is when data about nearby WiFi access points and cell towers is temporarily stored as part of our efforts to update and improve our database of available WiFi access points and cell towers. For example, a user may be using his or her movie application to find local movie times in a location where we have outdated or little to no information about nearby WiFi access points and cell towers. In those cases, Microsoft uses GPS to help provide location to the requesting application and also will look for the WiFi access points and cell towers that the device can detect from that location. The information about nearby WiFi access points and cell towers along with the corresponding GPS coordinates are temporarily stored on the device and are sent encrypted over HTTPS the next time the device either: (1) makes another request for location, or (2) the user connects to WiFi. Similar to the location data stored on the phone in the second instance, this is data that is used to determine the location of nearby WiFi access points and cell towers, not the location of a user. This data is not transferred to a personal computer and is encrypted when transmitted to Microsoft. Further, this data is not stored on a file on the device and is not designed to be accessible by any applications or features of the phone. The storing and

sending of this data about nearby WiFi access points and cell towers is used to update and improve our location database, so that the next time a device makes a request for location in that same area, our location service can provide location without relying on GPS.

4. How is that data accessible and who can access it? Is the data automatically transferred to your company or to other devices, or to third parties? If so, how and why? Is there any other manner in which the data can be transferred to or obtained by your company, or by other devices, or by third parties and, if so, how and why?

The location data stored on the phone is only accessed and used by Microsoft to calculate the location of a phone and provide it to user-authorized applications requesting location. The information stored on the phone is not made available to applications, other features of the phone or to third parties. Whenever this data is transferred from the phone to Microsoft, it is sent encrypted over HTTPS. The only time any of the data is transferred to a personal computer is when an encrypted backup of the phone is made when a user chooses to update a phone.

5. Is the user informed of, or given an opportunity to prevent, such tracking, use, storing, or sharing of data and, if so, how? Can the end-user disable the tracking, use, storing, and sharing of such data? Can the user delete the data?

A user must expressly allow an application to access and use location and such applications must actually request location before Windows 7 Phone can attempt to determine a device's location. Our Privacy Statement provides step-by-step instructions on how a user can enable or disable access to a phone's location information for a specific application, or enable or disable access to a phone's location information for all applications. If the location services on the phone are disabled or if a user-authorized application is not making a specific request for location, Microsoft will not collect, use or store any information used to determine the location of a device. Specific instructions for enabling and disabling the location services feature on a Windows 7 Phone is provided in our Privacy Statement,⁵ and this same information (along with helpful diagrams) is provided in the "Help and How-To" section of the Windows Phone website.⁶

6. How long does the device store the data?

The length of storage of location data on a device depends on the unique circumstances of the device and the actions of the user. For example, heavy users of location services will have location data stored on the phone frequently uploaded or updated. Less frequent users may have data persist for a greater period of time, but at the same time, the data would be

⁵ See *supra*, note [1](#).

⁶ See *supra*, note [2](#).

staler. In any event, other than the last known location of the phone used to provide the Find My Phone service, the location data that is stored on the phone is for the purpose of determining the location of nearby WiFi access points and cell towers, not the precise movements of users. While we cannot give precise storage times for location data stored on the phone, we can describe the circumstances under which location data stored on the phone is deleted, transferred or updated from the phone.

The last known location of the phone that is stored if the user has enabled the "Find My Phone" service will be stored on the phone until the user disables the service. Again, only the last known location of the phone is stored on the phone (based on the last time the service requested location); there is no historical record of these observations stored on the phone.

The snippets of our database of WiFi access points and cell towers that are stored on the device to more quickly resolve location requests are set to expire after 10 days and will be removed from the device either: (1) the next time a request is made from the phone to that snippet data after the expiration date; or (2) the local storage limit for this data has been exceeded at which point all expired snippets are removed from the phone.

The data about nearby WiFi access points and cell towers used to update and improve our database only is stored until the next time the device either: (1) makes another request for location; or (2) the user connects to WiFi at which point the data are sent to Microsoft encrypted over HTTPS.

None of the data that is temporarily stored on the device to provide location based services is synced to a personal computer except as part of an encrypted backup that is created when a user chooses to update their device.

