

December 12, 2019

Senator Coons
218 Russell Senate Office Building
Washington, DC 20510

Senator Hawley
212 Russell Senate Office Building
Washington, D.C. 20510

Dear Senator Coons and Senator Hawley:

Thank you for your November 19, 2019 letter requesting information about Facebook's practices concerning location information. We appreciate the opportunity to discuss these issues with you.

At Facebook, our mission is to give people the power to build community and bring the world closer together. Location-related information gives us the ability to facilitate these connections.¹ For example, people can choose to share location on Facebook to post when they're at a particular location or tag photos with a location, to search for things nearby, or to share where they are with friends, or inform people of emergencies using our Safety Check feature. Location-related information helps us show things relevant to where you are and to improve ads.

Location-related information also helps us keep people and our platform safe, like recognizing if people's accounts have been compromised. For example, if a person typically logs in to her account from a browser in London but someone tries to log in to that account from a browser in Sydney, our systems recognize this unusual behavior and send her an alert to confirm that the log in attempt actually came from her. Our ability to use location-related information to detect suspicious activity is also central to our effort to ensure integrity on the Facebook platform, including stopping the spread of false news.

In this response, we provide background on the types of location-related information we receive and how we process it, followed by answers to the specific questions raised in your letter.

A. How Facebook Receives Location

Facebook collects location-related information from people in three different ways:

1. When people enable Location Services

If a person chooses to enable Facebook to use Location Services on their device, their device will share location-related information with us. Depending on the device, these signals may include things like GPS, WiFi networks, and Bluetooth beacon signals. GPS information directly identifies a device's location, whereas Bluetooth and Wi-Fi information is not itself location data but can be used to understand location. We refer to

this information received through the operating system on people's devices as "precise location information."

Location Services is an "opt-in" feature—people must affirmatively enable Location Services, a setting offered by the operating system on their device, and in doing so, signal that they want to share this information with Facebook. The Location Services setting is not controlled by Facebook and is not a Facebook setting or product. Rather, it's a standard setting people will find on their devices that allow them to decide whether to share precise location information with Facebook.

Precise location information powers numerous experiences and products for people who have the Location Services setting on. If a person has enabled Location Services, Facebook can customize products and services to that person's specific location, such as more accurate weather forecasts, special offers for nearby stores, or our Nearby Friends product, which lets people know when their friends (if the friends also have enabled this feature) are close by.

2. Through people's activity on our services

Even if someone does not enable Location Services, Facebook may still understand information about their location based on information that they and others provide through their activities and connections on our services. For example, if someone responds to an event on Facebook for a local music festival, uploads a location-tagged post, or gets tagged by a friend in a check-in at a restaurant, these actions would give us information about that person's likely location. Similarly, a person might share where they live by setting a location in Marketplace or adding their address to their profile. While this kind of location sharing can help people connect on Facebook services, we also know that it can be inaccurate. For example, if a person reminiscing about their college experience ahead of their college reunion chooses to tag a photo with "University of Delaware" from their home in Colorado.

3. From IP addresses

Finally, in addition to location-related information that people share through their activities on Facebook and precise device location information sent from the devices of people who have enabled Location Services, we also receive IP addresses and other network information when people's devices connect to Facebook servers.

Every device that is connected to the internet is assigned an IP address that identifies its particular connection to the internet and that serves as a routing address for any data sent to and from the device. That address—like a return address on an envelope—identifies where the device is on the internet. The device necessarily transmits the address, and anyone the device communicates with receives it, whenever she sends or receives any messages or information.

The transmission of IP addresses is an inherent feature of how the internet works, and internet services use the IP address to deliver services to people -- for example, delivering a web page that they request to view. Anyone can see this type of location-

related information associated with an IP address through standard networking tools available on most computers.

While most IP addresses reflect the location of a device, the level of granularity of this information varies widely. For instance, an IP address assigned to a mobile device by a wireless carrier might reflect only the city or area where the device connected to the network, while a computer located on a company's corporate network may have an IP address associated with that business's offices. For this reason, IP addresses are generally considered to be imprecise ways of understanding location and can be inaccurate. For example, a particular IP address may cover a fairly large geographic area, and a mobile device on a cellular data network may connect to Facebook via an IP address associated with another city or state from the one where the device is physically located.

Throughout the remainder of this document, we will refer to the location data described under Scenarios 2 and 3 above as "rough" location data to distinguish it from the precise location data collected under Scenario 1 above.

* * *

To ensure that we are handling people's location-related information consistently, responsibly, and in conformance with people's choices, we have established a centralized engineering team dedicated to managing the infrastructure that we use to process this type of data. This team maintains internal application programming interfaces (APIs) that enable individual Facebook features -- from ads to News Feed to Safety Check -- to understand a person's location.

