IN THE SUPERIOR COURT OF THEDISTRICT OF COLUMBIA
CIVIL DIVISION

ELECTRONIC PRIVACY INFORMATION CENTER On behalf of itself, its members and the General Public
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009

Plaintiff,

v.

ACCUWEATHER INTERNATIONAL, INC.
385 Science Park Road,
State College, PA 16803

Defendant.

Case No. 2018 CA 001870 B

COMPLAINT

On behalf of itself, its members and the general public, Plaintiff Electronic Privacy Information Center ("EPIC"), a non-profit organization, brings this action against Defendant AccuWeather International, Inc. ("AccuWeather") regarding the company's deceptive and unlawful tracking of consumers' location through their mobile devices and the disclosure of personal location data to third party companies without consumers' knowledge or consent. Specifically, EPIC alleges two categories of deceptive business practices committed by AccuWeather, based upon information, belief, and the investigation of Counsel. First, AccuWeather collected and disclosed data revealing consumers' location even when consumers expressly denied AccuWeather permission to track their location. Second, AccuWeather presently collects and discloses personal location data for advertising purposes even when consumers give permission only to use their personal location data for weather forecasts and alerts.

SUMMARY OF THE COMPLAINT

1. AccuWeather is one of the world's largest weather media companies.[1]

2. AccuWeather offers a weather application ("app") for sale in the District of Columbia through Apple's iOS app store for consumers to purchase and download to their iPhones and iPads.[2]

3. AccuWeather serves consumers, who are users of the app, in the District of Columbia.

4. AccuWeather has and continues to collect consumers' personal location data (including precise latitude, longitude, and altitude data) and disclose that data to third parties for targeted advertising purposes.

5. As of August 2017, AccuWeather was collecting and disclosing to its marketing partner, Reveal Mobile, WiFi network information that revealed consumers' location, even when those consumers had expressly denied AccuWeather permission to track their location.

6. AccuWeather continues to materially misrepresent to consumers the extent to which it collects, uses, and discloses their personal location data.

7. AccuWeather continues to disclose consumers' personal location data to third parties for targeted advertising purposes, even when those consumers have granted permission only to use their personal location data for weather forecasts and alerts.

8. AccuWeather has and continues to profit from the deceptive and unlawful collection, use, and dissemination of consumers' personal location data.

---

[1] *See* AccuWeather, *About AccuWeather* (2018), https://corporate.accuweather.com/about ("Nearly 2 billion people worldwide rely on AccuWeather").

[2] *AccuWeather: Weather Tracker*, App Store Preview (2018) (showing a current rank of #3 in the Weather category, behind Weather Live and The Weather Channel), https://itunes.apple.com/us/app/accuweather-weather-tracker/id300048137?mt=8.

9. EPIC brings this action on behalf of itself, its members and the general public, seeking injunctive and declaratory relief including an injunction barring AccuWeather from collecting, disclosing, or allowing any third party to collect, consumers' personal location information without providing clear and prominent notice and obtaining consumers' express, affirmative consent.

JURISDICTION AND VENUE

10. This Court has personal jurisdiction over the parties in this case.

11. EPIC is a non-profit organization incorporated in the District of Columbia and, by filing this Complaint, consents to this Court's jurisdiction.

12. AccuWeather is headquartered in State College, Pennsylvania.

13. AccuWeather has consumers in the District of Columbia and has collected and used the location data of consumers in District who have installed the AccuWeather app on their iPhones or iPads. AccuWeather targets consumers in the District of Columbia with location-specific advertisements and services.

14. This Court has subject matter jurisdiction over this action pursuant to D.C. Code §§ 28-3905(k)(1)(B), (k)(1)(D), and (k)(2).

15. Venue is proper in the District under 28 U.S.C. § 1391(b). A substantial part of the events giving rise to this action, including the collection, use, and disclosure of consumers' location data, occurred in this District.

PARTIES

16. Plaintiff Electronic Privacy Information Center ("EPIC") is a 501(c)(3) non-profit public-interest organization and research center, incorporated in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to

protect privacy, freedom of expression, and democratic values in the information age.[3] EPIC is a public interest organization within the meaning of DC Code § 28-3905(k)(1)(D).

17. EPIC has a strong nexus to the consumers injured by AccuWeather's business practices. For over two decades, EPIC has worked to protect the privacy Internet users. EPIC has a particular interest in protecting consumers from invasive location tracking practices. EPIC maintains resources dedicated to educating the public about the unlawful collection, use, and disclosure of personal location data.[4] EPIC seeks to educate the public how companies surreptitiously gather personal location data and invade consumer privacy by tracking their movements. EPIC has previously submitted complaints to the Federal Trade Commission concerning companies' deceptive location tracking practices.[5] EPIC has also participated as amici in numerous cases involving location privacy.[6] And EPIC has opposed the warrantless collection of location data by law enforcement agencies.

18. By deceptively collecting consumers' personal location and sending that data to a third party, AccuWeather has frustrated EPIC's mission to protect privacy and to ensure that consumers are protected from unlawful location tracking.

---

[3] *About EPIC*, https://epic.org/about/ (2018).
[4] EPIC, *Location Privacy*, https://epic.org/privacy/location/ (2018).
[5] *See, e.g. In the Matter of Google, Inc.*, (2017) (EPIC Complaint, Request for Investigation, Injunctive and Other Relief), https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf (concerning Google's tracking of consumers' in-store purchases); *In the Matter of Uber Technologies, Inc.*, (2015) (EPIC Complaint, Request for Investigation, Injunctive and Other Relief), https://epic.org/privacy/internet/ftc/uber/Complaint.pdf (concerning Uber's deceptive location tracking practices).
[6] *See, e.g.*, Brief of *Amici Curiae* EPIC et. al, *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2016), *cert. granted* 137 S. Ct. 2211 (2017) (No. 16-402) (concerning law enforcement's warrantless access to cell phone location data); Brief of *Amici Curiae* EPIC et. al, *Riley v. California*, 134 S. Ct. 2473 (2014) (concerning the warrantless search of a cell phone incident to arrest); Brief of *Amici Curiae* EPIC, et. al, *United States v. Jones*, 565 U.S. 400 (2012) (concerning the warrantless tracking of a vehicle using GPS).

19. Defendant AccuWeather International, Inc. is a weather media company founded in 1962 and headquartered in State College, Pennsylvania.[7] It delivers weather forecasts and weather news through "smart phones, tablets, free wired and mobile Internet sites via AccuWeather.com."[8] AccuWeather also sells a weather app through Apple's iOS app store.