7. Section 222 of the Communications Act contains privacy provisions. Do those provisions apply to you? Should they? Does it make sense that similar information is afforded different privacy protections depending on what entity does the collecting and what service the data is collected from, especially since the entities collecting such information are increasingly competing against each other in today's information age?

The plain language of Section 222 of the Communications Act demonstrates that it applies only to providers of telecommunications services. Developers of mobile operating systems do not provide telecommunications services and thus are not subject to Section 222. Nevertheless, like many other entities that do not provide telecommunications services, developers of mobile operating systems (and providers of applications that run on those systems) are subject to similar privacy laws and regulations under Section 5 of the Federal Trade Commission Act -- laws and regulations to which providers of telecommunications services are not subject due to the "common carrier exemption" that applies to them under that Act. Developers of mobile operating systems and applications also are subject to state unfair and deceptive trade practice laws, which address privacy issues. And because mobile operating systems and applications typically are deployed globally, they also are subject to

privacy laws and regulations outside the U.S., many of which contain far more restrictive provisions than Section 222 and do not apply to providers of telecommunications services that do not operate in those jurisdictions. Although Section 222 does not and should not apply to developers of mobile operating systems and applications, it nevertheless is worth noting that the operation of location services in the Windows Phone 7 operating system is consistent with the requirements of Section 222 (and, more specifically, Section 222(f)) because it does not disclose location information without the consent of the user.

* * *

Again, Microsoft appreciates the opportunity to provide you with this information. Please direct any further questions regarding this matter to the undersigned.

Respectfully submitted,

Andy Lees
President, Mobile Communications Business

cc: The Honorable Henry A. Waxman, Ranking Member
House Energy and Commerce Committee

The Honorable Anna G. Eschoo, Ranking Member
House Subcommittee on Communications and Technology

The Honorable G.K. Butterfield, Ranking Member
House Subcommittee on Commerce, Manufacturing and Trade

EXHIBIT B

Research by Samy Kamkar

samy@samy.pl

<http://samy.pl>

August 23, 2011

Updated: August 27, 2011

Summary:

When using the prepackaged "Camera" application on a mobile phone running Windows Phone 7, upon initially accessing the Camera application, the phone asks whether you wish to share your location. When hitting "cancel" to prevent your location information from being shared, the phone continues to intermittently transmit information from wifi networks and cellular towers to a host owned by Microsoft Corporation leading to the user's location.

In addition, the phone begins sending location information while the location sharing dialog is open before the user has a chance to allow or disallow the sharing of this location information.

Tests performed on:

Phone model: Samsung Omnia 7

Software: Windows Phone 7

OS Version: 7.0.7004.0

Firmware revision number: 2424.10.11.4

Hardware revision number: 3.15.0.4

Radio software version: 2424.10.11.1

Radio hardware version: 0.0.0.800

Bootloader version: 4.11.2.6

Chip SOC version: 0.36.2.0

SIM card carrier: AT&T

Physical location of the device during tests:

1140 N. Formosa Avenue

West Hollywood CA 90046

Additionally, tests were confirmed on a separate mobile device using a newer version of the OS and firmware:

Phone model: Samsun Omnia 7

Software: Windows Phone 7

OS Version: 7.0.7392.0

Firmware revision number: 2424.11.1.1

Hardware revision number: 3.15.0.4

Radio software version: 2424.11.1.1

Radio hardware version: 0.0.0.800

Bootloader version: 4.1.0.5

Chip SOC version: 0.36.2.0

When using the default Camera application on the Windows Phone 7 software for the first time, as well as after a full reset of all configuration settings, the software asks the following:

"Allow the camera to use your location? Sharing this information will add a location tag to your pictures so you can see where your pictures were taken. This information also helps us provide you with improved location services. We won't use the information to identify or contact you. Privacy Statement." The user is given the option to "allow" or "cancel."

While this prompt is displayed, the phone is already sending information regarding the user's location consistently, and is slightly unexpected behavior.

If the user hits "allow", the phone continues to the camera application and continues to send location info, as expected.

However, if the user hits "cancel", the phone continues to the camera application, however will intermittently send location information to a domain owned by Microsoft Corporation.