An important function of these internal APIs is to process people's location-related information at a level of granularity that is consistent with the choices they've made. For example, if someone has not enabled Location Services on their device, our APIs will typically provide only rough (i.e., city- or zip code-level) location information derived from IP address or other network information for that person, even where a more granular location could theoretically be determined from an IP address. (We discuss below some exceptions to this rule, such as when the IP address is needed to protect safety -- for example, in the case of imminent risk of suicide -- or to counter attackers attempting to compromise the security of our services.)

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we provide this information to people in a variety of ways. For example, we include explanations about how we handle people's location-related information in our Terms of Service¹ and Data Policy²; in Privacy Basics,³ which provides walkthroughs of the most common privacy questions we receive; on the Facebook service itself, such as in "Learn More" education available from Location settings; and in blog posts and news releases like the one that you cite in your letter.

¹ <https://www.facebook.com/terms.php>

² <https://www.facebook.com/policy.php>

³ <https://www.facebook.com/about/basics>

As an example, the Location walkthrough within our Privacy Basics feature⁴ explains:

Connection information like your IP address or Wi-Fi connection and specific location information like your device's GPS signal help us understand where you are.

This information can be used to help you find events nearby and show you local ads and news stories. Or power Safety Check on Facebook, which lets friends check in as 'safe' during crisis events around the world. Location can also help keep your account secure. We use where you normally log-in combined with other information to detect suspicious activity.

You can control whether your device shares precise location information with Facebook Products via Location Services, a setting on your mobile device, and if you've given us permission, when you are not using Facebook Products. We may still understand your location using things like check-ins, events, and information about your internet connection.

B. Responses to Specific Questions

With this context in mind, we are glad to address in more detail the specific questions posed in your letter.

1. *Does Facebook collect any information about a user's location if the user has turned off or limited Location Services for Facebook? If so, please explain why Facebook collects such information and the process used to collect that data.*

When Location Services is off, Facebook may still understand people's locations using information people share through their activities on Facebook or through IP addresses and other network connections they use.

For example, as a part of using Facebook, people may provide Facebook with specific information about their location. As discussed above, they may check-in at a restaurant or a store, or apply a location tag to a photo, or their friend might tag them in a check-in post. In these circumstances, people choose to provide Facebook with location-related information. We understand in these cases that sometimes people share location-related information that does not accurately reflect their current location, as is the case for the Colorado user mentioned above who tags a photo with "University of Delaware."

In addition, even when Location Services is off, Facebook necessarily receives IP addresses whenever a person's device connects to our servers, and these IP addresses can reflect some sense of a person's location. This can happen when people access Facebook directly or if they visit apps and websites that use Facebook's business tools, like Facebook's pixel. As explained above, if someone has not enabled Location Services on their device, our APIs will typically provide only rough (i.e., city- or zip code-level) location information derived from IP address or other network information for that

⁴ <https://www.facebook.com/about/basics/manage-your-privacy/location>

person, even where a more granular location could theoretically be determined from an IP address, except in situations involving safety and security.

When we receive this type of location-related information, we use it to customize people's experience, including by identifying the appropriate language based on their location, showing ads and other content relevant to the area where they are located, and to comply with legal rules, including those that prohibit us from showing certain types of advertisements in particular jurisdictions.

Importantly, location is also an important element of Facebook's safety, security, and integrity efforts. Facebook uses information about locations to verify accounts and account activity. If someone who normally logs in from London suddenly logs in from Sydney, that may be a sign that the person's account has been compromised. Rough location data is also a fundamental component of our ability to identify fake accounts and detect and stop accounts, Groups and Pages engaged in coordinated inauthentic behavior.

2. Does Facebook collect any information about a user's location based only on information about a user's internet connection?

As explained above, we receive IP addresses that reflect the internet connection a device uses to connect to our servers and this information is used to determine a device's rough location. In some cases, we receive other types of information about a device's internet connection, such as the Wi-Fi network. For devices on current versions of the Android and iOS operating systems, we do not collect information about individual Wi-Fi networks if Location Services is turned off.

3. How frequently does Facebook collect location data based on information about a user's internet connection when a user has turned off or limited Location Services?

If a person has selected the "While Using" setting in Location Services on their device, Facebook will receive Location Services information (i.e., precise device location information received through the device operating system) only while the person is using the Facebook app. How often the Facebook app receives updates about a device's location is dynamic and determined by a number of factors, such as how long the person has the app open in the foreground and whether they take actions such as a check-in or a local search. As discussed above, if a person has turned Location Services off, the person's device does not send precise location information to Facebook. In these cases, Facebook still receives location-related information if it is provided as a part of someone's activity on our services, and we receive the device's IP address when the device interacts with our services, including Facebook technologies on third-party websites and apps. (In the answer to Question 4, we describe how we reduce the granularity of this data when people have turned off Location Services.)

4. *What is the difference between the "precise" location information collected when a user has Location Services enabled and the location information collected by Facebook using other data, such as the user's internet connection, when a user has turned off or limited Location Services? How detailed is the location data that Facebook collects when a user has turned off or limited Location Services?*

When Location Services is enabled, the precision of the location-related information that Facebook receives is determined by the device's operating system and the data available to the operating system. When Location Services is enabled, authorized applications may access the device's coordinates from the operating system. These coordinates are based on a number of signals determined by the device, including GPS and network connection signals, and the accuracy of this information can vary. For instance, if it is a cloudy day or a person is in a building that blocks a GPS signal, the operating system will have and will transmit less precise GPS information. If a person has Location Services enabled, we also may use additional signals, such as Wi-Fi network, as a part of determining precise location.

When a person has turned off Location Services, Facebook does not collect precise location information. As described above, we still may receive information about the person's location in these situations from their activity on our services or based on their IP address when their device connects to our servers.

With respect to IP addresses, as explained above, if someone has not enabled Location Services on their device, our APIs will typically provide only general (i.e., city- or zip code-level) location information derived from IP address or other network information for that person, even where a more granular location could theoretically be determined from an IP address. However, we may try to determine a more specific location associated with an IP address where needed to protect safety and security. Most commonly, this happens in cases where we believe there is imminent risk of physical harm, such as a suicide attempt, or where we are investigating attempts to compromise the security or integrity of our systems.

5. *Does Facebook target advertisements or otherwise monetize the location information it collects when a user has turned off or limited Location Services?*

Yes. By necessity, virtually all ads on Facebook are targeted based on location, though most commonly ads are targeted to people within a particular city or some larger region. Otherwise, people in Washington, D.C. would receive ads for services or events in London, and vice versa. We use location-related information, including rough locations understood from IP address, subject to the limitations described above, to decide what ads to show people. In cases where people have limited Location Services by choosing the "while using" option, we only use precise location received while they are using our app. If people have disabled Location Services, they may still see ads based on their location, but this will be at a reduced granularity as discussed above. (For example, in this situation a person might see an ad because Facebook understands that she lives in Washington, D.C. but would not see an ad based on her precise location.)

We describe this practice in several of the disclosures discussed above. For example, in the “Learn More” information accessible from our Location settings, we explain that Facebook “may still understand your location using things like check-ins, events, and information about your internet connection” when Location Services is off or limited and that “[w]e use this information to provide more relevant and personalized experiences, protect your account, and provide better ads.” Likewise, our Privacy Basics feature explains, “We may still understand your location using things like check-ins, events, and information about your internet connection.”

We provide more information about how we use location as a part of aggregated reporting in our answer to Question 7, below.

6. *If Facebook does target advertisements based on the location information that it collects when a user has turned off or limited Location Services, is it possible for a user to configure his or her privacy settings such that Facebook never monetizes any location information about that user?*

As explained above, by necessity, virtually all ads on Facebook are shown based on the general location – for example, city – where we estimate a person may be located. While we provide controls over whether Facebook collects precise location information, we don’t offer the option to turn off ads based on location.

7. *Does Facebook share the location information that it collects when a user has turned off or limited Location Services with third parties?*

Facebook does not sell people’s information to anyone. Moreover, we only share individually identifiable location-related information with third parties in limited situations, such as in response to a law enforcement or legal request, or if a person specifically chooses to share their information. A person may share their location with their chosen audience, for example, if they choose to check in at a location or add a location to their profile, or with advertisers where a user chooses to submit their address through our Lead Ads feature. Facebook may also make people’s information available to vendors and service providers who support Facebook’s business, including by providing technical infrastructure services, analyzing how Facebook’s products are used, providing customer service, facilitating payments, or conducting surveys. These vendors and service providers are allowed to use the information only for the limited purposes for which it is shared. We describe Facebook’s sharing of information with third-party partners in Facebook’s Data Policy.

Facebook uses aggregated location-related information that is not individually identifiable as a part of certain services that we provide. For example, we may provide reports to advertisers that show the areas where their ads were most commonly viewed, but we do not show where any specific person who saw the ad is located. We also

produce aggregated maps showing the coverage of various mobile networks and offer aggregated location maps to governmental and non-governmental organizations and universities working to serve the public good – for example, to track aggregate movement following a disaster.

Thank you again for the opportunity to answer your questions. We hope this response is helpful, and we would be happy to discuss further at your convenience.

Respectfully submitted,



Rob Sherman

Vice President & Deputy Chief Privacy Officer, Policy

ⁱ As discussed in detail throughout this letter, some information that people provide gives Facebook direct information about their location, while other information does not provide information about a device's location itself, but may be combined with other data to understand certain more general information about a device's location, such as a broader geographic area. For ease of reference in this letter, we refer to all of the information that relates, broadly-speaking, to location as "location-related information," even if this information may not itself reveal a location.