20. EPIC brings this action as a non-profit public interest organization on behalf of the general public under D.C. Code § 28-3905(k)(1)(C). EPIC is a non-profit organization established under D.C. Code § 28-3901(a)(14). EPIC is a public-interest organization as defined in D.C. Code § 28-3901(a)(15).

21. Defendant AccuWeather is a merchant as defined in D.C. Code § 28-3901(a)(3).

BACKGROUND

The Significant Consumer Privacy Interests in Location Data

22. Mobile device location data is among the most sensitive personal information; it can reveal the most intimate details of a person's life. Location data precisely records where a particular person is at a particular moment in time.

23. Today, almost everyone carries a cell phone. The U.S. Supreme Court recently observed that, "the proverbial visitor from Mars might conclude they were an important feature of the human anatomy." *Riley v. California,* 134 S. Ct. 2473, 2484 (2014). But cell phone location data provides a far more intimate portrait of a person's private life than most people realize. Cell phone location records provide a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political professional, religious, and sexual associations." *Riley* 134 S. Ct. at 2490 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

---

[7] AccuWeather, *About AccuWeather*, https://corporate.accuweather.com/about.
[8] *Id.*

24. A Government Accountability Office ("GAO") study found that the collection of location data poses serious risks to consumer privacy.[9] Storing location information over time "create[s] a detailed profile of individual behavior, including habits, preferences, and routes traveled," the exploitation of which can lead to identity theft or threats to personal safety.[10]

25. Location data is especially vulnerable to hackers, who can use it to commit stalking or burglary. For example, a website called "Please Rob Me" aggregated location information from the mobile app Foursquare and other location-based services and published a list "of all those empty homes out there" waiting to be robbed because location data suggested that no one was home.[11]

26. Besides these risks, there are many other reasons consumers wish to keep their location data private. For instance, if a consumer visits a cancer clinic, it can reveal that she has cancer. If a consumer visits an elementary school, it can reveal that she has young children. Indeed, location data is prized by advertisers precisely because it reveals intimate details about a person's life.

27. Consumers are deeply concerned with controlling access to their personal information. 93% of consumers say that it is important to control who has access to their personal information, and 74% of consumers say it is *very* important.[12] 90% of consumers say it

---

[9] U.S. Gov. Accountability Office, GAO-14-649T, *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers* (2014), https://www.gao.gov/products/GAO-14-649T.

[10] *Id.*

[11] *Please Rob Me: Site Tells The World When You're Not Home*, Huffington Post (May 25, 2011), https://www.huffingtonpost.com/2010/02/17/please-rob-me-site-tells_n_465966.html.

[12] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center, (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

is important to control what information is collected about them, and 65% of consumers say it is very important.[13]

Apple Requires Companies to Obtain Consumers' Express Affirmative Consent to Access Personal Location Data Using the "Location Services" Function

28. In response to these concerns, Apple requires app companies to obtain consumers' express affirmative consent before accessing their location. Apple also requires companies to notify consumers of why they are requesting location data.[14]

29. Mobile devices, including phones running the Apple iOS operating system, have the ability to identify their precise location, at a specific moment in time, using several different techniques. Devices are equipped with GPS receivers,[15] Bluetooth antennas,[16] wireless network radios,[17] and cellular network radios.[18] Mobile devices running Apple's iOS operating system have a "location services" feature that "uses GPS, Bluetooth, crowd-sourced WiFi hotspot, and cell tower to determine the location of your device."[19]

---

[13] *Id.*

[14] Apple, *Requesting Permission*, https://developer.apple.com/ios/human-interface-guidelines/app-architecture/requesting-permission/ (last visited Dec. 19, 2017).

[15] The Global Positioning System is a "U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services." Nat'l Coordination Office for Space-Based Positioning, Navigation, and Timing, *What is GPS?* (2017), https://www.gps.gov/systems/gps/. Consumer GPS devices receive "signals from the GPS satellites and uses the transmitted information to calculate the user's three-dimensional position and time." *Id.*

[16] Bluetooth® is a radio-based communications standard used to connect various devices. *Bluetooth Technology* (2018), https://www.bluetooth.com/bluetooth-technology/. Bluetooth radios can be tracked using a "real-time location tracking system . . . . to monitor movements within a physical space." Accuware, *Bluetooth Beacon Tracker* (2018), https://www.accuware.com/products/bluetooth-beacon-tracker/.

[17] Wireless networks enable radio signal communications under standards (referred to as 802.11) established by the Institute of Electrical and Electronics Engineers (IEEE). *IEEE 802.11 Wireless Local Area Networks* (2018), http://www.ieee802.org/11/. All mobile devices, including Apple iOS devices, are equipped with wireless networking capabilities. Wireless networking signals can also be used to locate a mobile device. *See* Wigle, *Frequently Asked Questions* (2018), https://wigle.net/faq/.

[18] Cell phone carriers offer data access over their networks, which operate under radio spectrum rules established by the Federal Communications Commission. *See* Fed. Commc'ns Comm'n, *Wireless Services* (2017), https://www.fcc.gov/wireless/wireless-services.

[19] Apple, *About Location Services and Privacy* (2017), https://support.apple.com/en-us/HT207056.

30. Apple provides for specific user settings in iOS that "protect your private information, including your location, on your iPhone, iPad," and other devices.[20] The system is configured such that "you need to enable Location Services and give permission to each app or website before it can use your location data."[21]

31. AccuWeather and other companies can collect personal location data from an iOS device by obtaining permission to access the Application Programming Interface (API),[22] which is part of Apple's "Core Location" framework.[23]

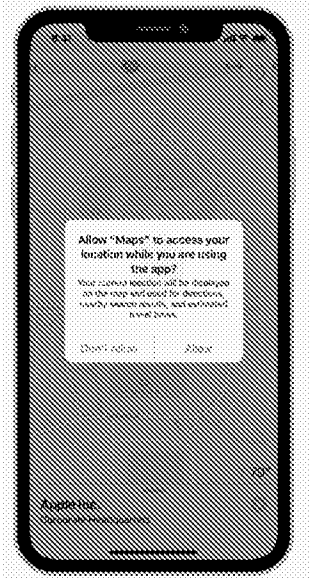
32. A company must obtain the consumer's express affirmative consent to access the Core Location API.[24] As Apple explains in its developer guide, "[a]lthough people appreciate the convenience of using an app that has access to this information, they also expect to have control over their private data."[25]