Here are two example packets that were sent while the phone was set to not transmit location information (after hitting "cancel" to the location sharing dialog):

HTTPS request to inference.location.live.net:443:

```
POST /inferenceservice/v21/pox/GetTileUsingPosition
HTTP/1.1
Accept: */*
Accept-Language: hu-HU
Content-Type: application/xml; charset=utf-8
UA-CPU: ARM
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
5.1)
Host: inference.location.live.net
Content-Length: 1014
Connection: Keep-Alive
Cache-Control: no-cache

<?xml version="1.0" encoding="UTF-8"?><GetTileUsingPosition
xmlns="http://inference.location.live.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><RequestHeader
><ApplicationId>00000001-7eba-4f0d-82e5-
8f88bd1c2e8c</ApplicationId><DeviceProfile DeviceType="WM7"
ClientGuid="f842a4f5-34df-1ed4-7d13-72d6f9ff94fc"
OSVersion="7.0.7004.WM7_7.0_Ship(mojobld).20100916-1429"
```

```
LFVersion="2.0" ExtendedDeviceInfo="SAMSUNG/OMNIA7"  
Platform="SAMSUNG Electronics/SAMSUNG  
MITs/I8700XXJK1/35367904137101801"  
DeviceId="f5a442f8df34d41e7d1372d6f9ff94fcfe36b56f"/><Autho  
rization/><TrackingId>6a1089a6-1d8b-5cf9-56b1-  
70499a23c6ab</TrackingId><Timestamp>2011-06-  
28T19:15:19.113-  
08:00</Timestamp></RequestHeader><TileParameters  
TileSizeInBytes="100000" BlobType="Wm7Hash1XmlText"  
DeltaType="Complete" IncludeTileData="Complete"  
BeaconGroupMask="Gsm"/><Position Latitude="34.0907297"  
Longitude="-118.3485880" Altitude="0"/><OperatorId  
mcc="310" mnc="410"/></GetTileUsingPosition>
```

Notice the latitude and longitude sent. Additionally, cell tower information (mcc, mnc) were sent which can also lead to geolocation information.

```
A separate HTTPS packet sent to inference.location.live.net:443:  
POST /inferenceservice/v21/pox/GetLocationUsingFingerprint  
HTTP/1.1  
Accept: */*  
Accept-Language: hu-HU  
Content-Type: application/xml; charset=utf-8  
UA-CPU: ARM  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT  
5.1)  
Host: inference.location.live.net  
Content-Length: 1160  
Connection: Keep-Alive  
Cache-Control: no-cache
```

```
<?xml version="1.0" encoding="UTF-  
8"?><GetLocationUsingFingerprint  
xmlns="http://inference.location.live.com"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><RequestHeader  
><ApplicationId>00000001-7eba-4f0d-82e5-  
8f88bd1c2e8c</ApplicationId><DeviceProfile DeviceType="WM7"  
ClientGuid="f842a4f5-34df-1ed4-7d13-72d6f9ff94fc"  
OSVersion="7.0.7004.WM7_7.0_Ship(mojobld).20100916-1429"  
LFVersion="2.0" ExtendedDeviceInfo="SAMSUNG/OMNIA7"  
Platform="SAMSUNG Electronics/SAMSUNG  
MITs/I8700XXJK1/35367904137101801"  
DeviceId="f5a442f8df34d41e7d1372d6f9ff94fcfe36b56f"/><Autho  
rization/><TrackingId>9dcb10b0-b514-4d1e-1bcb-
```

```
75eed4376441</TrackingId><Timestamp>2011-06-
28T19:15:08.240-
08:00</Timestamp></RequestHeader><BeaconFingerprint><Detect
ions><Gsm7 mcc="310" mnc="410" cid="11202" lac="55047"
arfcn="0" baseid="0" rx="0" ta="0"/><Wifi7
BssId="16:9a:dd:84:4e:b7" rssi="-65"/><Wifi7
BssId="10:9a:dd:84:4e:b7" rssi="-67"/><Wifi7
BssId="30:46:9a:44:be:53" rssi="-85"/><Wifi7
BssId="00:16:b6:dc:99:e4" rssi="-87"/><Wifi7
BssId="00:1e:8c:cd:0e:59" rssi="-
91"/></Detections></BeaconFingerprint></GetLocationUsingFin
gerprint>
```

In these packets, we can see some interesting information:

ApplicationID: 00000001-7eba-4f0d-82e5-8f88bd1c2e8c

This appears to be a unique identifier for the application being used, however remained the same across two different mobile devices.

