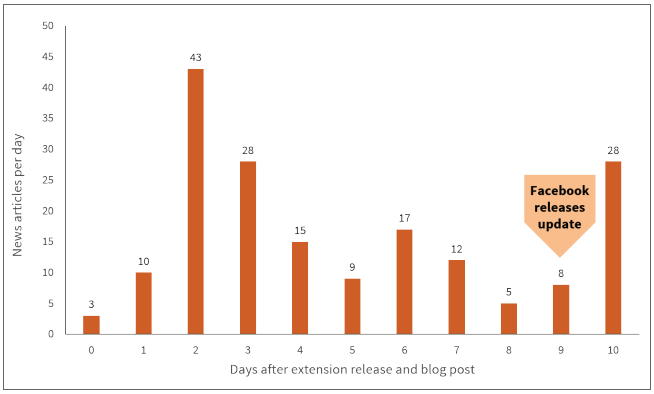
Khanna A. Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger. Technology Science. 2015081101. August 11, 2015. http://techscience.org/a/2015081101

Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger

Aran Khanna

Highlights

- In 2012, a media outlet reported that Facebook Messenger shared personal geolocations by default
- In 2015, my demonstration displayed Facebook's shared data on a map; it was downloaded over 85,000 times
- After 9 days of news coverage, Facebook released an update that requires a user's permission to share geolocations



News coverage by day

Abstract

Facebook allows users to chat among themselves on a mobile app called Facebook Messenger. From 2011 to the start of this study in May 2015, Facebook Messenger collected and shared user geo-locations as the default setting for every message sent from the Android mobile app. These locations were visible to anyone in a group chat, regardless of his or her relationship to the sender on the Facebook social network. Noticing a lack of significant public response to the visible nature of geo-location data on Facebook Messenger, despite

media coverage dating back to 2012, I hypothesized that users were either (1) not aware, or (2) not concerned about the collection and visibility of their geo-location data on the app. This study explored this hypothesis by testing how the public responded to easily seeing the historical geo-location data collected and shared by Facebook Messenger. This study also tested the response from Facebook, a company with a reputation for encouraging outside-the-box "hacking". I wrote a browser application that requires a Facebook user to log into their Facebook account and then displays on a map the geo-location data shared with that user through Facebook Messenger chats. I announced the tool in a blog post and publicized it on Twitter and a few other online forums. The immediate public response was that of surprise and concern over the privacy issue raised by the collection and visibility of the geo-location data.

Results summary: My tool has been downloaded over 85,000 times since its release, and more than 170 global news publications linked to my post. During the first three days after release of the geo-location mapping tool, Facebook also responded by demanding that I take down the tool, which I did. Nine days after the release, Facebook made sharing geo-location data an opt-in feature, allowing users to select to share personal geolocations in Facebook Messenger, although all historical geo-location data is still archived and shared. The results of the study suggest sufficient public attention may be necessary for redress of reported privacy concerns.

Introduction

Hundreds of millions of people share personal information on Facebook. Starting in 2011, Facebook implemented initiatives focused on "frictionless sharing" to automatically post a user's activity on music apps, such as Spotify, or news readers, such as *The Washington Post*, that use Facebook's Open Graph to integrate their websites more closely with Facebook. [1] This automatic posting of songs listened to and articles read was not very popular with users, and Facebook announced in May 2014 that it would decrease the visibility of passively shared user activities on their friends' news feeds. [2, 3, 4]

Regulators have also expressed privacy concerns with regard to how Facebook handles sharing of user data. For example, in Europe, the Belgian Privacy Commission found that Facebook "fails to offer adequate control mechanisms" for the use of user data. Furthermore, "Facebook places too much burden on its users, [who are] expected to navigate Facebook's complex web of settings in search of possible opt-outs." Finally the commission stated that, "Facebook's default settings related to behavioral profiling … are particularly problematic." [5, 6]

Background

In 2011 Facebook launched Facebook Messenger, an application (or "app") for Android and iOS mobile devices. Messenger has the ability to share geo-location with messages. [7] When

a Facebook user sends a message from a smartphone using Messenger, the user's physical location can also be sent. Prior to a June 2015 update, unless a user changed the initial default settings of the program, the app would collect and display geo-location information with message content by default in all conversations on the Android app, including conversations in chat groups with people who are not direct friends on Facebook's social network. When the app first installs on a mobile device, a notice appears that informs the user that the app will collect and share geo-location information. After that notice appears, the only other indicator of location data collection and sharing is a small blue icon next to the textbox in a conversation. Figure 1 shows a screenshot of the Messenger app with this icon highlighted in Android.

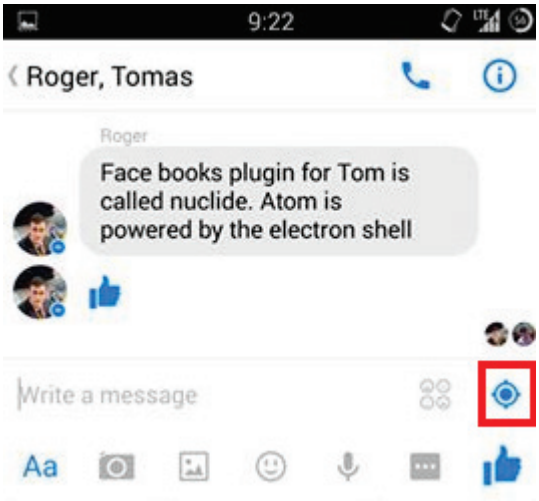


Figure 1. Image of Facebook Messenger's Android application showing a message sent by Roger. The small icon in the lower right, highlighted by a red box, is colored blue, showing that geo-location is being broadcast along with the message.

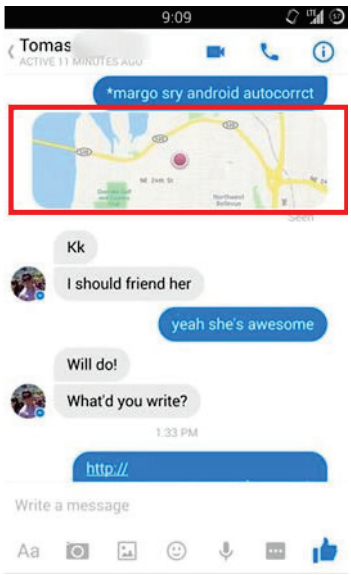


Figure 2. The results of tapping a message with location attached on the Android app. Tapping on the message "*margo sry android autocorrct" reveals a map showing where the message originated.

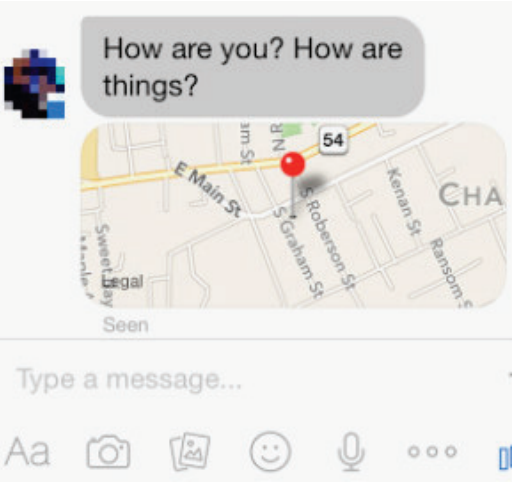


Figure 3. iOS app showing sender's location after the recipient clicks on a message with location attached. [8]

Other Facebook users can view shared geo-locations on the Facebook Messenger application by tapping on individual messages in their chat log, which reveals a map of the location where the individual was when the message was sent (Figure 2). On iOS, the application requests access to the device's geo-location data [9], and a similar interface for sharing location data in chats exists in the iOS Messenger app (Figure 3). On the desktop version of Messenger [10], geo-locations can be viewed by moving a mouse over a small pin attached to a message, to reveal a similar map (Figure 4).



Figure 4. An image of a chat with Keyon from Facebook Messenger's desktop web application. The small pins next to the messages, highlighted by red boxes, show that

geo-location is attached to these messages (and can be viewed by hovering the mouse over the pins).

A user can disable geo-location sharing for individual conversations by pressing the blue icon in the app. A user can also disable geo-location sharing at any time for all messages by going into the application settings and finding the option to disable it. Adjusting privacy controls for location sharing on mobile operating systems is not entirely intuitive, as evidenced by the number of popular sites that have felt the need to publish guides on how to adjust geo-location controls. [11] Prior to the June 2015 Messenger update, location data sharing was on by default in Android. It required user permission to become perpetually active in the iOS Messenger app. [8]

In 2012, CNET was the first major website to raise concerns about the privacy implications of Facebook Messenger's geo-location sharing feature. [12] A few other publications subsequently voiced concerns. [13, 14] Facebook did not take significant action to change the software in response to these concerns, and so the geo-location sharing continued to operate unchanged.

There was not significant public pressure for change after the initial news coverage about Facebook's location sharing settings. This raises two questions: (1) whether Facebook users knew about the geo-location collection and sharing, and (2) whether they cared about its privacy implications.

Facebook's location data practices presented an opportunity (1) to study how easy it is for a computer program to systematically copy the data and (2) to test whether Facebook's initial notification on app installation, along with the options to disable geo-location sharing within the Messenger app and through the Android and iOS system settings, were sufficient to satisfy the privacy concerns of users aware of the data sharing.

My interest in Facebook Messenger

I became interested in this issue during the spring of 2015. At the time, I was a junior at Harvard College and had been offered a summer internship position at Facebook doing software development. I had secured the internship through Harvard's Office of Career Services' (OCS) On Campus Interview program. The internship was a paid position starting June 1, 2015, and I had signed a letter of intent to join the company, although I was not to be considered an employee until my June 1 start date, meaning that I was not privy to any proprietary information. I was attracted to work at Facebook by the popularity of its products and its publicly professed "hacker culture", where "code wins arguments". [15]

Methods

My approach was to build an extension for a common web browser so that a person running the extension could see the geo-locations of any Facebook user who is sending them (or a chat group they are in) messages through Facebook Messenger. I would then make the extension publicly available and alert the public through a blog post, Twitter and online forums. This approach made public what some may already be doing – harvesting geo-location information about Facebook users they have been in conversations with. It also provided transparency and feedback to users about their geo-location settings on Facebook. If there was no reaction by users or Facebook, then Facebook's current geo-location data practices were potentially sufficient to address privacy concerns. My expectation was that the historical pattern of lack of public pressure on this issue evidenced from 2012 through May 2015 would continue.

The extension

The extension is a lightweight program (called a "script") that runs on Google's popular web browser, Chrome. After a user logs into a Facebook account, when the Facebook Messenger page appears on Chrome on a desktop computer, the script runs in the background. It detects calls to update the message page, requests a copy of the content and then plots the location data associated with the content onto a map that appears in the browser. This approach allows the extension to access all the geo-location data delivered to the browser. The precision of the location coordinates was accurate enough to locate a user to within a meter. It is important to note that all the data retrieved were accessible without the extension if a user clicked on the map icon for each message. The script did nothing illegal or malicious; rather, it accessed and displayed data already available to the user. Furthermore, the data aggregated on the map remained temporarily in memory and was discarded when the page reloaded. A full technical overview of the system can be seen in Figure 5. Using the extension, a user can choose to see a map of the geo-location data collected and shared by Facebook Messenger about the user and about others users in the same chat group. Figure 7 shows a demonstration of a map created with the extension.

I uploaded the Chrome extension to the Chrome Web Store, marking it as unlisted so that only those with a specific link, which I shared on my blog, could access it. [16] The title of the extension on the Chrome Web Store was "Marauder's Map", which can be seen in Figure 6. I also archived an open source copy of the code for the extension in an MIT-licensed Github repository with the title "marauders-map". [17] This repository contained the code and setup instructions for creating the extension from source.

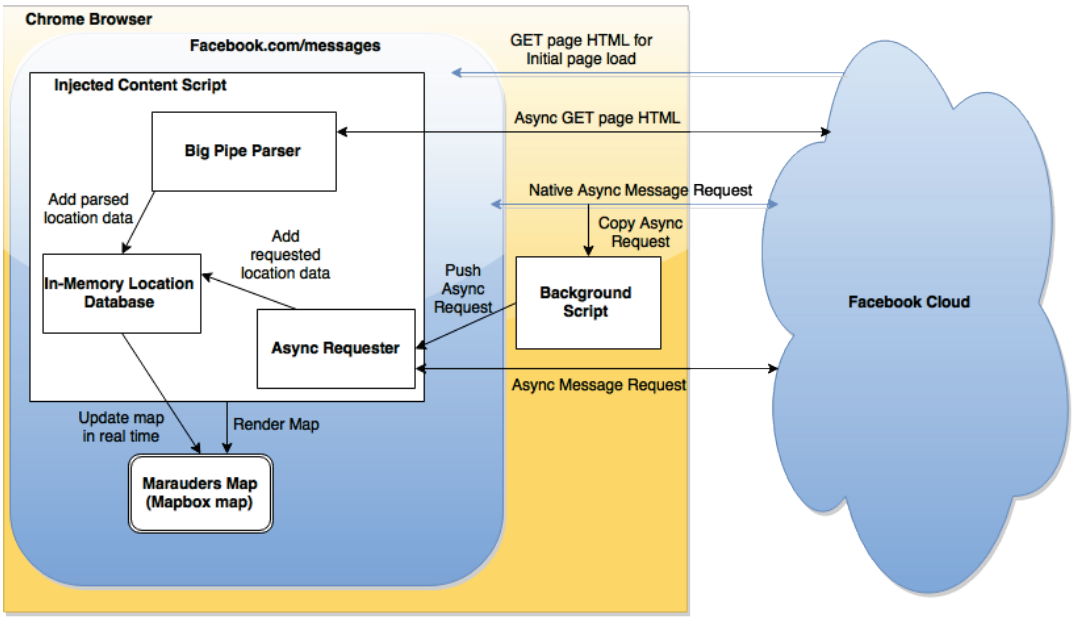


Figure 5. A graphical depiction giving a full technical overview of the marauders-map Chrome extension. White boxes represent the components injected by the extension. The extension consists of a Chrome background script that copies asynchronous requests from the desktop Facebook Messenger page to the Facebook cloud endpoint for retrieving messages, and then passes the HTTP bodies of these requests to an injected content script running on the Facebook Messenger page. This content script then emulates the original asynchronous request (automatically adding the appropriate headers) and plots the location data returned by Facebook onto a map drawn using the Mapbox API. With this base code, the extension can collect data on all messages loaded onto the page asynchronously. However, owing to optimizations in how Facebook delivers data to the browser, some messages are sent embedded in the initial HTML packet (via a protocol known as BigPipe). Using a simple asynchronous GET request, the content script pulls this HTML packet and uses a regular expression to parse the embedded location data from the messages, then plots the data on the map.

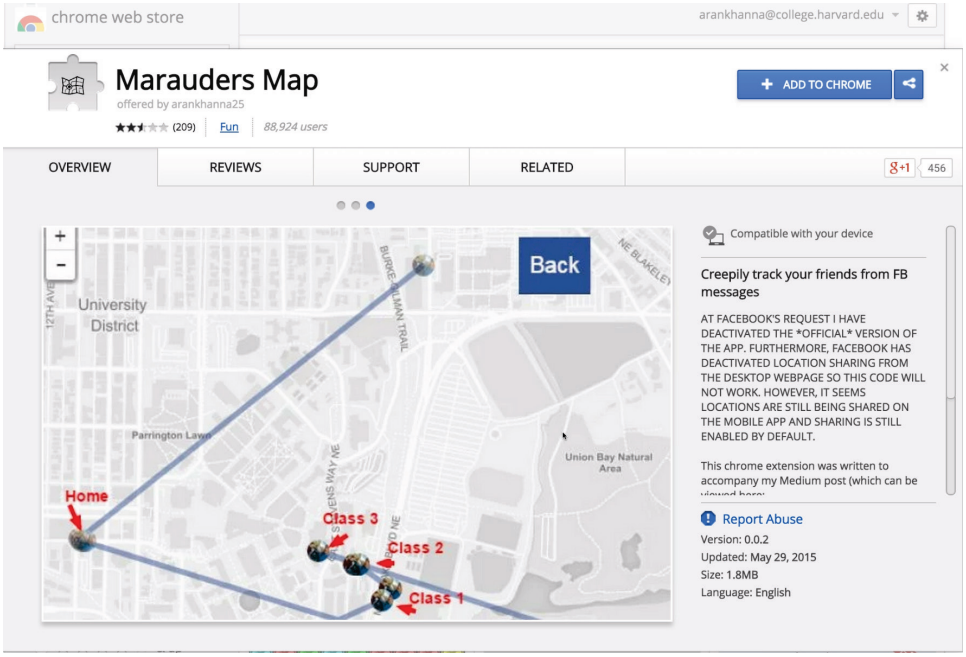


Figure 6. A screenshot of the extension download page in the Google Play store. Clicking the "Add to Chrome" button allowed users to automatically install the extension. The total number of users (88,924) the extension had acquired over its lifetime is visible next to the star rating in the top left.

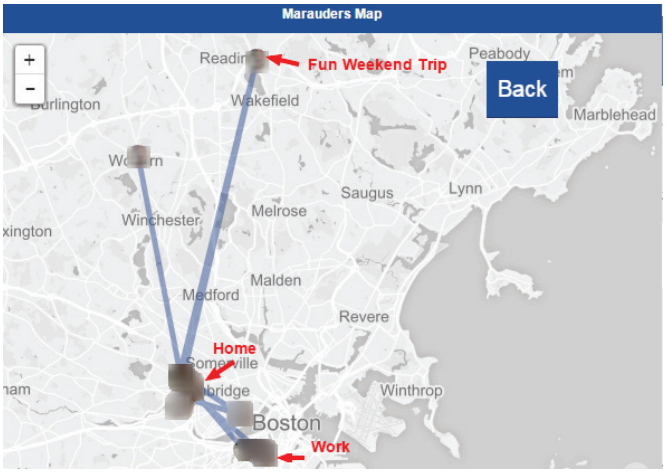


Figure 7. A labeled example of a map created by the extension

The blog post

I drafted a blog post that introduced me as an avid user of Facebook Messenger. The post highlighted the fact that the Facebook Messenger App transmits geo-locations alongside many of the messages sent from mobile devices. The post went on to describe how the

Marauder's Map extension aggregates this data onto a map. It noted that, at least on Android devices, the default setting for Messenger sends geo-location with messages. The blog also provided some examples from using the extension, including how a person's geo-location can accumulate over time to reveal travel patterns and other information.

Publicizing the blog

On May 26, 2015, I published the blog post and corresponding code on Medium.com. [18] I also posted URL links to the blog post and extension to both Reddit (reddit.com/r/privacy) [19], a popular forum for discussions on data privacy, and Hacker News (news.ycombinator.com) [20], a popular technical forum. Medium, Reddit, and Hacker News all have a voting system so that the most interesting articles are voted (or recommended) upwards to the top listings. Finally, using my public Twitter handle (@arankhanna), I sent out a tweet [21] asking my followers, consisting mainly of family and friends, to read the post.

This study used, as one measure of public concern over Facebook Messenger's sharing of geo-location data, the popularity ranking of my posts on the three sites. If the public response to the posts was indifferent, then the ratings would likely not increase on these forums. This study also examined the quantity of news coverage received and the total number of downloads of the extension as other measures of public concern. Finally, the study examined Facebook's response to any public concern.

Results

Media coverage

News of the blog went viral, starting within 24 hours of posting and continuing for about 72 hours afterwards.

For the first 12 hours of posting, little happened. The Reddit post received 7 upvotes, the Hacker News link also received 7 upvotes, and the Medium story had 3 recommendations by the end of the day. By the morning of the 27th, the story gained momentum on Twitter. Figures 8 and 9 show the Twitter responses to my posts over the week after I initially posted the blog. A total of 611 tweets and retweets reached a total follower audience of 3.63 million Twitter users.

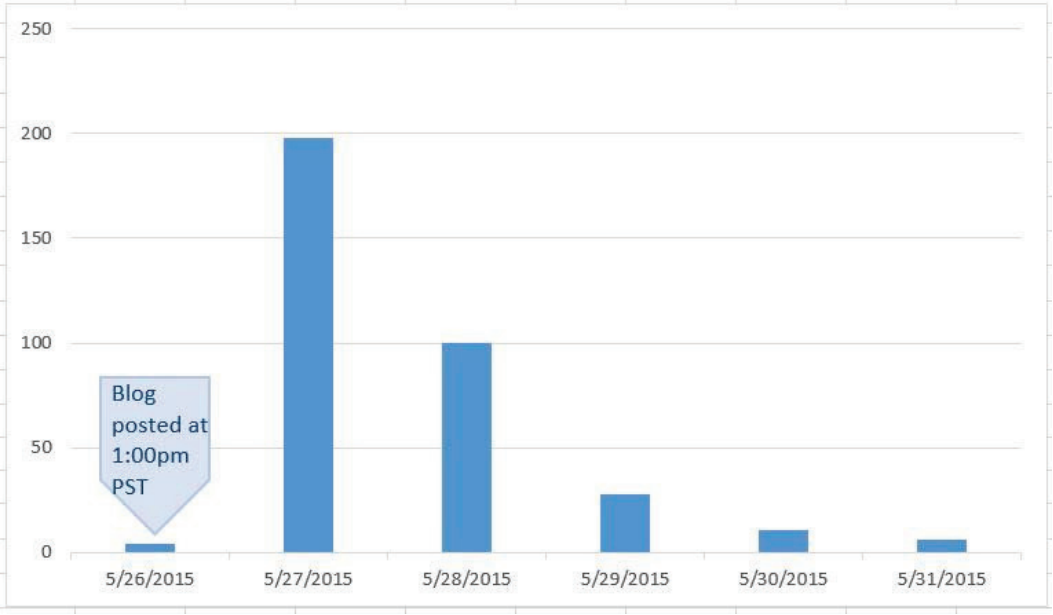


Figure 8. Twitter Activity after initial blog post. The total number of tweets about my posts per day between 5/26 and 5/31.

Of the public tweets, 57% appeared on 5/27 as the story initially went viral globally and hit the front page of various forums such as Medium, Reddit Privacy, and Hacker News. The Twitter data for Figures 8, 9, and 12 was gathered by searching through all public Tweets between 5/26 and 6/5 (using Twitter's native search) for mentions of my name, my Twitter handle, Marauder's Map, and links to any of my postings and then recording all relevant tweets, their author, and their time of release.

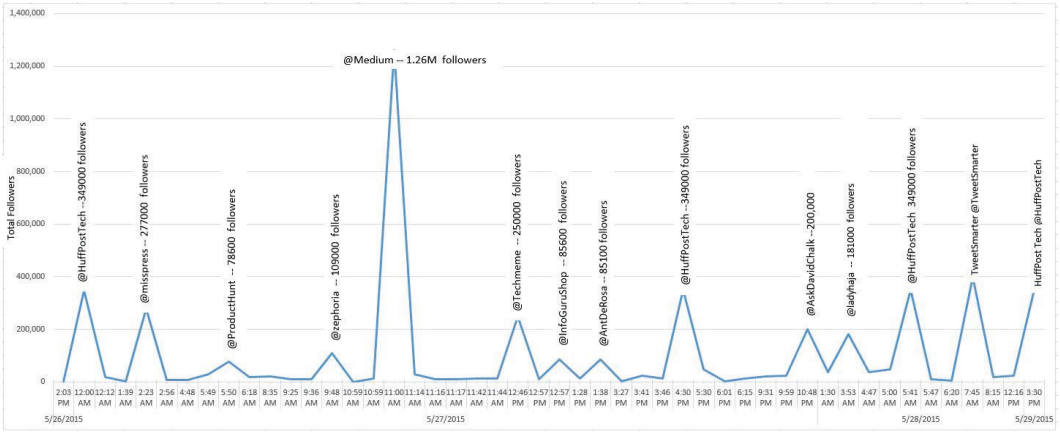


Figure 9. Twitter timeline. Total reach of tweets about my posts over the active hours between 5/26 and 5/29. The total number of tweets and retweets was 611 and the total number of Twitter followers reached was 3.63M.

The measure of reach is the number of followers the tweets were delivered to. The figure shows the total number of tweets and the total number of followers reached. The biggest boost came from Medium.com, which tweeted about the post and promoted it on its site. The tweets from the largest influencers (those with over 10k followers) are labeled.

The increased traffic to my posts raised their rankings. For example, my post on Medium became the most recommended story of the day. Posts linking to my blog and extension on both Hacker News and Reddit Privacy rose to the front page of both by 8 a.m. PST. By 9 a.m. PST, tech bloggers and content aggregators including *The Next Web*, *Computerworld,* and *The Huffington Post* covered the story in their blog posts and articles. *The Huffington Post* asked to directly cross-publish my Medium blog post on its site. Afterward, information about my posts spread to *Al Jazeera*, *The International Business Times,* and other major news organizations.

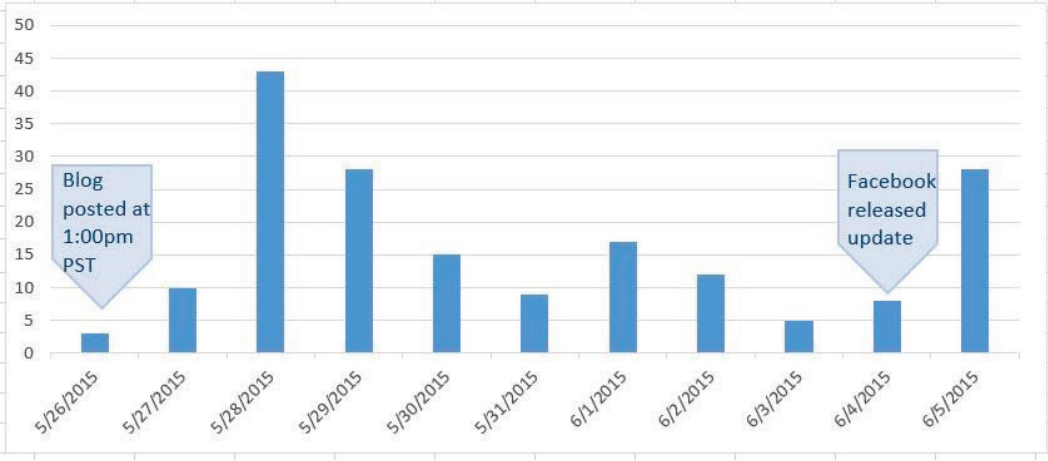


Figure 10. Press coverage after initial blog post. The total number of press stories about my posts per day between 5/25 and 6/5. I gathered the news data for Figures 10, 11, and 12 by searching for mentions of my name, my Twitter handle, Marauder's Map and links to any of my postings between 5/26 and 6/5 on Google News and recording all relevant stories, their author, their time of release and their country of origin.

By the 28th, only two days after my original posting, news stories about my posts appeared on *CNN*, *The Guardian*, *The Washington Post,* and many large international European, Australian, and Brazilian publications (e.g. *La Stampa*, *Der Standard*, *Globo*, *NDTV*, *The Sydney Herald*). By the 28th, large TV networks such as CNBC, ABC, CBS, and CNN had covered my posts as well. Figure 11 shows the total number of stories written about my posts per country.

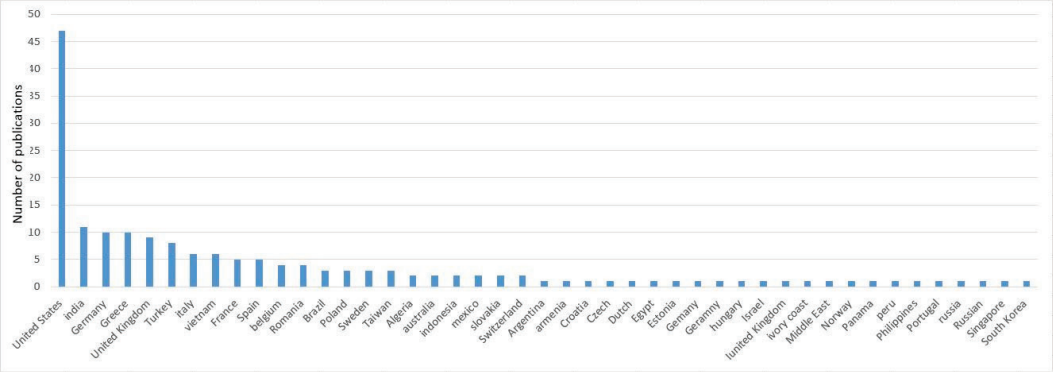


Figure 11. News coverage count by country. Count of news publications about my posts published on or before 6/5 grouped by country of origin.

The United States, Europe and India were the top three origins for stories overall, with the United States accounting for over a third of all stories written.

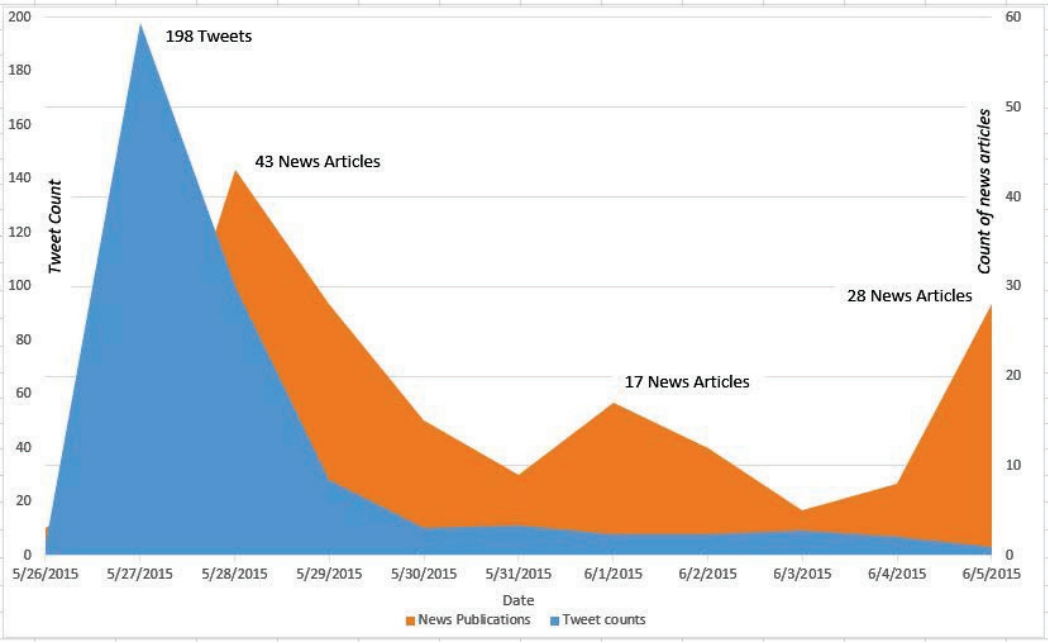


Figure 12. Twitter activity and news coverage by day. Number of tweets (right vertical axis) and press stories (left vertical axis) about my posts per day between 5/27 and 6/5. The total count of news publications was 178 and the total count of tweets was 347. The count of tweets and stories appearing on peak days are displayed.

Extension downloads

There have been more than 85,000 downloads of the Chrome extension since its release (Figure 6). Users continued to download the extension even after I deactivated it in response to Facebook's request, as described below.

Facebook's response

The afternoon of the 27th, one day after the Medium blog post's publication, Facebook contacted me. My future manager phoned and asked me not to speak to any press; however, I was told that I could keep my blog post up. By that evening, the global communications lead for privacy and public policy at Facebook called me to clarify Facebook's expectations that I not speak to the press, saying that his objective was to hamper the spread of what had become a damaging story.

By midday of the 28th, the global communications lead for privacy and public policy at Facebook requested by email that I disable the extension. I complied within the hour by deactivating the Mapbox API key associated with the extension so that all current and future users could no longer load the map used to display geo-location data.

On the morning of the 29th, three days after my initial posts, media reported that my Chrome extension was turned off and no longer viable. Additionally, Facebook had tweaked its code to remove location data from browsers. This alteration did not change Facebook's policy of collecting and sharing geo-location data by default from the Facebook Messenger app on Android and with user permission on iOS. However, Facebook no longer transmitted this location data to browsers. This action merely halted the use of an extension such as mine that uses browser data. Geo-locations remained visible on the Facebook Messenger mobile application, and seemingly, the map could be rebuilt using an interface to the mobile application.

On the afternoon of the 29th, three days after my initial posts, Facebook phoned me to inform me that it was rescinding the offer of a summer internship, citing as a reason that the extension violated the Facebook user agreement by "scraping" the site. The head of global human resources and recruiting followed up with an email message stating that my blog post did not reflect the "high ethical standards" around user privacy expected of interns. According to the email, the privacy issue was not with Facebook Messenger, but rather with my blog post and code describing how Facebook collected and shared users' geo-location data.

On June 4, nine days after my original posts, Facebook officially announced a Messenger update with a new feature requiring users to opt into sharing their location during chats. Sharing would no longer be the default. The press release did not mention the previous default settings for geo-location data and did not disclose with whom Facebook would share the previously collected data. [22] As of June 2015, shared geo-location data from before the update remains viewable on the mobile application, and users who did not update to the

new versions of the Messenger app on iOS and Android still share geo-locations in the same manner as before.

Discussion

At the beginning of the study, historical behavior by Facebook and its users suggested that there might not be significant public concern about Facebook Messenger's sharing of geo-location data. Even though the media had highlighted the issue four years earlier, Facebook had not been concerned enough to make any fundamental change to its software. So, why the big change now?

What seems to have made the difference was transparency. It is possible that before my extension and blog post, the degree of location data collection and sharing by Facebook Messenger was hard for an average user to notice and thus did not raise significant concern. Without public pressure, Facebook may have lacked significant incentive to change. My extension and blog post made the data collection and sharing practice real and transparent. The resulting public attention, with over 85,000 downloads of my tool, more than 170 news articles, and 3.6 million Twitter users exposed to my posts through tweets and retweets, seemed to motivate Facebook to react.

What does this say about privacy protection? Can we reasonably expect Facebook or others with an interest in collecting and sharing personal data, to be responsible guardians of privacy? Could this work have been done inside Facebook to understand how its users view the collection and sharing of their data?

Must future privacy guardians always be on the outside?

References

1. Darwell B. Facebook's frictionless sharing mistake. SocialTimes. January 22, 2013. http://www.adweek.com/socialtimes/facebooks-frictionless-sharing-mistake/289289

2. Facebook. Making It Easier to Share With Who You Want. May 22, 2014. http://newsroom.fb.com/news/2014/05/news-feed-fyi-giving-people-more-control-over-when-they-share-from-apps/

3. Hamburger E. Facebook gives up on automatically posting everything you do online. The Verge. May 27, 2014. http://www.theverge.com/2014/5/27/5754862/facebook-gives-up-on-automatically-sharing-everything-you-do-online-open-graph

4. Popper B. Facebook's social reader apps nosedive in popularity. The Verge. May 7, 2012. http://www.theverge.com/2012/5/7/3005580/facebook-open-graph-frictionless-social-reader-decline

5. Interdisciplinary Centre for Law and ICT. ICRI/CIR and iMinds-SMIT advise Belgian Privacy Commission in Facebook investigation. KU Leuven. March 31, 2015. http://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation

6. Because Facebook in Europe officially operates out of Ireland, the firm states that it formally abides by Irish regulations in the EU. See Facebook. Facebook Response to European Commission Communication on personal data protection in the European Union. Accessed July 30, 2015. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf

7. Facebook. A Faster Way to Message on Mobile. October 9, 2011. https://www.facebook.com/notes/facebook/a-faster-way-to-message-on-mobile/10150249543542131

8. McHugh M. Facebook Messenger Will Finally Stop Telling People Where You Are. Wired. June 5, 2015. http://www.wired.com/2015/06/stop-facebook-messenger-telling-people/

9. Burnham K. Facebook Messenger: 5 Misconceptions. InformationWeek. August 11, 2014. http://www.informationweek.com/software/social/facebook-messenger-5-misconceptions/d/d-id/1297913

10. Facebook Messages. https://www.facebook.com/messages/

11. Nickinson P. How to keep Facebook Messenger from sharing your location. Android Central. August 9, 2014. http://www.androidcentral.com/how-keep-facebook-messenger-sharing-your-location

12. Ciprani J. How to prevent Facebook Messenger from sharing your location. CNET. May 10, 2012. http://www.cnet.com/how-to/how-to-prevent-facebook-messenger-from-sharing-your-location/

13. Brinkmann M. Beware: Facebook Messenger Reveals Locations, Introduces Read Confirmations. gHacks Tech News. May 5, 2012. http://www.ghacks.net/2012/05/05/beware-facebook-messenger-reveals-locations-introduces-read-confirmations/

14. Murphy D. Facebook Adds Locations, Read Receipts to Messenger App. PCMag. May 6, 2012. http://www.pcmag.com/article2/0,2817,2404031,00.asp

15. Letter from Mark Zuckerberg pg. 67-70 of Facebook. Form S-1 for United States Securities and Exchange Commission. February 1, 2012.

http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm#toc287954_10

16. arankhanna25. Marauders Map. Chrome Web Store. May 26, 2015. https://chrome.google.com/webstore/detail/marauders-map/mliofombcghaamgjkmmmmlepkiacdhkh

17. arank. marauders-map. Github. May 26. 2015. https://github.com/arank/marauders-map

18. Khanna A. Stalking Your Friends with Facebook Messenger. Medium. May 26, 2015. https://medium.com/@arankhanna/stalking-your-friends-with-facebook-messenger-9da8820bd27d

19. arankhanna. I wrote a chrome extension to show how easy it is to track your friends' locations with Facebook Messenger. Reddit. May 26, 2015. https://www.reddit.com/r/privacy/comments/37db80/i_wrote_a_chrome_extension_to_show_how_easy_it_is/

20. arankhanna. Hacker News. May 26, 2015. https://news.ycombinator.com/submitted?id=arankhanna

21. @arankhanna. Check out this blog + extension I wrote about how your friends can track you from Facebook Messenger https://medium.com/@arankhanna/stalking-your-friends-with-facebook-messenger-9da8820bd27d … . Twitter. May 26, 2015. https://twitter.com/arankhanna/status/603293036693463040

22. Facebook. A New Way to Send a Location in Messenger. June 4, 2015. http://newsroom.fb.com/news/2015/06/a-new-way-to-send-a-location-in-messenger/

Authors

Aran Khanna is a senior at Harvard College majoring in Computer Science joint with Mathematics. During his time at Harvard he has interned at Microsoft, Novus, a hedge fund data analysis startup based in New York City, and Marianas Labs, a deep learning startup based in Mountain View. Aran is an active blogger in his free time and is passionate about the impact the increasing role of technology in our lives is having on our privacy.

Editor: Latanya Sweeney

Citation

Khanna A. Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger. Technology Science. 2015081101. August 11, 2015.

Data

Khanna A. Replication Data for: Facebook's Privacy Incident Response, a study of geolocation sharing on Facebook Messenger. Harvard Dataverse. August 10, 2011. http://dx.doi.org/10.7910/DVN/D2SNRI