33. Apple explicitly directs its app developers to "[r]equest personal data only when your app clearly needs it," to "[e]xplain why your app needs the information if it's not obvious," to "[r]equest persmission at launch only when necessary for your app to function," and "[d]on't request location information unnecessarily."[26]

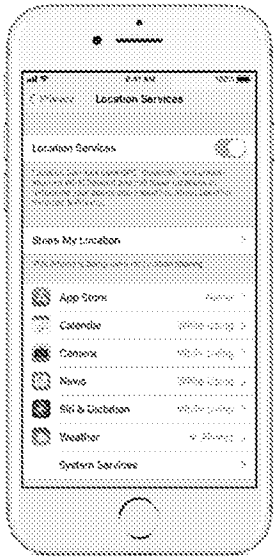
---

[20] *Id.*
[21] *Id.*
[22] An API is a software tool that facilitates the exchange of prespecified data between different programs and systems. *See* Jenn Chen, *What Is an API & Why Does It Matter?*, Sprout Blog (Jan. 31, 2018), https://sproutsocial.com/insights/what-is-an-api/.
[23] *See* Apple, *Getting the User's Location* (2016), https://developer.apple.com/library/content/documentation/UserExperience/Conceptual/LocationAwarenessPG/CoreLocation/CoreLocation.html.
[24] Apple, *Requesting Permission* (2018), https://developer.apple.com/ios/human-interface-guidelines/app-architecture/requesting-permission/.
[25] *Id.*
[26] *Id.*

34. One mechanism that iOS provides for requesting user permission to access location data is a notification displayed centrally and prominently on the device:[27]



35. The other mechanism that iOS provides to manage user permissions for access to location data is the "Location Services" dashboard in Settings > Privacy:[28]



[27] *Id.*

[28] Apple, *Turn Location Services and GPS on or off on your iPhone, iPad, or iPod touch* (2017), https://support.apple.com/en-us/HT207092; *see also* Apple, *About Privacy and Location Services in iOS 8 and Later* (2018), https://support.apple.com/en-us/HT203033.

36. The first time an app attempts to access location data, "its authorization status is indeterminate and the system prompts the user to grant or deny the request[.] The system records the user's response and does not display this panel upon subsequent requests."[29]

37. User permissions for per-app access to location data in iOS include three settings: (1) no access, (2) limited access ("only when you're using the app"), and (3) full access ("even when you aren't using the app").[30]

38. Apple recommends that developers "request only when-in-use authorization whenever possible."[31]

39. If a user grants permission for an app to gain full or limited access to their location data, the app can then use the Core Location API to access the consumer's location data.

40. Apple recommends that "[a]pps that use location services should not start those services until they're needed. With a few exceptions, avoid starting location services immediately at launch time or before such services might reasonably be used."[32] As Apple explains, "improper and unnecessary use of location can prevent the device from sleeping, keep location hardware powered up, drain the user's battery, and create a poor user experience."[33]

41. The Core Location API "provides services for determining a device's geographic location, altitude, orientation, or position relative to a nearby iBeacon. The framework uses all

---

[29] Apple, *Core Location* (2018), https://developer.apple.com/documentation/corelocation.
[30] Apple, *Choosing the Authorization Level for Location Services* (2018), https://developer.apple.com/documentation/corelocation/choosing_the_authorization_level_for_location_services; *see also* Apple, *About Location Services and Privacy* (2017), https://support.apple.com/en-us/HT207056.
[31] *Id.*
[32] Apple, *Location and Maps Programming Guide: Getting the User's Location* (2016), https://developer.apple.com/library/content/documentation/UserExperience/Conceptual/LocationAwarenessPG/CoreLocation/CoreLocation.html#//apple_ref/doc/uid/TP40009497-CH2-SW1.
[33] Apple, *Reduce Location Accuracy and Duration* (2016), https://developer.apple.com/library/content/documentation/Performance/Conceptual/EnergyGuide-iOS/LocationBestPractices.html#//apple_ref/doc/uid/TP40015243-CH24.

available onboard hardware, including WiFi, GPS, Bluetooth, magnetometer, barometer, and cellular hardware to gather data."[34]

42. The "Standard Location Service" in the Core Location API is "highly configurable, letting [the developer] specify the preferred accuracy for locations and the distance that the user must travel before new updates are delivered."[35] Apple recommends that developers "never set the desired Accuracy property to a higher accuracy than what you actually need" and "set the distance Filter property to the greatest value that meets the needs of your app."[36]

43. Apps can set the standard location service accuracy to a numerical distance in meters or select from one of six preset options: (1) "highest possible accuracy [combined] with additional sensor data"; (2) "highest level of accuracy"; (3) "within ten meters of the desired target"; (4) "within one hundred meters"; (5) "to the nearest kilometer"; (6) "to the nearest three kilometers."[37]

44. Although the standard location service uses precise GPS coordinates, "the system might disable GPS and use only the WiFi hardware" to provide location data if the desired accuracy is set to a kilometer range, "which would save power and still give [the app] greater accuracy than [r]equested."[38]

Consumers' Location Can Be Inferred Based on Unique Identifiers of WiFi Networks

45. Consumers connect to WiFi networks through devices called Access Points (APs).

---

[34] Apple, *Core Location* (2018), https://developer.apple.com/documentation/corelocation.
[35] Apple, *Using the Standard Location Service* (2018), https://developer.apple.com/documentation/corelocation/getting_the_user_s_location/using_the_standard_location_service.
[36] *Id.*
[37] Apple, *CLLocationAccuracy* (2018), https://developer.apple.com/documentation/corelocation/cllocationaccuracy.
[38] Apple, *Using the Standard Location Service*, *supra*.

46. Each Access Point has a unique identification number assigned to its network interface, which is commonly referred to as a Media Access Control (MAC)[39] address or Basic Service Set Identifier (BSSID).

47. Each BSSID is unique to a single access point and is typically expressed as six groups of hexadecimal digits (e.g. 01-23-45-67-89-ab).

48. In addition to functioning as an identifier within a WiFi network, a BSSID can be used to infer the location of a device based on the location of the Access Point.

49. For example, Apple's Core Location API uses BSSID data from nearby WiFi networks as part of its system for determining a device's precise location. In order to do this, Apple maintains a "database of WiFi hotspots and cell towers" that they use to "rapidly and accurately calculate [a device's] location when requested."[40]

50. But Apple is not the only company that can infer a device's location based on WiFi network data. There are numerous databases that provide this functionality. For example, Wigle "consolidate[s] location and information of wireless networks world-wide into a central database, and have user-friendly desktop and web applications that can map, query and update the database via the web."[41]

51. AccuWeather and other third-party companies can therefore identify the location of an iOS device, even without obtaining proper Location Services permissions from the consumer, if they can obtain WiFi network information from the device.

---

[39] The IEEE MAC address uses a 48-bit address space, which means that there are potentially 2^{48} or 281,474,976,710,656 possible MAC addresses.
[40] Press Release, Apple, *Apple Q&A on Location Data* (Apr. 27, 2011), https://www.apple.com/newsroom/2011/04/27Apple-Q-A-on-Location-Data/.
[41] *See, e.g.*, Frequently Asked Questions, *https://wigle.net/faq*.

52. Yet despite the fact that Apple has an entire permissions structure to control access to location data, apps can still track consumers' devices without their permission by collecting WiFi network data. Specifically, the iOS System Configuration Framework provides access to the BSSID of a user's current WiFi network through the "Captive Network" function.

53. The iOS platform does not require apps to obtain consumers' permission to access BSSID through the Captive Network function, and consumers do not have any way to deny an app access to this information.[42]

54. Apps on the iOS platform can thus be used to track a consumer's location using the BSSID of the WiFi router to which the device is connected without properly obtaining the consumer's permission to access location data.

AccuWeather's Deceptive and Unlawful Business Practices

AccuWeather's Deceptive Collection and Disclosure of WiFi Network Data Prior to August 2017

55. As of August 2017, AccuWeather configured its app to collect and disclose data that can be used to infer consumers' location, despite the fact that the consumers had explicitly denied AccuWeather permission to collect their location data.

56. Specifically, AccuWeather collected and disclosed to a third-party marketing company—Reveal Mobile, Inc., —the BSSID data identifying a consumer's current WiFi network even when the consumer had denied permission to access location data.

57. AccuWeather collected this BSSID data even when the app was not open.

58. AccuWeather disclosed the BSSID data to Reveal Mobile to facilitate its location-targeted advertising system.

---

[42] Nithan Sannappa & Lorrie Cranor, *A Deep Dive Into Mobile App Location Privacy Following the InMobi Settlement*, Tech@FTC (Aug. 9, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement.

59. AccuWeather's collection of BSSID data was enabled by the Reveal Mobile software development kit (SDK), which AccuWeather integrated into its app.

60. AccuWeather's practices were first discovered by security researcher Will Strafach.[43] Strafach ran a test of his iPhone and found that while the AccuWeather app was running in the background it transmitted the name and BSSID of his WiFi router to Reveal Mobile a total of 16 times every 36 hours, or about once every few hours.[44]

61. Consumers expressed widespread outrage at AccuWeather's location tracking without their consent, and many consumers pledged to delete the AccuWeather app as a result of the incident.

AccuWeather's Deceptive Collection and Disclosure of Personal Location Data Using iOS Location Services

62. In addition to the practices described above, AccuWeather is currently collecting and disclosing to third-party marketing companies personal location data even when consumers have granted permission only to use Location Services "While In the App" for weather forecasts and alerts.

63. When consumers first open the AccuWeather app, they are given a prompt that requests that they allow the app to access their location "even when you are not using the app." This is the "Always" allow setting in iOS Location Services.

64. If consumers agree to the prompt or otherwise configure their device to allow access "Always," then the AccuWeather app collects their precise location data, uses it to sell "contextual advertising" and discloses it to "third party marketing" companies.

---

[43] Will Strafach, *Advisory: AccuWeather iOS App Sends Location Information to Data Monetization Firm*, Hackernoon, (Aug. 21, 2017), https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870.
[44] *Id.*

65. Consumers who refuse to allow the AccuWeather app to "Always" access their location data can instead configure their device to only permit access "While Using the App" in order to determine the current weather conditions in their area.

66. However, if consumers configure their devices to allow location data access only "While Using the App," AccuWeather still collects their personal location data and discloses it to third parties.[45]

67. Thus, even when the "Always" permission is not granted, AccuWeather discloses to the ad exchange Nexage the following personal location data elements collected from the iOS Core Location API:

- Geographic coordinate information in the form of latitude and longitude;
- Altitude, measured in meters;
- A timestamp, which is converted into a date and time in GMT (e.g. 14 Mar 2018 15:00:00 GMT);
- Horizontal accuracy, or the radius of uncertainty for location, measured in meters;
- Vertical accuracy, or the radius of uncertainty of the altitude value, measured in meters;
- And bearing, in compass degrees, and speed, in meters.

68. An Apple iOS device uses a combination of GPS, Bluetooth, WiFi, and cellular data to generate the personal location data that AccuWeather accesses and discloses.

[45] *See* Zack Whittaker, *Despite Privacy Outrage, AccuWeather Still Shares Precise Location Data with Ad Firms*, ZDNet (Aug. 25, 2017), http://www.zdnet.com/article/accuweather-still-shares-precise-location-with-advertisers-tests-reveal/; *see also* Sam Bakken, *AccuWeather iOS App Privacy Issues: Lessons & Takeaways*, NowSecure (Sept. 1, 2017), https://www.nowsecure.com/blog/2017/09/01/accuweather-ios-app-privacy-issues-lessons-takeaways/.

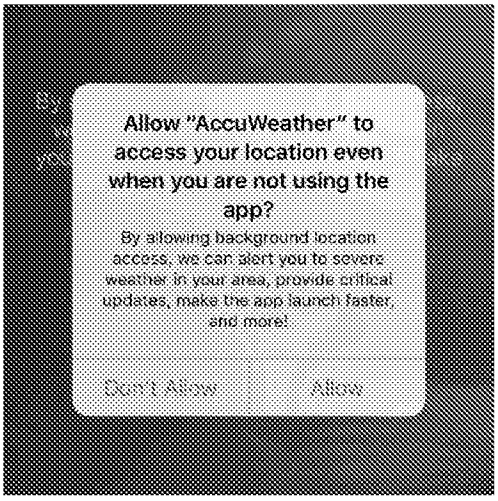
69. The accuracy of location data depends on a number of environmental factors, but currently available mobile devices are capable of generating location data accurate to within 5 meters.[46] New chips being released this year will enable accuracy down to 30 centimeters.

70. The personal location data that AccuWeather requests and discloses to Nexage is able to accurately locate a consumer down to a specific street and even building in most cases.

71. In addition to the personal location data disclosed to Nexage, AccuWeather also discloses to DoubleClick location data identifying the city, state, and neighborhood for which the consumer is currently requesting weather information. AccuWeather discloses this location data to DoubleClick even if the consumer has chosen to "Never" allow tracking via Location Services.

AccuWeather's Representations Regarding Location Data Collection and Disclosure Prior to August 2017

72. Prior to August 2017, when consumers downloaded the AccuWeather app from the iOS app store and opened it for the first time, they were prompted with the following iOS permissions request and notification:



[46] Samuel K. Moore, *Superaccurate GPS Chips Coming to Smartphones in 2018*, IEEE Spectrum (Sept. 21, 2017), https://spectrum.ieee.org/tech-talk/semiconductors/design/superaccurate-gps-chips-coming-to-smartphones-in-2018.

73. Based upon the above representation, a reasonable consumer would believe that clicking "Don't Allow" meant that AccuWeather would not track the consumer's location.

74. AccuWeather stated in its app permissions notification that, "[b]y allowing background location access, we can alert you to severe weather in your area, provide critical updates, make the app launch faster, and more!"

75. AccuWeather did not indicate that it would collect or disclose a consumer's WiFi network data even if the consumer chose "Don't Allow" locations services permissions.

76. A reasonable consumer who read AccuWeather's notification would not expect such an additional, undisclosed collection, use, or disclosure of BSSID data.

77. AccuWeather also did not indicate that it would track a consumer's BSSID data in the background to infer the consumer's location for targeted advertising purposes or disclose that data to marketing affiliates.

78. A reasonable consumer who read AccuWeather's notification would not expect such an additional, undisclosed use of BSSID data to infer the consumer's location. The listed uses of location data all pertained to the consumer's interactions with the app itself ("alert you to severe weather in your area, provide critical updates, make the app launch faster"). Although AccuWeather added "and more!" at the end of this list, no reasonable consumer would expect the "and more" to refer to sending location information to third-party marketing affiliates for targeted advertising purposes. This use bears no relation to the other in-app uses that AccuWeather disclosed and is far more invasive.

79. AccuWeather's permissions notification appeared when consumers first open the app, and consumers relied upon that representation when deciding whether to use or delete the app.

AccuWeather's Current Representations Regarding Location Data Collection and Disclosure

80. Following the discovery of AccuWeather's collection and disclosure of BSSID data in August 2017, the company made changes to its app and to its representations.

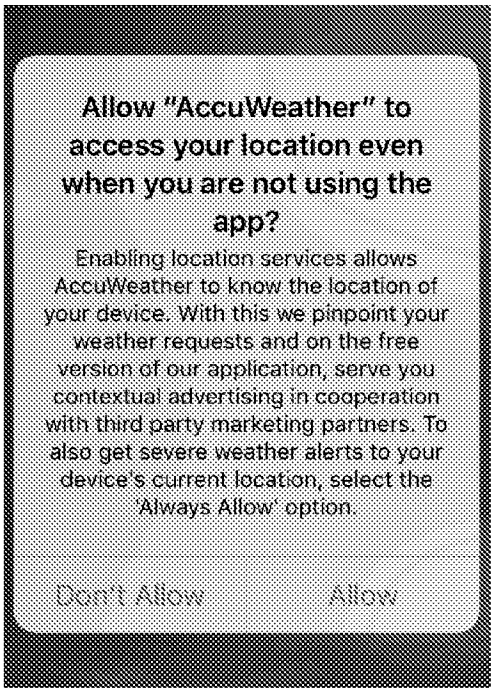
81. When consumers download the current version of the AccuWeather app and open it for the first time, they are presented with a "Terms of Use" page that links to a "Terms & Conditions" document and a "Privacy Statement."

82. If a consumer browses to the AccuWeather Privacy Statement, the first paragraph the consumer sees reads:

> AccuWeather wants to assure that Users of the AccuWeather Sites are provided with appropriate information and choice mechanisms about AccuWeather's relevant policies and practices so that these Users may make informed decisions on whether or not to use the AccuWeather Sites.

83. On an iPhone 6S device, a consumer attempting to read the entire AccuWeather Privacy Statement would be required to scroll through roughly twenty-three screens of text.

84. When a consumer opens the AccuWeather app for the first time, the consumer is prompted with the following iOS permissions notification:

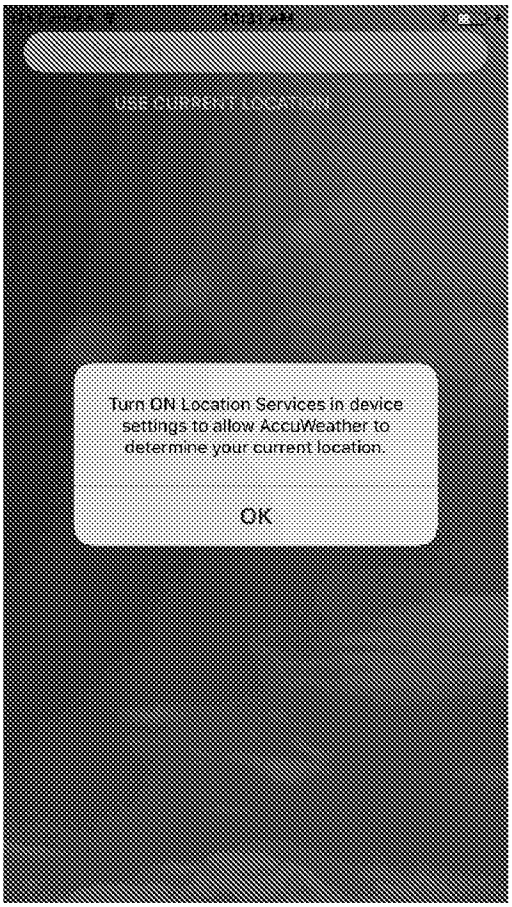


85. If the consumer selects "Allow," iOS Location Services permissions are set to allow location access "Always." If the consumer selects "Don't Allow," then iOS Location Services permissions are set to allow location access "Never."

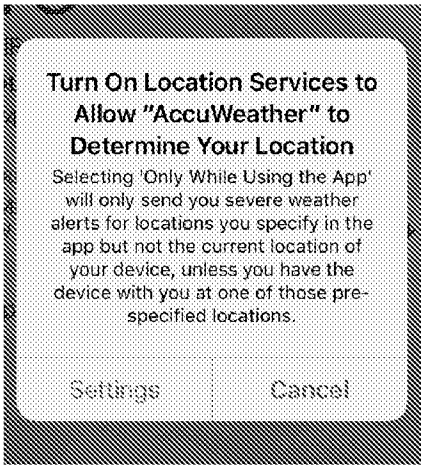
86. In the iOS Location Services control center, the same notification text that was in the permissions notification appears under "App explanation" when a user selects "Always":

> Enabling location services allows AccuWeather to know the location of your devices. With this we pinpoint your weather requests and on the free version of our application, serve you contextual advertising in cooperation with third party marketing partners. To also get severe weather alerts to your device's current location, select the 'Always Allow' option."

87. If a consumer chooses not to allow "Always" location tracking, then the AccuWeather app gives the consumer the following in-app alert:



88. If a consumer continues to use the AccuWeather app with location permissions set to "Never," the app will eventually request Location Services permissions be set to "While Using the App" in an in-app permissions notification:



89. When a consumer goes to Location Services in device settings, as instructed by the AccuWeather app, the consumer is given three options: allow location access Never, While Using the App, or Always.

90. If a consumer chooses to allow location access "While Using the App," the "app explanation" contains the same text that appeared in the permissions notification:

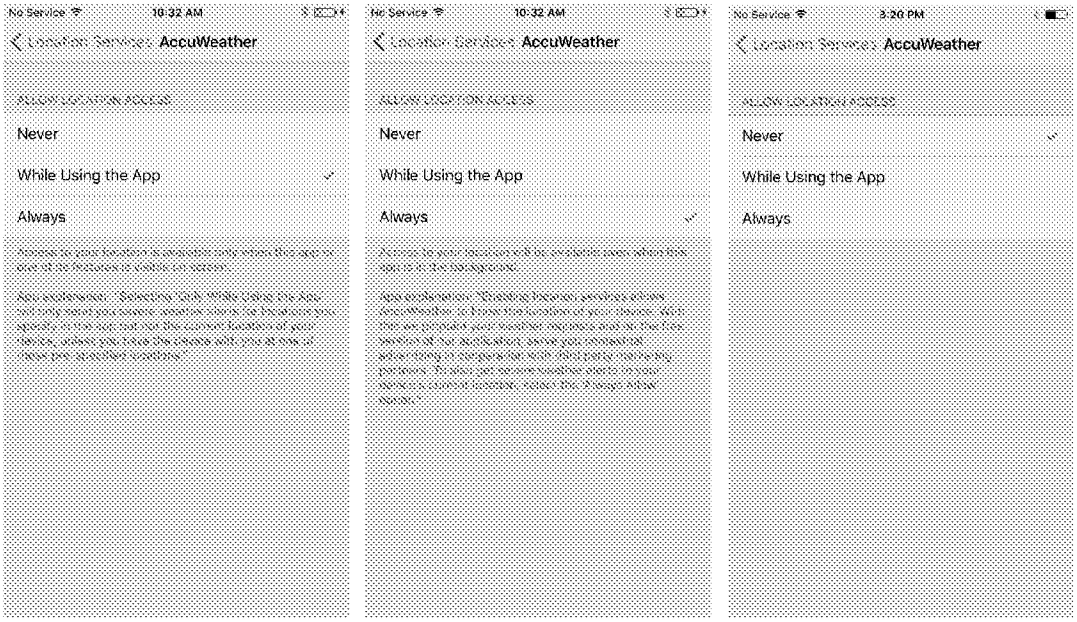
> Selecting 'Only While Using the App' will only send you severe weather alerts for locations you specify in the app but not the current location of your device, unless you have the device with you at one of those pre-specified locations.

91. AccuWeather does not represent that it will collect, use, or disclose consumers' location data for advertising purposes or to third-party marketing partners in the app explanation for the "While Using the App" permissions setting.

92. In contrast, AccuWeather explicitly represents that it will collect, use, and disclose consumers' location data for "contextual advertising in cooperation with third party marketing partners" in the app explanation (and permissions notification) for the "Always" permissions setting.

93. A reasonable consumer recognizes this contrast and believes that AccuWeather will only collect, use or disclose location data for advertising purposes when the consumer enables the "Always" permissions setting.

94. If a consumer chooses to set Location Services permissions to "Never," the consumer is not shown any app explanation.



95. AccuWeather does not represent to consumers that it uses, or discloses their location data for advertising purposes when Location Services permissions are set to either "Never" or "While Using the App."

How AccuWeather and Its Marketing Partners Use Personal Location Data

96. Advertising produces enormous revenues for mobile apps like AccuWeather. Recent reports estimate that businesses will spend $147 billion on mobile advertising in 2018.[47]

97. There are two kinds of advertisements that target mobile devices: website ads and in-app ads.[48]

98. Mobile ads can be targeted using a variety of different methods and data points including, in particular, latitude and longitude (location data).[49]

---

[47] Lucy Handley, *Half of All Advertising Dollars Will Be Spent Online by 2020, Equaling All Combined 'Offline' Ad Spend Globally*, CNBC (Dec. 4, 2017), https://www.cnbc.com/2017/12/04/global-advertising-spend-2020-online-and-offline-ad-spend-to-be-equal.html.
[48] AppNexus, *Industry Reference: Introduction to Mobile Advertising* (2017), https://wiki.appnexus.com/display/industry/Introduction+to+Mobile+Advertising.
[49] *Id.*

99. A mobile ad transaction involves several entities: "publishers" who sell the ad space on a website or app, "advertisers" who buy that ad space, "ad networks" who act as brokers between buyers and sellers, "users" who are the targets for the advertisements, and other data providers and platforms who sell information about websites and users to facilitate ad targeting.[50]

100. Most publishers, advertisers, and ad networks interact through systems called "ad exchanges" that set prices, deliver ads, and transfer user and other data.[51]

101. One of the key factors that ad exchanges use to determine which ads to serve and what price to charge is user data, including "geography."[52]

102. AccuWeather sells in-app advertising through an ad exchange that uses location data to target consumers.

103. The Apple iOS system creates a unique identifier for each mobile device called the Apple Identifier for Advertising (IDFA).

104. AccuWeather sells advertising on both "DoubleClick for Publishers" and "Nexage" ad exchanges.

105. DoubleClick for Publishers is owned and operated by Google.[53]

106. Nexage was acquired by AOL when it purchased bought Millennial Media.[54] AOL was acquired by Verizon Communications in 2017, and Verizon subsequently rebranded

---

[50] AppNexus, *Industry Reference: Introduction to Ad Serving* (2017), https://wiki.appnexus.com/display/industry/Introduction+to+Ad+Serving.
[51] *Id.*
[52] *Id.*
[53] https://www.doubleclickbygoogle.com/.
[54] Yuyu Chen, *Will It Blend? Oath Will Combine Disparate AOL-Yahoo Ad Tech Assets*, Digiday (Apr. 13, 2017), https://digiday.com/media/will-blend-oath-will-combine-disparate-aol-yahoo-ad-tech-assets/.

AOL and Yahoo as "Oath Inc."[55] Oath thus controls the merged advertising technology companies and assets that both AOL and Yahoo! had acquired:[56]

107. AccuWeather also uses mobile app analytics platforms to collect additional data about consumers in order to increase advertising revenue.

108. Prior to September of 2017, AccuWeather configured its iOS app to send consumer data to Reveal Mobile in exchange for mobile location analytics data.

109. Reveal Mobile is a "mobile audience analytics platform" that markets itself as being able to increase the "advertising performance" of app publishers like AccuWeather by "175-477%" and to increase their "advertising revenue" by "50-200%."[57]

110. Reveal Mobile provides three categories of services: "App Direct" location data used to target mobile advertising audiences through ad exchanges, a "Social Direct" data interface that enables marketers to catalog consumers' mobile location data into social media

[55] Niraj Chokshi & Vindu Goel, *Verizon Announces New Name Brand for AOL and Yahoo: Oath*, N.Y. Times (Apr. 3, 2017), https://www.nytimes.com/2017/04/03/technology/verizon-oath-yahoo-aol.html.
[56] Chen, *supra*.
[57] Reveal Mobile, *Reveal Mobile & Digital2Go Media Networks Partner for Beacon Powered Mobile Audience Data* (Nov. 9, 2015), https://revealmobile.com/20151119reveal-mobile-digital2go-media-networks-partner-for-beacon-powered-mobile-audience-data/.

audience lists, and "Data Monetization" services which enable app developers to sell their consumers' location data to third-party "mobile data partners."[58]

111. Reveal Mobile's SDK enables app developers to integrate Reveal's location data tracking mechanisms into their apps. When Reveal Mobile's SDK is integrated into an app, the SDK accesses location data that is collected by the app and sends that data to Reveal Mobile's servers.

112. Reveal Mobile has stated that location data can be used to track which retail stores a consumer visits and to build profiles on consumers based on where they work and live. "Location data also informs the home and work location of customers," Reveal CEO Brian Handly wrote last year. "Pairing this information with existing demographic targeting criteria allows retailers to target consumers with a high propensity to visit based upon two of their most relevant locations."[59]

113. The Mobile Marketing Association, a trade association for mobile advertising companies, has also recognized that there are significant privacy implications triggered by the collection and use of consumers' location data. The Association adopted a "Global Code of Conduct" in 2008 concerning the collection of consumers' location data by mobile marketing companies.[60]

114. Reveal Mobile is a member of the Mobile Marketing Association.[61]

115. Google is a member of the Mobile Marketing Association.[62]

---

[58] Reveal Mobile; Reveal Mobile, *Social Direct*, https://revealmobile.com/our-solutions/social-direct/; Reveal Mobile, *Data Monetization*, https://revealmobile.com/our-solutions/data-monetization/.
[59] Brian Handly, *How to Profit From Data on the Location of Mobile Shoppers*, Reveal Mobile, (May 1, 2017), https://revealmobile.com/profit-data-location-mobile-shoppers/.
[60] Mobile Marketing Ass'n, *Global Code of Conduct* 2 (2008), http://www.mmaglobal.com/files/codeofconduct.pdf.
[61] https://revealmobile.com/.
[62] http://www.mmaglobal.com/members/google.

116. AOL LLC (now Oath Inc.) was a member of the Mobile Marketing Association prior to its acquisition by Verizon Communications in 2015.

117. The Mobile Marketing Association's Global Code of Conduct states that members will "respect the right of the user to control which mobile messages they receive" and will "ask for and obtain consent by obtaining an explicit opt-in from the user for all mobile messaging programs."[63] The Code of Conduct also provides that members "must inform the user of both the marketer's identity or products and services offered, and the key terms and conditions that govern an interaction between the marketer and the user's mobile device."[64]

118. In 2016 the Federal Trade Commission ("FTC") brought a complaint against and reached a settlement with a InMobi, a mobile ad exchange.[65] The FTC alleged that InMobi deceptively collected and used consumers' location data to sell geo-targeted advertisements.[66] In particular, the FTC alleged that InMobi "represented, expressly or by implication, that it tracked the consumer's location and served geo-targeted ads only if the application developer and consumer had provided access to the Android and iOS location APIs."[67] But in fact, the FTC alleged, InMobi "tracked the consumer's location and served geo-targeted ads by collecting BSSID and other information related to the WiFi network to which a consumer's device was connected or in-range, even if the consumer had not provided access to the location APIs."[68]

---

[63] *Global Code of Conduct*, *supra*, 1.
[64] *Id.*
[65] Complaint for Permanent Injunction, Civil Penalties, and Other Relief, *United States v. InMobi Pte Ltd.*, No. 3:16-cv-3474 (N.D. Cal. filed June 22, 2016).
[66] *Id.* ¶¶ 28–38.
[67] *Id.* ¶ 51.
[68] FTC, *A Deep Dive into Mobile App Location Privacy Following the InMobi Settlement*, Press Release, (Aug. 9, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement.

119. AccuWeather has and continues to engage in similarly deceptive collection, use, and dissemination of consumers' location data.

Materiality of Third-Party Use and Disclosure of Location Data

120. Transmitting personal location data to a third party for targeted advertising purposes is a material practice that invades the privacy interests of consumers. As explained above, Apple requires all apps on the iOS operating system to disclose why they are requesting access to location information precisely because this data is sensitive personal information that many consumers wish to keep private.

CAUSES OF ACTION

121. Pursuant to D.C. Code § 28-3905(k)(1)(C), "[a] nonprofit organization may, on behalf of itself or any of its members, or on any such behalf and on behalf of the general public, bring an action seeking relief from the use of a trade practice in violation of a law of the District, including a violation involving consumer goods or services that the organization purchase or received in order to test or evaluate qualities pertaining to use for personal, household, or family purposes."

122. Pursuant to D.C. Code § 28-3905(k)(1)(D)(i), "a public interest organization may, on behalf of the interests of a consumer or a class of consumers, bring an action seeking relief from the use by any person of a trade practice in violation of a law of the District if the consumer or class could bring an action under subparagraph (A) of this paragraph for relief from such use by such person of such trade practice."

123. Pursuant to §§ 28-3905(k)(1)(C) and (k)(1)(D)(i), the DC CPPA allows for non-profit organizational standing and public-interest organizational standing to the fullest extent

recognized by the D.C. Court of Appeals in its past and future decisions addressing the limits of constitutional standing under Article III.

Count I:
Violation of the District of Columbia Consumer Protection Procedures Act For Making A Materially Misleading Statement

124. Each of the preceding paragraphs is incorporated by reference herein.

125. Through means described above, AccuWeather represented, expressly or by implication, that it did not collect, use, or disclose consumers' location data for marketing purposes unless they granted "Always" access permissions under the iOS Location Services controls.

126. In truth and in fact, as set forth in Paragraphs 55-79, AccuWeather did collect and use consumers' personal location data (including their latitude and longitude along with date, time, and a unique user identifier) for marketing purposes and disclosed that data to third-party marketing affiliates.

127. AccuWeather misled consumers by stating in its notification, "Allow 'AccuWeather' to access your location even when you are not using the app?" and by providing consumers with the option to click "Don't Allow."

128. AccuWeather's notification was materially false because AccuWeather continued to track consumers' location even if they clicked "Don't Allow."

129. AccuWeather's statement about location tracking was material to consumers in deciding whether to use the AccuWeather app.

130. Therefore, AccuWeather violated the DC CPPA, DC Code § 28-3904(e) which makes it unlawful to "misrepresent as to a material fact which has a tendency to mislead."

131. D.C. Code § 28-3901(c) establishes an enforceable right to truthful information

from merchants about consumer goods and services that are or would be purchased, leased, or received in the District of Columbia.

132. As a result of Defendant's unfair and deceptive trade practices detailed herein, Plaintiff and consumers in the District of Columbia are deprived of truthful information regarding the app.

133. As a result of this unfair and deceptive trade practice, EPIC seeks statutory damages, punitive damages, declaratory relief, injunctive relief, and reasonable attorney's fees.

134. As a result of this unfair and deceptive trade practice, EPIC seeks on behalf of the general public:

a. An injunction against Defendant, including that Defendant cease collecting from any mobile device any data that can be used to identify a consumer's location without providing clear and prominent notice to the consumer and obtaining the consumer's express, affirmative opt-in consent; and

b. A declaration that Defendant's collection, use, and disclosure of personal location data for advertising purposes was unlawful.

c. Reasonable attorney's fees.

Count II:
Violation of the District of Columbia Consumer Protection Procedures Act For Misleading By Failing To State A Material Fact

135. Each of the preceding paragraphs is incorporated herein.

136. AccuWeather misled consumers by failing to state the material fact that it was collecting, using, and disclosing consumers' location data for marketing purposes even when the users did not provide "Always" access permissions under the iOS Location Services controls.

137. In truth and in fact, as set forth in Paragraphs 55-79, Accuweather did collect and use consumers' location data (including their precise latitude, longitude, and altitude data) for marketing purposes and disclosed that location data to third party marketing affiliates.

138. The fact that AccuWeather sent consumers' location data to a third party was material to consumers in deciding whether to use the AccuWeather app.

139. Therefore, AccuWeather has violated the DC CPPA, DC Code § 28-3904(f), which makes it unlawful to "fail to state a material fact if such failure tends to mislead."

140. D.C. Code § 28-3901(c) establishes an enforceable right to truthful information from merchants about consumer goods and services that are or would be purchased, leased, or received in the District of Columbia.

141. As a result of Defendant's unfair and deceptive trade practices detailed herein, Plaintiff and consumers in the District of Columbia are deprived of truthful information regarding the app.

142. As a result of this unfair and deceptive trade practice, EPIC seeks statutory damages, punitive damages, declaratory relief, injunctive relief, and reasonable attorney's fees.

143. As a result of this unfair and deceptive trade practice, EPIC seeks on behalf of the general public:

a. An injunction against Defendant, including that Defendant cease disclosing to third parties and/or allowing third parties to collect from any mobile device any data that can be used to identify a consumer's location without providing clear and prominent notice to the consumer and obtaining the consumer's express, affirmative opt-in consent; and

b. A declaration that Defendant's collection, use, and disclosure of personal location data for advertising purposes was unlawful

c. Reasonable attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff EPIC prays for judgment against AccuWeather and the following relief:

A. A declaration that AccuWeather's conduct is in violation of the DC CPPA;

B. An order enjoining AccuWeather's conduct found to be in violation of the DC CPPA;

C. An order of disgorgement and restitution of all earnings, profits, compensation, and benefits received by AccuWeather as a result of its conduct found to be in violation of the DC CPPA.

D. An order granting Plaintiffs costs and disbursements, including reasonable attorneys' fees and expert fees, and prejudgment interest at the maximum rate allowable by law;

E. Statutory Damages for EPIC individually;

F. Punitive Damages;

G. Such further relief, including equitable relief, as this Court may deem just and proper.

Date: March 16, 2018

Respectfully submitted,

ELECTRONIC PRIVACY INFORMATION CENTER

Marc Rotenberg, Esq., Bar No. 422825

/s/ Alan Jay Butler
Alan Jay Butler, Esq., Bar No. 1012128
Sam Lester, Esq., Bar No. 888241885
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
butler@epic.org
rotenberg@epic.org
lester@epic.org
202-483-1148

NIDEL & NACE, PLLC

/s/ Jonathan B. Nace
Jonathan B. Nace, Esq., Bar No. 985718
Christopher T. Nidel, Esq., Bar No. 497059
5335 Wisconsin Ave., NW
Suite 440
Washington, DC 20015
chris@nidellaw.com
jon@nidellaw.com
202-478-9677

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

/s/ Jonathan B. Nace
Jonathan B. Nace, Esq., Bar No. 985718