ClientGuid: f842a4f5-34df-1ed4-7d13-72d6f9ff94fc

This appears to be a unique identifier to the mobile device being used and remains static across all requests.

ExtendedDeviceInfo: SAMSUNG/OMNIA7

The type of phone (hardware) being used.

DeviceType: WM7

The mobile operating system being used.

OSVersion: 7.0.7004.WM7_7.0_Ship(mojobld).20100916-1429

The version of the mobile operating system being used.

Platform: SAMSUNG Electronics/SAMSUNG

MITs/I8700XXJK1/35367904137101801

Additional information on the mobile device (hardware) being used.

DeviceId: f5a442f8df34d41e7d1372d6f9ff94fcfe36b56f

Another unique identifier of the phone which remains constant in all packets sent.

TrackingId: 6a1089a6-1d8b-5cf9-56b1-70499a23c6ab

A tracking identifier that seems to be related to uniquely identifying the packet. This changes in each tracking request.

Timestamp: 2011-06-28T19:15:19.113-08:00

A timestamp of when the phone found this tracking information, allowing the remote side to know at what point in time the device was at this location.

Latitude: 34.0907297

Longitude: -118.3485880

Approximate latitude and longitude coordinates of the phone.

Mcc: 310

Mnc: 410

Cid: 11202

Lac: 55047

Cellular tower information which can also help lead to the location of the mobile device.

Bssid="16:9a:dd:84:4e:b7" rssi="-65"

Bssid="10:9a:dd:84:4e:b7" rssi="-67"

Bssid="30:46:9a:44:be:53" rssi="-85"

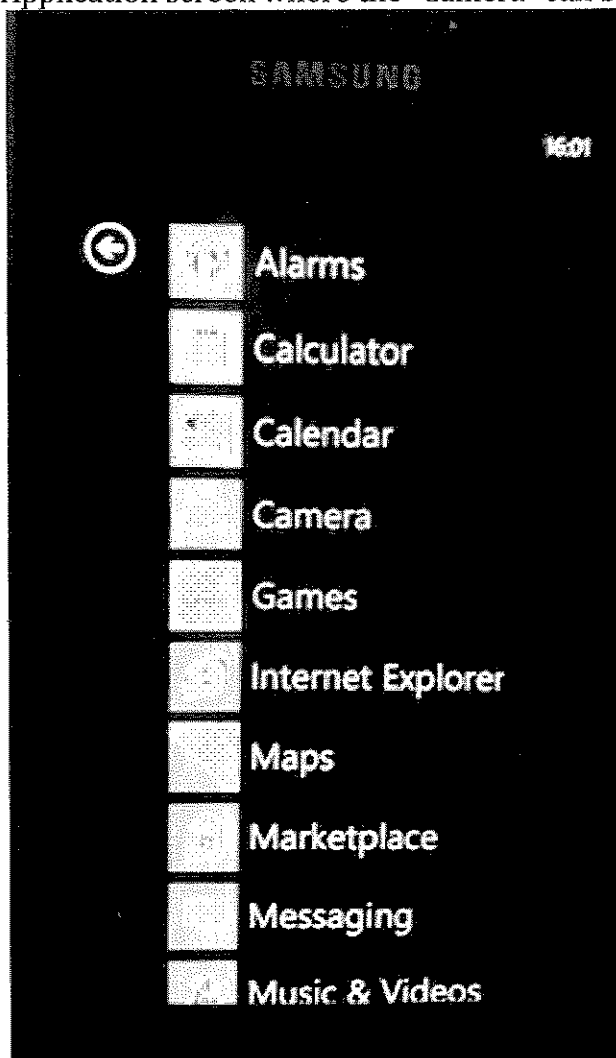
Bssid="00:16:b6:dc:99:e4" rssi="-87"

Bssid="00:1e:8c:cd:0e:59" rssi="-91"

