# CS 1699: Privacy in the Electronic Society
## *Homework 2 – Location Privacy*

Jonathan Dyer

April 5, 2018

### Application Description

This mobile application fulfills a basic and essential location-based need for all reasonable humans: ice cream. Specifically, this app (henceforth known simply as *IceCream*) helps users identify nearby locations offering ice cream, and also maintains rankings and reviews of businesses that sell ice cream. As ice cream is best appreciated in a social setting, the application allows you to connect with other services such as Facebook, Twitter, or Google to indicate to fellow ice cream lovers that you are enjoying a cold treat at some particular location.

Such an app is desirable for at least the following reasons:

- Low-quality ice cream is a crime against food (and by extension humanity), and should be avoided at all costs. To this end, consumers should be empowered to make informed decisions about the ice cream they enjoy so that they can avoid more of the bad and learn about more of the good.
- Discovery of top-notch ice cream is of such importance (tantamount only to maintaining one's privacy) that it should not be relegated to general restaurant reviews in another app that cannot provide this task with the attention it deserves. A dedicated app allows you to keep track of all your favorites and where you found them, as well as sharring the love (and your opinions) more effectively with other fans out there.
- Finally, the best ice cream deserves the best company with which to enjoy it. However it is not always the case that you are aware of which of your friends are simultaneously in a mood for exploring the colder side of their natures. With IceCream, it is easy to discover if your fellow dairy-lovers are nearby and similarly inclined by allowing you to share a current or intended location with friends from connected social platforms who are also users of IceCream.

Of course, in order to provide the above services some location data must necessarily be collected and analyzed. This includes:

- Personal data you provide to us when (and if) you choose to create an account, possibly including full name, email address, phone number, birthday, gender, city/location on account creation, and where applicable any username or other public data associated with your Facebook or Google account if you create an account using those credentials.
- Data about your current location and/or IP address whenever the app is open on your mobile device. If you have enabled background location services for the IceCream app, location data will be provided to us in accordance with your device settings even when the app is not open.
- Any data you voluntarily provide to us during the course of your usage of the app, including (but not limited to) pictures you upload, reviews/rankings you submit (and your chosen username when you do so), and information that you submit to us in order to tailor the user experience to your preferences and needs.
- Information necessary to identify and invite your friends that use the app, including usernames and email addresses.

Note that some of the provided services require that we query other services and share your location with 3rd-party entities. This is done in such a way as to maximize privacy (see the following sections for details).

### Location Privacy Configuration

As hinted above, we take privacy almost as seriously as we take ice cream. You should be able to enjoy a maximally delicious treat with a minimum of compromise. Therefore there are several configurable options that provide our privacy-conscious users with a pleasing variety of privacy 'flavors' to match their preferences. These flavors each

describe a different preset privacy level that users can easily view and adjust via the dedicated Privacy panel in the IceCream application. The exception to this are the popular 'Toppings', which allow users a more granular choice of privacy settings. All are described forthwith:

- **Vanilla**: The default setting, kept by those users with a less discriminating privacy palate. Under this setting, all data collected as described in the previous section will be kept indefinitely (or until the user requests that it is deleted). This data is used to personalize recommendations for ice cream venues based on past user rankings and reviews and according to location. By default the user's location is shared with all friends who are also actively using the app at the time of sharing, and background location tracking is on by default (to allow the fastest, most accurate and up-to-date results). This allows for maximal utility of the application and most effective ice cream enjoyment.

- **Cookie Dough**: For those who prefer a nice mix of privacy and utility. This setting disables background location tracking and resets a user's location history data *monthly*, with only the anonymized, aggregated trace left behind (details are in the next section). All derived IceCream preferences are retained and remain associated with that user's profile (unless otherwise indicated in Toppings below). Additionally, user postings and reviews are submitted online with some randomized variance (rather than immediately) and some location aggregation is introduced into user data (see next section). Although this setting provides greater privacy, it also prevents long-term tracking of favorites from specific locations, since all location-and-identity-specific data is deleted after each month. Also search results may not be quite as relevant as with the Vanilla setting.

- **Dark Chocolate**: Our setting for those who are very intense about privacy (and/or ice cream!). This setting is even more strict than Cookie Dough, resetting IceCream location history data *weekly* and requiring that the user configure the 'Friends' topping to at least a basic level. It has background location collection disabled by default, and automatically anonymizes all rankings and reviews posted by the user henceforth. These reviews are also posted with very high variance. Location aggregation zone size is increased. Based on the 'Preferences' topping, user preferences and insights may optionally by purged on a weekly basis as well. This option provides a high level of privacy while still maintaining most of the functionality of the application.

- **Froyo**: So-called because it isn't really ice cream. This option indicates that you wish to use the app without logging in or maintaining a user account. This provides maximal privacy, but means that 1) preference-tracking, 2) flavor insights, 3) leaving reviews or ratings, and 4) connecting with friends will all be disabled. The app will simply work to provide information and reviews of nearby ice cream locations when it is activated.

In addition to the basic flavors, various additional settings are configurable as 'Toppings', allowing greater flexibility and privacy control:

- **Friends**: Enable and configure this setting to choose who to automatically share your ice cream location with, who never to share it with, what times of day to share it, and more.
- **Preferences**: Indicate here whether you would like to have your personal ice cream preferences reset and how often. If you choose this option, an anonymized version of your data will be stored and the original data associated with your account will be deleted.
- **Background**: Switch this on/off to enable/disable background location data collection.
- **ForgetMe**: This option allows you to delete your account *and* all data associated with it.
- Other features forthcoming.

## Obfuscation and Anonymization

In order to ensure that any data that IceCream uses does not infringe upon the privacy of its users, several techniques are employed to obscure potentially sensitive data:

1. **Obfuscation** is achieved by storing data at a low *granularity* in time–meaning that users who visit ice cream shops can be grouped according to chunks of time (say, half-day or full-day increments). This obscures the exact IceCream-related location history of the user, but still allows users to look back on their own history and allows IceCream to make recommendations. We do not need to know what time of day you were at a given location in order to use the fact that you loved the ice cream there.
2. On the topic of time of day, **randomizing** the delay between the time a user submits a review or preference and the time it is actually transmitted from the mobile device prevents the aforementioned obfuscation from being undercut by correlation between online/review presence and location-based attendance at a given shop. Even we can't precisely determine your location beyond the time range plus review-time variance.

3. Further **anonymization** is achieved by introducing spatial aggregation for all location data reported *when the user is not currently at an ice cream shop*. This allows us to provide reasonably accurate and relevant results while keeping the user's precise non-IceCream location obscured within a certain region.
4. Finally, as per [3] we may shorten the associated timing trajectories in our anonymized data (i.e. the data that we retain after a user purge or deletion in the Cookie Dough or Dark Chocolate policies). This is a simple but effective method to increase persistent anonymity after data is disassociated with the user that generated it.

Note that the above tactics rely primarily on increasing granularity, which has been noted in [2] to be less effective with many data points, but for those who are concerned (and using a more stringent policy as described above), the odds are that in a given month or week some user will *not* accumulate a large number of IceCream data points. Thus there is a low chance that those points could be used to deanonymize a user's data or compromise their location privacy.

Also note that the methods above have been implemented *in the device software*, before any data makes it to IceCream's servers. Thus even we are prevented from compromising your privacy at any stage. We believe this mechanism helps provide maximal protection of privacy and confidence in our policies.

### Combination of User Preferences and Obfuscation Techniques

There are a few ways that user preferences may interfere with the effectiveness of the techniques just described. The most obvious is by selecting the Vanilla policy, which does not regard privacy as the top priority. Otherwise it is worth noting that the more stringent your policy is, the easier it is to obfuscate and anonymize your data. This may sound basic, but it is significant in that we are essentially presenting users with an option to configure how anonymous they wish to remain. Thus we see that with the Cookie Dough setting comes decreased granularity in time and space, and even lower granularity when Dark Chocolate is selected.

What is remarkable is that the utility of the app is still able to be maintained even given these large steps to promote privacy. This is most likely because the app has a very specific and somewhat occasional use case. Most people get ice cream infrequently enough that their data is rather easier to anonymize than, say, a service that navigates you to various locations. Thus we can see that the app remains an effective option even for those users who are more careful about their privacy. These anonymization techniques remain viable due to the less frequent nature of ice cream consumption and the high flexibility of the options above. Even sharing with friends could be improved and made highly secure/private by using the methods suggested in [1].

### Conclusion

In summary, the application in question, **IceCream**, provides a substantial amount of privacy protection in addition to a great location-based service. For those users who are more tech-savvy or simply looking for a solution to the two great problems in life–*ice cream* and *privacy*–the IceCream app has you covered. A flexible, easily configurable privacy offering makes IceCream the natural choice for those who want the highest-quality, most relevant ice cream recommendations without sacrificing too much information. Even should you choose to stop using the app, our obfuscation and anonymization techniques ensure that it won't be tracked back to you at any point.

## References


[1] Andrew J Blumberg and Peter Eckersley. "On locational privacy, and how to avoid losing it forever". In: *Electronic frontier foundation* 10.11 (2009).

[2] Yves-Alexandre De Montjoye et al. "Unique in the crowd: The privacy bounds of human mobility". In: *Scientific reports* 3 (2013), p. 1376.

[3] Yi Song, Daniel Dahlmeier, and Stephane Bressan. "Not So Unique in the Crowd: a Simple and Effective Algorithm for Anonymizing Location Data". In: *primarily SIGIR*. Citeseer. 2014, pp. 19–24.