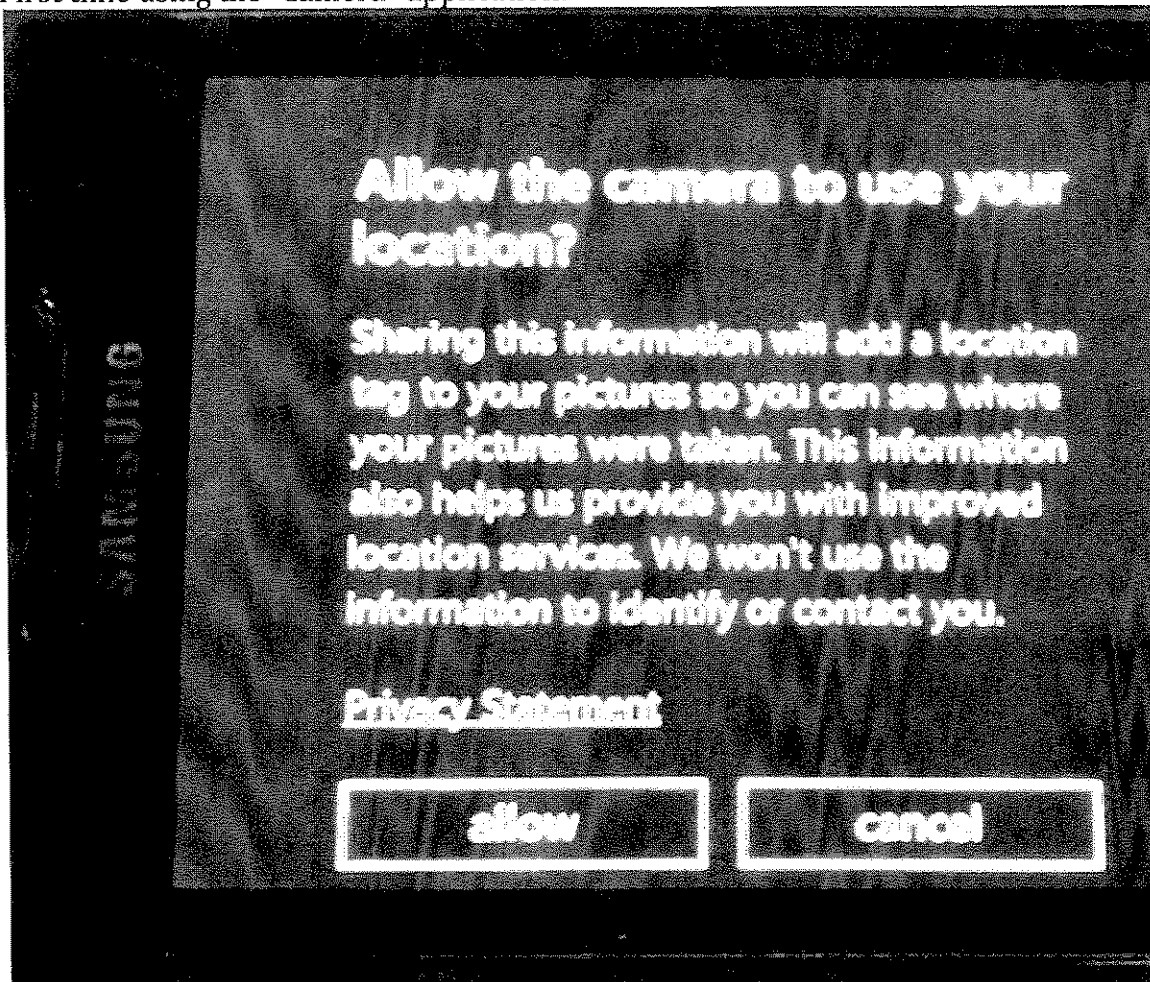
Wireless router MAC addresses (BSSIDs), unique to every router in the world, along with RSSI, or signal strength information. This allows them to correlate the routers with location, as well as using the signal strength information to help triangulate a more accurate position of the user.

The Windows Mobile operating system is clearly sending information that can lead to accurate location information of the mobile device regardless of whether the user allowed the Camera application to share location information or not.

Application screen where the "Camera" can be accessed:



First time using the "Camera" application:



Screenshot of the "Settings->about" screen:

