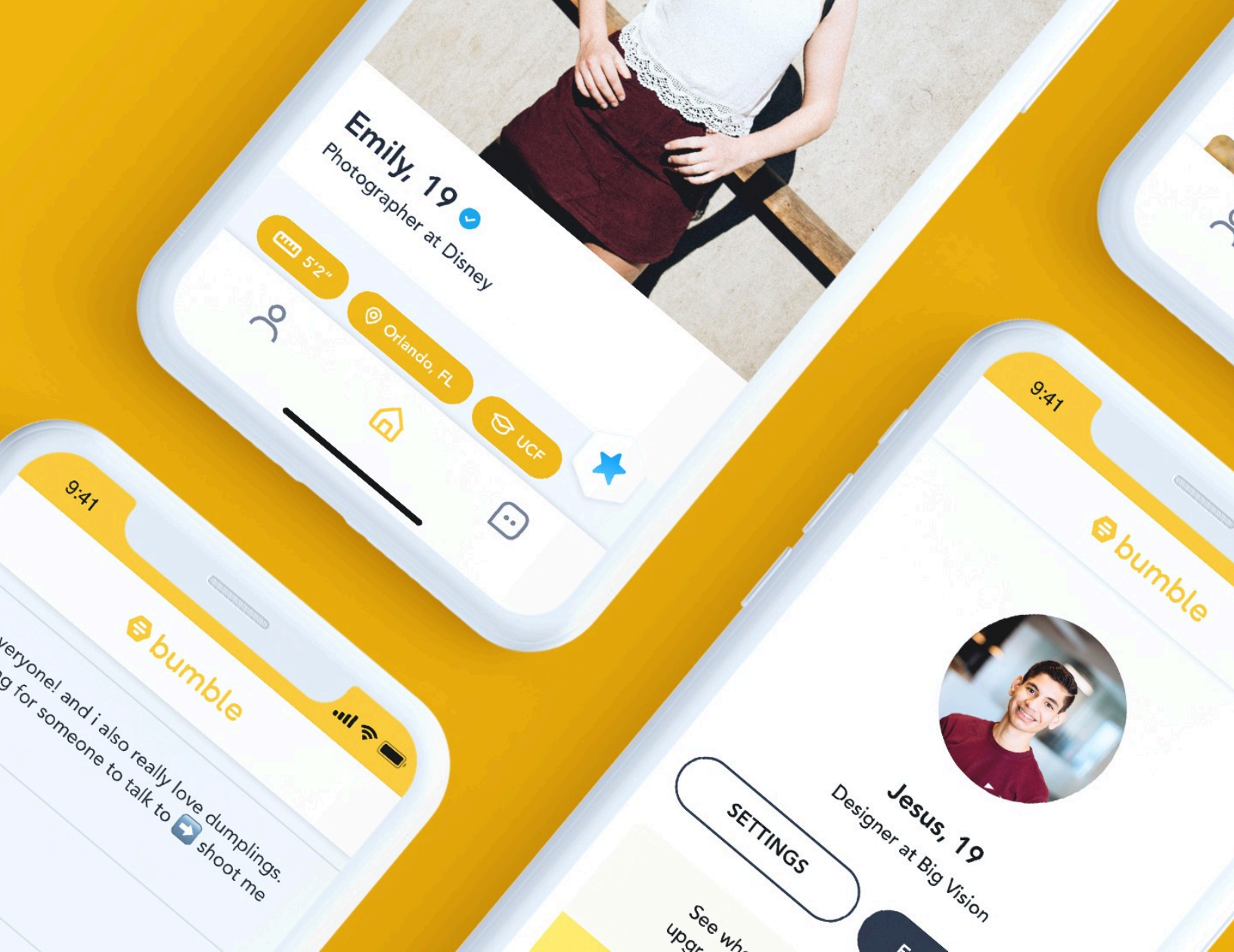




# Bumble Dating App

## Privacy Impact Assessment

*Cami Goray, Mariah Jacobs, Chris Kurien, Jinghan Ni*

*SI 540 - Privacy in Information Technology - Winter 2021 - Florian Schaub*

## Table of Contents

|                                                                |           |
|----------------------------------------------------------------|-----------|
| <b>Executive Summary</b>                                       | <b>3</b>  |
| <b>Introduction</b>                                            | <b>5</b>  |
| <b>What is Bumble?</b>                                         | <b>5</b>  |
| <b>Threshold Assessment</b>                                    | <b>5</b>  |
| <b>Stakeholders</b>                                            | <b>6</b>  |
| Bumble Users                                                   | 6         |
| Bumble Inc.                                                    | 8         |
| Third-Party Providers                                          | 8         |
| <b>Data Processing &amp; Information Flows</b>                 | <b>9</b>  |
| <b>Privacy Risk Analysis</b>                                   | <b>11</b> |
| Identified Privacy and Related Risks                           | 12        |
| Collection & Disclosure of Sensitive Profile Information       | 12        |
| Collection & Disclosure of Location Data                       | 14        |
| Linked Accounts                                                | 15        |
| Screenshotting & Screen-recording Information on Bumble        | 16        |
| Surveillance of User Messaging/Chat                            | 17        |
| Users Creating False Identities for Catfishing                 | 17        |
| Default Sharing Data with Third-Party Advertisers              | 18        |
| Privacy Settings Exist Behind Paywall                          | 19        |
| Zombie Accounts                                                | 20        |
| Compliance with Laws, Regulations, Codes and Guidelines        | 20        |
| Collection & Dissemination of Sensitive Personal Information   | 20        |
| GDPR                                                           | 21        |
| CCPA                                                           | 21        |
| Collection & Dissemination of Location Information             | 21        |
| FTC                                                            | 21        |
| Linked Accounts                                                | 22        |
| Screenshotting Personal Information & Catfishing               | 22        |
| <b>Privacy Risk Mitigations &amp; Recommendations</b>          | <b>24</b> |
| Mitigation Measures                                            | 24        |
| Risk: Collection & Disclosure of Sensitive Profile Information | 24        |
| Risk: Collection & Disclosure of Location Data                 | 25        |
| Risk: Screenshotting & Screen-recording                        | 26        |
| Risk: Users Creating False Identities for Catfishing           | 26        |
| Risk: Surveillance of User Messaging/Chat                      | 27        |

|                                                                            |           |
|----------------------------------------------------------------------------|-----------|
| Risks: Linked Accounts & Default Sharing Data with Third-Party Advertisers | 27        |
| Risk: Zombie Accounts                                                      | 28        |
| Risk: Privacy Settings Exist Behind Paywall                                | 28        |
| Recommendations                                                            | 29        |
| Recommendation 1: Control over badge visibility                            | 30        |
| Recommendation 2: Privacy features by default                              | 30        |
| Recommendation 3: Inform of friend's list linking                          | 30        |
| Recommendation 4: Location control                                         | 31        |
| Recommendation 5: Account deletion reminders                               | 31        |
| Recommendation 6: Screenshotting Policy                                    | 31        |
| <b>Solution Proposal</b>                                                   | <b>32</b> |
| Design Proposal 1: Location Control                                        | 32        |
| Rationale                                                                  | 32        |
| Prototype                                                                  | 33        |
| Limitations                                                                | 34        |
| Design Proposal 2: Screenshotting Policy                                   | 35        |
| Rationale                                                                  | 35        |
| Prototype                                                                  | 35        |
| Limitations                                                                | 39        |
| <b>Conclusion</b>                                                          | <b>40</b> |

## Executive Summary

Our privacy impact assessment (PIA) process followed David Wright's methodology in "Making Privacy Impact More Effective."<sup>1</sup> Our initial analysis includes a threshold assessment to justify why this PIA is necessary. We describe the stakeholders involved, as well as how the information is shared, stored, and transmitted throughout the app, paying special attention to data vulnerabilities. We then provide an in-depth outline of the privacy risks discovered in the app. Those risks are compared to appropriate laws and regulations. Finally, we conclude by sharing what is currently done to mitigate risks, our recommendations for how to prevent further risk, and potential solutions in the form of a documented prototype. A summary of our findings can be found below.

### ***Stakeholders***

Three stakeholders were identified: (1) Bumble users, (2) Bumble Inc, and (3) Third-Party Providers. Each stakeholder is directly responsible for impacting users' privacy (Bumble Inc. and Third-Party Providers) or have their privacy impacted (Bumble users) by using Bumble.

### ***Information Flows***

To document the flow of data within the Bumble ecosystem, we created an information flow diagram. Key information flows from our information flow diagram of Bumble are as follows: (1) user account registration, (2) user account maintenance, (3) user profile creation and editing, and (4) user interaction.

### ***Identified Privacy Risks***

To evaluate the privacy risks associated with Bumble, the team used a privacy risk analysis matrix to place nine identified privacy issues into an overall risk category based on the likelihood of harm and the severity of the harm of each issue. The risks that were identified as high risk are highlighted below in bold.

- **Collection & Disclosure of Sensitive Profile Information**
- **Collection & Disclosure of Location Data**
- **Linked Accounts**
- **Screenshotting & Screen-recording Information on Bumble**
- **Users Creating False Identities for Catfishing**
- Surveillance of User Messaging/Chat
- Default Sharing Data with Third-Party Advertisers
- Privacy Settings Exist Behind Paywall
- Zombie Accounts

---

<sup>1</sup> David Wright. "Making Privacy Impact Assessment More Effective". The Information Society: An International Journal. 29(5):307–315, 2013. <http://dx.doi.org/10.1080/01972243.2013.825687>

## ***Mitigation Strategies***

Throughout the course of this assessment 18 potential mitigation measures were identified to combat the 6 high-risk privacy risks. The measures were ranked based on (1) feasibility in terms of resources (time and money) required, (2) impact on user experience in terms of how it will enhance the utility, usability, and enjoyment of engaging with the app, (3) urgency (legal and financial consequences of not implementing the measure). The top six measures were:

1. Allow increased user control over Bumble badge visibility (Technological)
2. Provide more privacy features by default and reject monetization of privacy measures (Technological, Organizational)
3. Inform users in the app if their friends lists will be or already has been shared as a result of linking accounts (Technological, Procedural)
4. Allow users to hide their specific location or adjust their location manually (Technological)
5. Send users mobile notifications to delete their profile if they have not actively used Bumble in the past 30 days. (Technological, Procedural)
6. Strike policy for screenshotting for serial-screenshotters (Technological, Procedural)

## ***Solutions***

Two distinct solutions were developed in accordance with mitigation strategies 4 and 6 as they provided the most interesting design challenges.

### ***Solution 1: Location Control***

We propose an alternative onboarding process that allows the user more choice in location settings and provides better privacy notice about the visibility of their personal information. Rather than allowing Bumble to access a user's phone geolocation coordinates, during their onboarding process, users should be able to input an approximate location, as well as select whether this information is visible to other Bumpers. Bumble could also allow users to specify in what location they are looking for matches, and within what radius, to allow them to see matches in a more specific area than the location that they're willing to share they are located.

### ***Solution 2: Screenshotting Policy***

To deter people from repeatedly capturing permanent photos and videos of other users' profiles, we are proposing Bumble develop a Screenshotting Policy. The crux of this new policy would be a tiered strike system that keeps track of when users screenshot other people's information. With each screenshot (strike) that a user makes they would be given a specific consequence. If users screenshot their own profile, they do not receive a strike.

## Introduction

We performed a privacy impact assessment on the dating app Bumble. Today, the app boasts over 40 million users. Bumble differentiates itself by enabling women in heterosexual matches to initiate the conversation by sending the first message. Bumble's CEO, Whitney Wolfe, has been vocal about the app's efforts to mitigate harassment through measures such as the implementation of a new moderation policy prohibiting erotic content. It also bans profile photos that do not contain the profile user.

Bumble's privacy policy can be found here: <https://bumble.com/privacy>.

## What is Bumble?

Launched in 2014, Bumble is a dating app that utilizes a swipe right/left model to help users sort through and connect ("match") with potential partners. Bumble caters to a diverse audience and supports heterosexual and non-heterosexual relationships. Since its founding, Bumble has grown to support several "modes". Users can be in a dating mode, BFF mode (for those looking to find platonic friends), and Bizz mode (for those looking for career networking). For this PIA, only the dating mode will be assessed<sup>2</sup>. Bumble also supports a web version of their app (Bumble Web) that allows the same functionality as their mobile application<sup>3</sup>.

What makes Bumble unique in the online dating market is their goal of empowering women to control the conversation when dating<sup>4</sup>. Bumble does this by requiring women to send the first message in a heterosexual match. If she does not make a move within 24 hours of a match, the match will expire<sup>5</sup>. Bumble claims that prompting women to initiate the conversation has led to "the highest post-match chat rate in the industry"<sup>6</sup> as well as lower rates of harassment and abuse.

## Threshold Assessment

Like many other dating apps, Bumble presents several privacy risks, from the moment users are onboarded to when they match with other users. When users create a profile, they have the option of signing in with their Facebook account. Bumble states in their privacy policy that this allows them to see the user's Facebook data, including their friends' lists. Users may also choose to sign in with either an Apple ID or a phone number. These sign-in methods are more limited in the amount of data they make available to Bumble; however, they are far from anonymous or

---

<sup>2</sup> Johnson, D. (2021, March 2). What is Bumble? How the dating app differs from its competition, and what it offers women. Retrieved March 11, 2021, from Business Insider website: <https://www.businessinsider.com/what-is-bumble-app>

<sup>3</sup> What is Bumble Web? (2020). Retrieved March 11, 2021, from Bumble website: <https://bumble.com/en/help/what-is-bumble-web>

<sup>4</sup> What is Bumble? (2020). Retrieved March 11, 2021, from Bumble website: <https://bumble.com/help/what-is-bumble>

<sup>5</sup> Unless the user pays for Premium features.

<sup>6</sup> What is Bumble? (2020). Retrieved March 11, 2021, from Bumble website: <https://bumble.com/en/help/what-is-bumble>

pseudonymous, since Bumble still collects this data and uses authentication measures to verify the person creating the profile. For example, Bumble requires that at least one of the photos in the profile is *only* of the individual user. Bumble also screens this photo to ensure that it is not a fake photo found on the internet or a photo of an underaged (< 18 years old) user. User verification is one strategy to mitigate catfishing.

Even though potential matches and matches can only see the user's first name, with the amount of information in the profile -- especially geographic location -- it does little to protect the user's identity. For example, if people state the company they work for or university they attend, other users can simply search in a public directory like a school directory, voter registration database, or on LinkedIn to locate the individual.

Furthermore, users are encouraged to link other social accounts, such as Instagram or Spotify, to their profile so that potential matches can access more information about them. While it is optional for users to link their accounts, peer pressure in the form of *herd behavior* nudges users to reveal more information about themselves.

In summary, these issues strongly indicate that a PIA is necessary to further understand not only how Bumble users' data may be at risk, but also to what extent they are given control of their data. Some questions we hope this PIA will answer include:

- How can dating app users be empowered to have a choice in sharing or retracting their information?
- How can online dating apps like Bumble balance the privacy of personal information while also validating true identities?
- How long does Bumble keep user profiles? Even if the app is deleted, will the information still be kept in a database?
- How does Bumble communicate with users how personally identified information is stored?
- How can platforms like Bumble implement privacy measures that help mitigate the potential risks users face by sharing personal information with strangers?

## Stakeholders

### ***Bumble Users***

Online dating has become one of the most common ways to find a romantic partner in the United States. In fact, according to a 2019 survey<sup>7</sup>, almost 40% of heterosexual couples and 65%

---

<sup>7</sup> Rosenfeld, M. J., Thomas, R. J., & Hausen, S. (2019). Disintermediating your friends: How online dating in the United States displaces other ways of meeting. *Proceedings of the National Academy of Sciences*, 116(36), 17753–17758. <https://doi.org/10.1073/pnas.1908630116>

of same-sex couples now meet online. Simply put, online dating is becoming an unavoidable part of dating culture and draws in a wide variety of users.

Since the purpose of online dating is to find a potential partner, creating a profile on dating apps often requires users to share personal details about themselves with complete strangers and the company providing the service. Bumble in particular allows users to share photos, interests, work, education, political affiliation, sexual preference, habits (smoking, exercise, etc.), and more. While some of this information seems rather benign on its own, combined together it gives insight into who a person is, the things they like, and what they do with their time. All this information when used for intended purposes can result in successful matches; however, when used for unintended purposes, it can result in devastating privacy consequences for users. Though online dating users typically use positive terms to describe their experiences, there have been growing concerns of harassment, stalking, and sexual assault due to the nature of the information that is shared on these platforms. These issues are most often experienced by women under the age of 35. A 2020 Pew study found that of women under the age of 35 who have used online dating sites/apps<sup>8</sup>:

- 60% say someone has continued to contact them after they were not interested (compared with 27% of men in this age range)
- 57% say they have received a sexually explicit message or image they did not ask for (compared with 28% of men in this age range)
- 44% say they were called an offensive name (compared with 23% of men in this age range)
- 19% say they were threatened with physical harm (compared with 9% of men in this age range)

Looking into the types of information that Bumble collects and displays from users will provide valuable insight into how well existing privacy features are protecting users from the pitfalls of online dating. Additionally, Bumble provides some of the sensitive information that is collected to third party advertisers. This poses various privacy concerns for users who do not want the information from their dating profile to inform the advertisements they get.

Additionally, Bumble users also pose privacy risks to each other as information on dating applications can be screenshotted and shared with non-Bumble users. Some users may also provide false information and catfish others, resulting in them getting access to personal information.

---

<sup>8</sup> Anderson, M., Vogels, E. A., & Turner, E. (2020, February 6). The Virtues and Downsides of Online Dating. Retrieved March 11, 2021, from Pew Research Center: Internet, Science & Tech website: <https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/>



The results from this assessment will be helpful to current users who want to see if they should continue using Bumble and for new users to determine whether Bumble is the right dating application for them.

### ***Bumble Inc.***

Since Bumble is directly responsible for deciding how it conducts business and what services to offer, the company is one of the key stakeholders for this assessment. Bumble is responsible for deciding what information to collect, how to store it, and how to ultimately use it. These are all decisions that will have a direct impact on users' privacy. These decisions are made by C-level executives as well as various managers and directors.

Within Bumble, product designers and managers also play a role in users' privacy experiences. These people are directly responsible for developing and implementing features that help account for some of the external harms like stalking/harassment that can come from sharing personal information with strangers.

Other Bumble employees that impact users' privacy include chat moderators who will have access to user's chat content which may contain more personal details like phone numbers or explicit content.

### ***Third-Party Providers***

Currently, Bumble sends user information to third-party advertising networks. The ways in which users' information is used by these networks plays a direct role in the privacy a user experiences. Getting advertisements for personal information that was only shared on Bumble may feel like an intrusion of privacy for some users.

Bumble allows users to connect their Instagram account with their Bumble profile, meaning that people can view up to 24 recent posts from a user's Instagram account without ever having to leave the Bumble app. While Bumble does not reveal a user's Instagram username or any of the tags, comments, and captions from a post, people can still view many personal photos. This integration can provide people with more information about a person. Additionally, with the integration Instagram gets access to user information entered in Bumble.

When users first create accounts on Bumble, they are allowed to use Apple or Facebook to make an account. As a result, Apple and Facebook receive access to information from Bumble. Bumble's Privacy Policy reminds users that "when you register with a third party, you are also giving them personal information, so we recommend that you read their Privacy Policies as

Bumble does not control how they use their information”<sup>9</sup>. Policies created by these companies also play a role in how user data is used.

## Data Processing & Information Flows

To visually illustrate the stakeholders and the flow of data within the Bumble ecosystem, we have created an information flow diagram. The diagram’s key lists five stakeholders and four color-coded ways in which data is handled to show when it is collected, stored, protected, and shared. These four codes are inspired by the Department of Homeland Security’s (DHS) privacy office official guidance<sup>10</sup>. DHS indicates that the “PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed.” Therefore, in the diagram below, we aim to identify and map out the following, as recommended by the DHS:

1. Data in the system (e.g. what data is collected and why)
2. Attributes of the data (e.g. use and accuracy)
3. Sharing practices
4. Notice to Individuals to Consent/Decline Use
5. Access to data

We are limiting our investigation to the free Bumble account, although a paid premium option is available to users, and they can activate it anytime during their use of Bumble. More features are available in the premium option, with additional data points and information flows; however, it is out of scope for our research and investigation.

Key information flows from our information flow diagram of Bumble are as follows:

- **User account registration** involves collection of user data by Bumble, third-party authentication services, and potentially linked third-party social media platforms. User data is also stored by Bumble on a global network of servers.
- **User account maintenance** involves collection of user data by Bumble, which may also be stored by Bumble for designated periods of time.
- **User profile creation and editing** involves collection and storage of a large amount of user data, as well as the sharing of that information with Bumble and potentially third party social media platforms and third party advertisers. If the user opts out of targeted ad data collection, their data will be protected from being shared with third party advertisers.
- **User interaction** involves the collection and storage of user swiping pattern behavior with Bumble in order to train their matching algorithm to display relevant matches to a

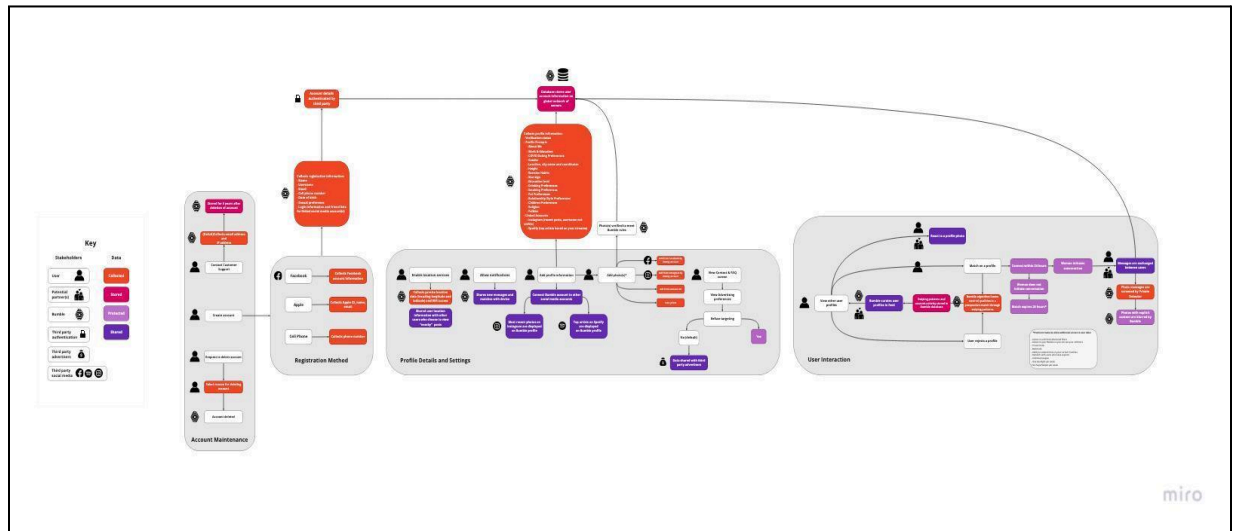
---

<sup>9</sup> Bumble - Privacy. (2021). Retrieved March 30, 2021, from Bumble website: <https://bumble.com/privacy>

<sup>10</sup> [https://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_guidance\\_june2010.pdf](https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf)

user. It also involves sharing of a user's profile information with other users on their match feeds, but offers some protection of (and from) personal data through measures such as requiring the woman to initiate conversation or screening users' exchanged messages for explicit photos.

The full information flow can be viewed in detail on [Miro](https://miro.com/app/board/o9J_kk4AFs4=/)<sup>11</sup>. Below is a preview of the diagram.



<sup>11</sup> [https://miro.com/app/board/o9J\\_kk4AFs4=/](https://miro.com/app/board/o9J_kk4AFs4=/)

## Privacy Risk Analysis

In order to evaluate the privacy risks associated with Bumble, the team used a privacy risk analysis matrix to place nine identified privacy issues into an overall risk category based on the likelihood of harm and the severity of the harm of each issue. In the **Identified Privacy and Related Risks** section, each risk is discussed in greater detail. In the **Compliance with Laws, Regulations, Codes and Guidelines** section, the team examines Bumble's five highest risks (as determined by the risk analysis matrix) in relation to the existing policies that relate to and address (or fail to address) the identified risks.

## Privacy risk analysis

| Severity of impact | Serious harm   | Likelihood of harm |                        |                      |
|--------------------|----------------|--------------------|------------------------|----------------------|
|                    |                | Remote             | Reasonable possibility | More likely than not |
|                    |                | Likelihood of harm |                        |                      |
|                    | Some impact    | Low risk           | Medium risk            | High risk            |
| Minimal impact     | Minimal impact | Low risk           | Low risk               | Low risk             |
|                    |                | Low risk           | Low risk               | Low risk             |

|                                                             |                 |                                       |                                                   |
|-------------------------------------------------------------|-----------------|---------------------------------------|---------------------------------------------------|
| Collection & Dissemination of Location Data                 | Linked Accounts | Screen-shotting & screen-recording    | Default Sharing Data with Third-Party Advertisers |
| Collection & Dissemination of Sensitive Profile Information |                 |                                       |                                                   |
| Users Creating False Identities for Catfishing              |                 |                                       |                                                   |
| Surveillance of User Messaging                              | Zombie Accounts | Privacy Settings Exist Behind Paywall |                                                   |

## Assessment metrics

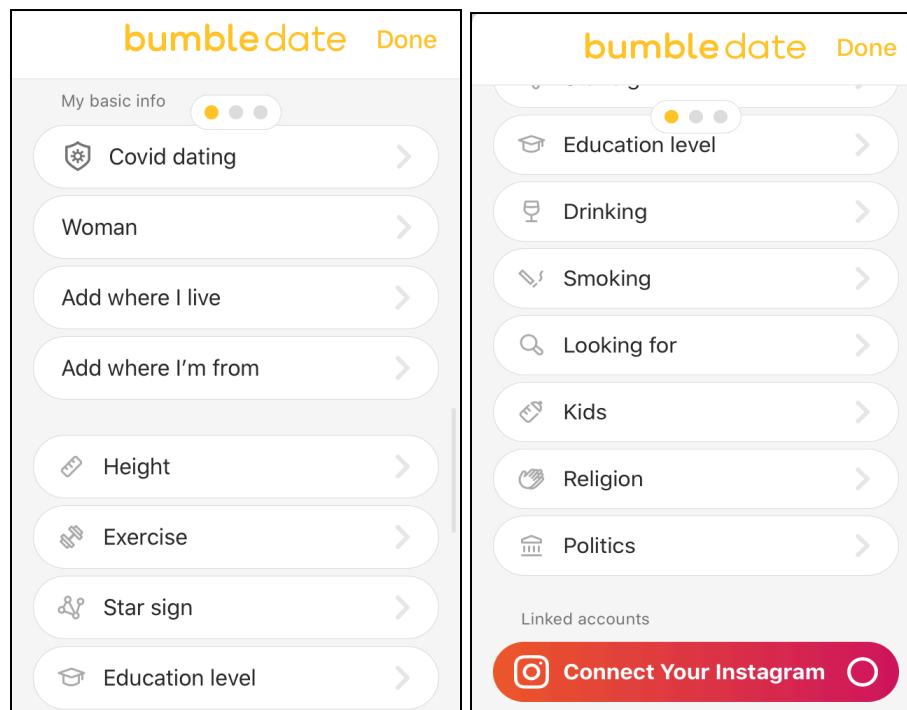
- Likelihood of harm (remote, possible, probable)
- Severity of harm (minimal, significant, severe)
- Overall risk (low, medium, high)

Figure 1: Privacy Risk Analysis Matrix for Bumble

## Identified Privacy and Related Risks

### Collection & Disclosure of Sensitive Profile Information

When a user creates an account on Bumble and then proceeds to fill out their dating profile, they are asked to disclose detailed personal information. This information is specified in the data processing and information flow diagram on page 7. As a dating service, Bumble profiles have more opportunities for sensitive disclosure of personal information than other user profiles on social media platforms like LinkedIn, Twitter, Instagram, or even Facebook. Bumble allows users to select and display badges on their profiles to represent personal attributes like sexual identity and preferences; religious and political affiliation; education level; preferences for children; and even health details, such as height, exercise habits, drinking habits, and smoking habits (Figures 2-3).



Figures 2-3: User Profile Badges on Bumble

Once a tag is added to a user's profile, it is visible to every other user on the app who sees that profile as a suggested match. It is up to a user's discretion what details they choose to provide.

The Bumble Privacy Policy notes this with the following statement:

*"Please be careful about posting sensitive details about yourself on your profile such as your religious denomination and health details. You may also choose to add sensitive information about yourself when you add certain Bumble Badges to your profile, such as*

*your religion and political leanings. While you may voluntarily provide this information to us when you create your profile, including your sexual preferences, there is no requirement to do so.”<sup>12</sup>*

However, users may feel pressured to supply the information in a few different ways. First, a user may feel pressured to “complete their profile,” an action which is prompted by Bumble on the user’s home screen, along with a displayed status of the percentage that the profile is “complete”. Second, users may suspect that Bumble ranks more complete profiles more highly with their algorithms, resulting in these profiles getting shown to other users more often; based on the language on Bumble’s website, users would be correct in this assumption<sup>13</sup>. This assumption about the Bumble algorithm could also serve as an incentive to disclose more details than they normally would to the platform and to other users on the app. Third, and finally, users may feel an aspect of social pressure to disclose their personal details — either because it is an expected social norm<sup>14</sup> or because they view it as an important part of finding a good match which, again, Bumble encourages<sup>15</sup>.

Disclosing such a large amount of detailed personal information comes with a decent amount of risk. According to Solove’s taxonomy of privacy harms<sup>16</sup>, there is opportunity for privacy harm to occur during the collection, processing, and dissemination of a user’s profile information:

- When a user’s information is **collected** by Bumble, it could be surveilled by someone who is monitoring the user’s wireless connection or surveilled by Bumble itself. The collected data may also be retrieved via reverse engineered REST API attacks, as was exposed by researchers at the Independent Security Evaluators (ISE) Labs in November 2020<sup>17</sup>.
- When the information is **processed**, it becomes an aggregated collection of data that can be used to identify a user and could be sold to third-party advertisers for secondary use.
- When the information is **disseminated** to others on the platform and outside of it, Bumble runs the risk of exposing private information about users to entities beyond their control or even knowledge. According to Bumble’s Privacy Policy, users’ profile badges are sold to third party advertisers if the user does not opt out of targeted advertisements. Additionally, other Bumble users may use profile information in a harmful way -- such as by targeting a user for catfishing or blackmail by screenshotting

---

<sup>12</sup> <https://bumble.com/privacy>

<sup>13</sup> <https://bumble.com/the-buzz/how-to-get-more-matches>

<sup>14</sup> See Warner et. al (2020)’s work on “Evaluating ‘Prefer not to say’ Around Sensitive Disclosures” for a discussion on how opting not to disclose personal information invites suspicion of dishonesty, and even ostracization, for users who try to retain their privacy.

<sup>15</sup> <https://bumble.com/the-buzz/how-to-use-filters-on-bumble>

<sup>16</sup> Solove, D. J., (2006, January). *A Taxonomy of Privacy*. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, GWU Law School Public Law Research Paper No. 129, <https://ssrn.com/abstract=667622>

<sup>17</sup> Sarda, S. (2020, November 24). Reverse Engineering Bumble’s API - Independent Security Evaluators. Medium. <https://blog.securityevaluators.com/reverse-engineering-bumbles-api-a2a0d39b3a87>

the information and sharing it outside of the Bumble platform, potentially even with people who know the user in the offline world, but may not know such sensitive details about their identity or preferences.

In addition to Solove's risks, these occurrences could result in data problems such as stigmatization or discrimination, as outlined by the National Institute of Standards and Technology Privacy Risk Assessment Methodology (NIST PRAM)<sup>18</sup>. As an example, imagine that an individual's sexual preferences were visible on Bumble, but the user did not openly share those preferences in offline life. If someone with malicious intent were to find the user's Bumble profile, they could choose to out them to their employer, family, friends, or others -- potentially at the cost of their job, home, or personal safety. There are documented instances of these situations happening on other, similar dating apps; for example: in 2016, a journalist outed gay Olympians by collecting personal information on the closeted athletes after their dating profiles on Tindr were screenshotted<sup>19</sup>. For reasons like this, we've identified the collection of sensitive personal information as a high privacy risk aspect of Bumble.

### ***Collection & Disclosure of Location Data***

As is typical with dating apps, Bumble also collects users' locations to show potential matches nearby. Bumble uses GPS (longitude and latitude) to pinpoint a user's location, and when disabled, collects information from both their router and ISP to pinpoint where they are in the world<sup>20</sup>. Users do not have the option to manually change their location unless they utilize Travel mode, a paid feature, or they physically go to a new location. Users also have to grant Bumble some level of location permissions or else the app is rendered unusable. On iOS, the least intrusive location permission is to allow location access while using the app.

Compounding this issue, a user has no control over the visibility of their location data as Bumble lists a user's specific location on their profile. Users can also see how far away another person is from them in miles. This is due to the fact that Bumble primarily uses a "proximity" system to help users find potential matches near them. As a result, a user's location is continuously broadcast to find nearby users or locations<sup>21</sup>. This can become troublesome when a user lives in a small city/town where they can be easily identified or found online. For example, in Figure 4, Sunrise is a city located in Florida, a state that lists all voter registration information (including

---

<sup>18</sup> National Institute of Standards and Technology (NIST), Brooks, S., Garcia, M., Lefkowitz, N., Lightman, S., & Nadeau, E. (2017, January). An Introduction to Privacy Engineering and Risk Management in Federal Systems (NISTIR 8062). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.IR.8062>

<sup>19</sup> Cobb, C., & Kohno, T.. (2017). How public is my private life? Privacy in online dating. 26th International World Wide Web Conference, WWW 2017 (pp. 1231–1240).

<sup>20</sup> Bumble - Privacy. (2021). Retrieved March 29, 2021, from Bumble website: <https://bumble.com/privacy>

<sup>21</sup> Farnden, J., Martini, B., & Choo, K.-K. (2015). Privacy Risks in Mobile Dating Apps. Retrieved from website: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2017/10/21180944/1505.02906.pdf>

address) publicly on the Internet. It would not be hard to find a user's address if you have access to their city, name, and other private information. This lack of privacy can result in serious consequences like stalking and harassment.

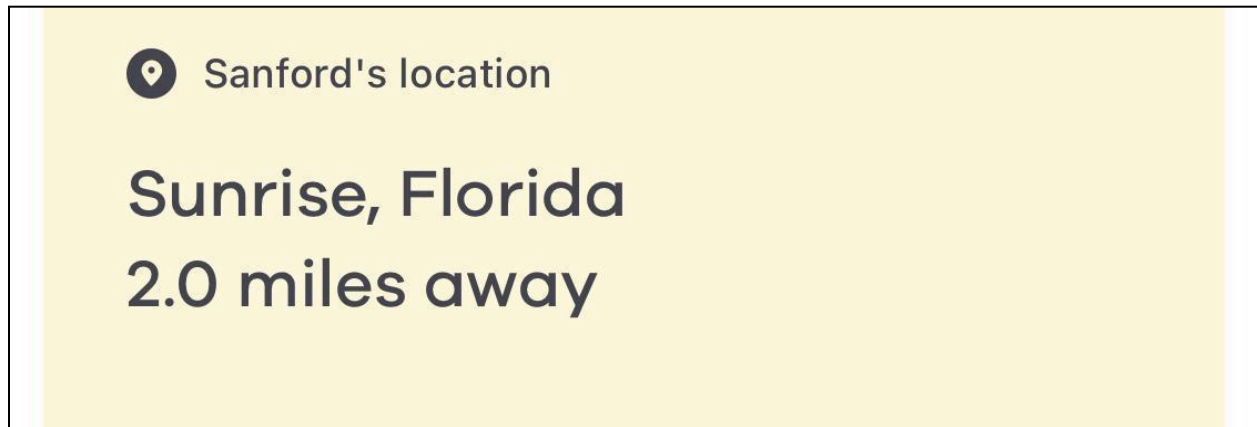


Figure 4: User Location Display on Profile

### Linked Accounts

Throughout the registration and account creation process, a user is prompted to connect their Bumble account to other social media accounts to either register and validate their account or to provide supplemental information like profile photos from Facebook, music taste from Spotify, or recent photos from Instagram. This practice runs the risk of cross-platform identification during the information processing process, as well as induced disclosure and increased accessibility to a user's personal data, which are two of Solove's privacy harms<sup>22</sup>.

According to Bumble's Privacy Policy, if a user registers or logs in to the app using a Facebook account, the user authorizes Bumble to access Facebook account information including a user's Facebook friends list, current location, and friends a user has in common with other Bumble users<sup>23</sup>. Data sharing occurs on the backend of the social media platforms, even if the extent of the data that is shared between the two platforms is not visible on the front-end of the Bumble app. Although linking Instagram and Spotify accounts also does not make the user's full linked account directly accessible to other users on Bumble (Figure 5), it is reasonable to assume that Bumble still gains access to much more data on the backend. Again, in the REST API exploit that ISE Labs uncovered in late 2020, linked account data was vulnerable to being accessed and dumped via a Python script; this included Facebook "interests" or pages that a user had liked if the user's account is connected to Facebook.<sup>24</sup>

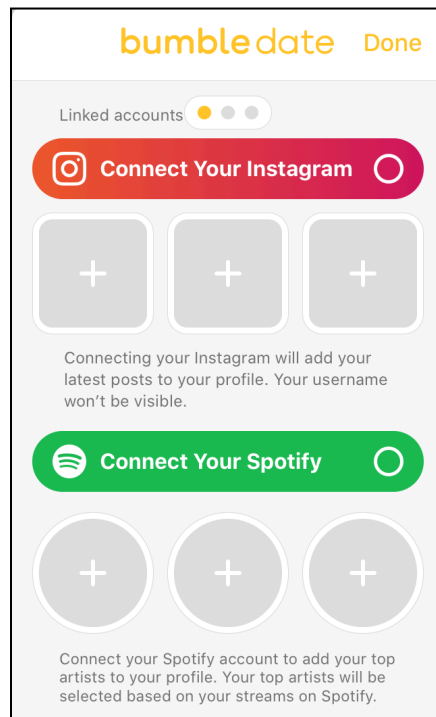
<sup>22</sup> Solove, D. J., (2006, January). *A Taxonomy of Privacy*. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, GWU Law School Public Law Research Paper No. 129, <https://ssrn.com/abstract=667622>

<sup>23</sup> <https://bumble.com/privacy>

<sup>24</sup> Sarda, S. (2020, November 24). Reverse Engineering Bumble's API - Independent Security Evaluators. Medium. <https://blog.securityevaluators.com/reverse-engineering-bumbles-api-a2a0d39b3a87>



Due to the large amount of data that is shared between Bumble and linked third party social media platforms on their backends -- with minimal explanation or notification to the user of this occurring, outside of reading the Privacy Policy -- we have identified this as another high privacy risk of the app.



**Figure 5: Linked Accounts Section of User Profile**

### **Screenshotting & Screen-recording Information on Bumble**

Bumble does not have screenshot alerts. In other words, users have no control over who takes screenshots of their profiles or private messages and shares their information with others or in the public. Bumble's Privacy Policy makes this clear that they will not be held responsible for any consequences caused by a user sharing their personal information:

*"Where you do upload and choose to tell us sensitive information about yourself, you are explicitly consenting to our processing of your information and making this public to other users. When you post information about yourself or use the messaging function, the amount of personal information you share is at your own risk."*<sup>25</sup>

<sup>25</sup> <https://bumble.com/privacy>

Personal information on a user's profile, conversations, and photos shared in private messages can contain sensitive personal information. Without good privacy-preserving features, such as providing user notification when personal information is captured by screenshots or screen recording, people on Bumble may misuse or share other's private information for malicious purposes and interests (e.g. stalking, posting it on other platforms without user consent). Not getting alerted by someone taking screenshots of your profile or private chat can be considered an "unanticipated disclosure" and might be a violation of the Right to be Informed listed in the GDPR, which states there is *"a need for transparency regarding the gathering and use of data in order to allow EU citizens to exercise their right to the protection of personal data."*<sup>26</sup>

### **Surveillance of User Messaging/Chat**

Bumble implemented a Private Detector in their in-app messaging feature. The Private Detector works by using artificial intelligence to automatically detect and blur a nude image shared within a message exchange. It will then alert users that they've been sent something potentially inappropriate; it is up to the users to decide whether to view or block the image. Users can also easily report the image to Bumble. Although this feature allows the company to filter unsolicited and inappropriate images, it doesn't censor text-based content. However, Bumble clarifies that it also can and will take measures to monitor users' messages. According to Bumble's guidelines outlined in their Privacy Policy, they *"use a combination of automated systems and a team of moderators to monitor and review accounts and messages for content that indicates breaches of these Guidelines and our [Terms and Conditions](#)."*<sup>27</sup> According to an anonymous interview<sup>28</sup> with a moderator working for a dating company, moderators are in charge of responding to user reports and any cases where a stock word triggers the system. They are responsible for taking a look at the case and report any suspicious behavior like "raping, zoophilia, etc" to their manager to get the police involved.

### **Users Creating False Identities for Catfishing**

Catfishing, which is when someone creates a fake identity to connect with someone online, is a common problem in dating apps. Catfishers may go by a fake name and upload pictures they found on the web. The greatest risk of a catfishing scheme is the potential for blackmail. A catfisher can collect many intimate details about the victim including where they live, photos of them, and what they've said in conversation, but the victim does not know the true identity of the catfisher. Solove defines blackmail as *the threat to disclose personal information*<sup>29</sup>. Catfishing is related to problems of *user authentication*. Recently, Bumble has tried to build

---

<sup>26</sup> <https://gdpr-info.eu/issues/right-to-be-informed/>

<sup>27</sup> <https://bumble.com/privacy>

<sup>28</sup> Falconer, E. (2018, December 28). Confessions Of A . . .Dating App Moderator. Refinery29.

<https://www.refinery29.com/en-gb/dating-app-moderator-job>

<sup>29</sup> Solove, D. J., (2006, January). *A Taxonomy of Privacy*. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, GWU Law School Public Law Research Paper No. 129, <https://ssrn.com/abstract=667622>

trust among users with their photo verification feature. Using photos, a person is checked for authenticity by a real person at Bumble.<sup>30</sup> In our risk assessment, we judged the potential of users expiring the risk of catfishers as a reasonable possibility. Even though Bumble has measures to promote the users to verify their identities, such as the blue check marks on profiles, these features are not required. Catfishers could easily masquerade as someone else. We rated the severity of the harm of interacting with a catfisher to be significant to severe because of the potential loss of self-determination and unanticipated revelation. This is why Bumble states in their Privacy Policy, *“When using Bumble, you should assume that anything you post or submit on the App may be publicly-viewable and accessible, both by Users of the App and non-Users of the App.”*<sup>31</sup>

One challenge in the design of dating apps is how to enable users to convince other users that they are not bots while not revealing private information.<sup>32</sup> For example, many users rely on seeing the name of their matches’ schools on their profiles; however, revealing where one went to school can make them more findable because of public directories.

### **Default Sharing Data with Third-Party Advertisers**

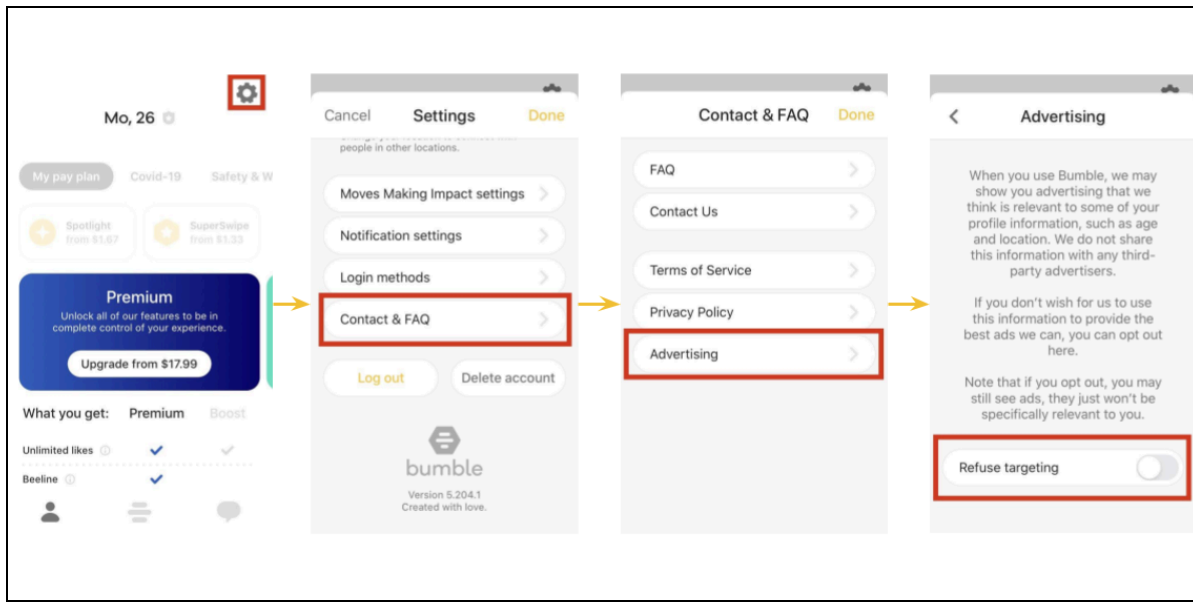
Bumble’s Privacy Policy states that the app may share user data with third parties. This is not surprising, as many mobile apps by-default share data with advertisers and data brokers. Bumble users are sharing data such as their device identifiers and demographic information. This becomes a risk of secondary use of information, in which third parties can sell a user’s relationship status to marketers. Furthermore, there is the aforementioned risk that if a user’s account is linked to another social media platform like Facebook, Bumble has data on their friends. It is not only a risk of surveillance for the user, but to people in their social network. People oftentimes share similar traits to people they are friends with. If Bumble has a user’s friends list, they have a more targeted audience to advertise to. Users do have the option to stop targeted advertising; however the app does not make it easy. Users must opt-out of targeted advertising by visiting the “Contact & FAQ” page in Settings to reverse the default through a four step interaction (Figure 6).

---

<sup>30</sup> <https://bumble.com/the-buzz/the-end-of-catfishing-introducing-photo-verification>

<sup>31</sup> <https://bumble.com/privacy>

<sup>32</sup> Cobb, C., & Kohno, T. (2017, April). How public is my private life? Privacy in online dating. In *Proceedings of the 26th International Conference on World Wide Web* (pp. 1231-1240).



**Figure 6: Process to Opt-Out of Targeted Ads**

### **Privacy Settings Exist Behind Paywall**

Currently, Bumble has a free base product that allows users to create profiles and match with each other. Bumble has also developed a Premium version of their app that offers users additional features.

For applications like Bumble that operate on a swipe right/left model, the decision to match ultimately lies in the hand of the user. There are, however, cases where a user accidentally swipes on a person that they were not intending to. Though the intention was not there, a match may still occur, which gives each party access to the other person's profile. On Bumble, a Premium user has the option to "Backtrack" on their swipe, which allows them to reconsider their latest swipe. This feature allows users to undo any mistakes and avoid any uncomfortable situations that may arise. There have been many stories where users, mainly women, have faced harassment, threats of violence, and stalking when men feel that their interest is not reciprocated. Therefore, limiting the Backtrack feature to only paying users puts regular users at risk when they accidentally swipe on someone they did not want to.

Another privacy feature that exists behind a paywall in Bumble is "Incognito Mode". This premium feature allows users to only be seen by people who they swiped right on. This ensures that profiles are only seen by people the user is interested in. This feature also helps put more power in the hands of the user and adds another layer of privacy for their personal information. Users who rely on the free version of the Bumble app also lack access to this feature.

## **Zombie Accounts**

When a user decides they no longer need or want to use Bumble, they cannot simply delete the app from their phone and expect their data to be deleted. As stated in Bumble's Privacy Policy *"simply removing, uninstalling or deleting the Bumble app from your phone will not erase your account entirely"*<sup>33</sup>. Rather, users must navigate to settings within Bumble and to actually delete their account. However, this process may not be clear to everyone, resulting in many "Zombie Accounts"<sup>34</sup>. For these accounts, Bumble still has access to all of the personal information that the user input into their account. Bumble does stop showing profiles of people who have not been active within 30 days to other users. However, 30 days is still a long period of time and exposes that user's information to others, though a user did not necessarily want to continue using the platform. If a user does end up deleting their account, backup copies may be saved for up to 28 days to enable restoration<sup>35</sup>.

Additionally, within Bumble's Privacy Policy, they mention the term "deactivate", which appears to be used interchangeably with the word delete/deletion. This assumption is being made because there is no documentation on Bumble's website as to what deactivation means or how to go about deactivating an account. There is, however, information on Bumble's site about how to delete their profile. The use of these two terms can be confusing to users, as deactivate typically means that users can still access their profile when they decide they want to, while deleting a profile typically means you lose access to all of the information.

## **Compliance with Laws, Regulations, Codes and Guidelines**

The following section examines how compliant Bumble is with current legal and regulatory policies in relation to the three greatest privacy risks we've identified within the Bumble app: Collection of Sensitive Personal Information, Linked Accounts, and Screenshotting Personal Information & Catfishing.

### **Collection & Dissemination of Sensitive Personal Information**

Bumble collects a significant amount of personal information about many of its users; it also stores and shares this information to other entities, as shown by our information flow diagram (page 7). Bumble's Privacy Policy includes sections that directly and indirectly mention its compliance with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

---

<sup>33</sup> <https://bumble.com/privacy>

<sup>34</sup> Nield, D. (2019, July 14). How To Clear Out Your Zombie Apps and Online Accounts. Retrieved March 29, 2021, from Wired website: <https://www.wired.com/story/delete-old-apps-accounts-online/>

<sup>35</sup> <https://bumble.com/privacy>

## GDPR

Section 11 of the Privacy Policy, “Your UK and EU Rights”, specifically addresses users’ rights under the GDPR. The policy briefly lists and defines the eight rights that apply to all users: right to be informed, right of access, right of rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights related to automated decision making including profiling.<sup>36</sup> The Privacy Policy also has a table that outlines the legal bases on which user data is collected and used, and why. Bumble defines the legal basis for using collected information to be “legitimate interests” in most cases. While these instances may be in the interest of the company, they may not always be the interest of the user. Regardless, they are clearly listed for compliance with the GDPR.

There is one statement in the “Data Storage” section of Bumble’s Privacy Policy that seems questionable in relation to the GDPR: the company states that Bumble stores user data on global servers, including in the United States and this means that by using the app, *“the storage of your personal data may not provide you with the same protections as you enjoy in your country of residence”* even if *“you live in a country with data protection laws”*.<sup>37</sup>

## CCPA

To comply with the CCPA’s “right to know” clause, Bumble has updated its Privacy Policy to include a section that clearly lists the personal information that the app collects about a user under Section 1, “Collection of Information”. Other sections of the Privacy Policy also comply with the user’s “right to delete” and “right to opt-out”, as defined by the CCPA. Section 10, “Your California Privacy Rights” also specifically addresses California law and users’ rights.<sup>38</sup>

## Collection & Dissemination of Location Information

Both GDPR and CCPA count location data as personal data/information, as a result the level of compliance listed above for collection and dissemination of personal information also applies to location information.

## FTC

In recent years, the FTC has also provided guidance for platforms utilizing geolocation. In its 2013 FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency, the FTC states that platforms should *“provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation”*.<sup>39</sup>

---

<sup>36</sup> <https://bumble.com/privacy>

<sup>37</sup> <https://bumble.com/privacy>

<sup>38</sup> <https://bumble.com/privacy>

<sup>39</sup> Federal Trade Commission. (2013). Mobile Privacy Disclosures: Building Trust Through Transparency. Retrieved from <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>

Currently, users do get a just-in-time disclosure of geolocation tracking, as first-time users are asked to enable location services as part of their onboarding process. However, Bumble falls flat on “affirmative express consent”<sup>40</sup> as users are not told how their information will be used by Bumble or third parties during the onboarding process. The Privacy Policy is not also clearly linked during the onboarding process; rather, Bumble links to their guidelines.

### **Linked Accounts**

Bumble does not communicate clearly with the user the amount of information they access from the user's linked account on other social media platforms (e.g. Facebook). The language in Bumble's Privacy Policy remains vague. In the example below, in the Facebook default setting, the app can access the user's name and profile picture, email address, birthday, photos, gender, page likes, current city and friend list, and app visibility. In this sense, without telling the user exactly what they collect about users' data from another linked account, Bumble might violate the privacy rights stated in the Art. 7 GDPR Condition and Consent, which states: “Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.”<sup>41</sup> Because this setting exists in a linked app (Facebook), Bumble does not explicitly get direct consent from the user to share this personal data with Bumble.

### **Screenshotting Personal Information & Catfishing**

While catfishing itself is not currently considered illegal in the United States, it can often lead to illegal activities. For example, if the catfisher screenshots and uses the victim's photos to impersonate them on another platform or they ask the victim to send money, it becomes a crime. California and Louisiana have passed legislation designed to address online impersonation.<sup>42</sup> In summary, there is evidence that existing online impersonation laws are broad enough to combat catfishing.<sup>43</sup> The risks of online impersonation include fraud, emotional duress, misappropriation for likeness, and invasion of privacy.

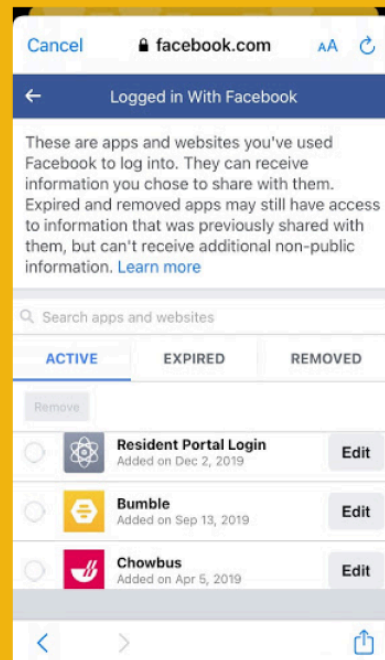
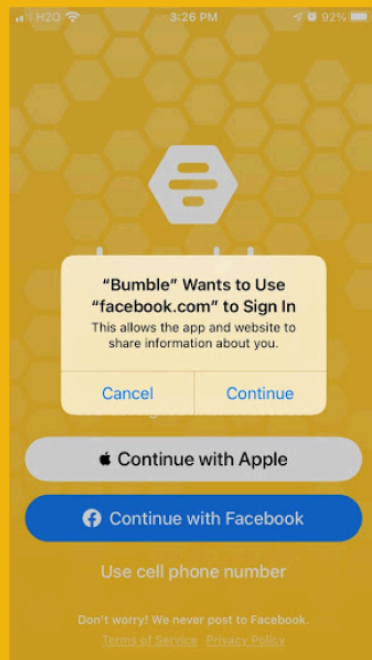
---

<sup>40</sup> [https://www.ftc.gov/system/files/documents/cases/1523134\\_lenovo\\_united\\_states\\_agreement\\_and\\_do.pdf](https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_agreement_and_do.pdf)

<sup>41</sup> <https://gdpr-info.eu/art-7-gdpr/>

<sup>42</sup> Reichart Smith, L., Smith, K. D., & Blazka, M. (2017). Follow Me, What's the Harm: Considerations of Catfishing and Utilizing Fake Online Personas on Social Media. *J. Legal Aspects Sport*, 27, 32.

<sup>43</sup> Derzakarian, A. (2017). The dark side of social media romance: Civil recourse for catfish victims. *Loy. LAL Rev.*, 50, 741.



Linking Facebook with a Bumble account shares information from Facebook with Bumble by default, which is only visible and controllable in Facebook's settings, not Bumble's.

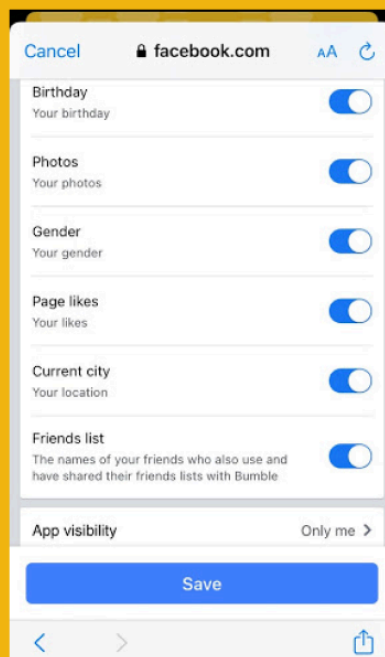
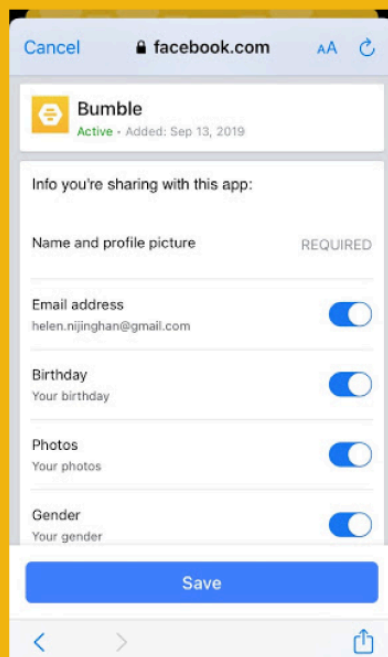


Figure 7: Shared Data Among Bumble and Linked Third Party Social Media



# Privacy Risk Mitigations & Recommendations

## Mitigation Measures

For each identified privacy risk on Bumble, we have outlined potential mitigation measures in order to reduce the impact of that risk. Each mitigation measure has been classified as either a technological, procedural, or organizational measure, where we have defined a **technological mitigation** as a measure that is a code-related change that would be implemented by software engineers, a **procedural mitigation** as a measure that is a change to the app's user flow or the process in which users interact with Bumble, and **organizational mitigation** as a measure that is a change to how Bumble, as a company, operates in terms of policies, values, or structure. In some cases, a mitigation measure may fall into multiple categories.

### Risk: Collection & Disclosure of Sensitive Profile Information

**Mitigation 1:** Minimize the amount of personal data collected (Technological/Procedural)  
Minimizing the amount of and type of data collected about Bumble users would help mitigate many of the identified privacy risks on Bumble because, as Jaap-Henk Hoepman states in *Privacy Design Strategies (The Little Blue Book)*, “nothing can go wrong with data you do not collect”<sup>44</sup>. For example, instead of collecting the user's birthday when only their age is needed for verification purposes, Bumble could consider simply asking the user to input their age in years or Bumble could use a more complex, authentication-based credential privacy enhancing technology like IBM's Idemix<sup>45</sup> and Microsoft's U-Prove<sup>46</sup>, which can securely and cryptographically verify specific attributes of a user's identity without revealing additional information about the user.

**Mitigation 2:** Allow increased user control over Bumble badge visibility (Technological)

To help further mitigate the risks associated with personal information collection and dissemination of user profile data on Bumble, the app could also allow users more fine-grained control over which tags they would like to display to which users. For example, users could choose to reveal their religious or political affiliation with tags only after a user had exchanged messages with a person and decided that they are trustworthy enough to view that information; to all other unmatched users, this information would not be visible on their profile.

---

<sup>44</sup> Hoepman, J. (2018). *Privacy Design Strategies (The Little Blue Book)*. Retrieved April 10, 2021 from <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>

<sup>45</sup> IBM Research. (n.d.). MSP Implementation with Identity Mixer — hyperledger-fabricdocs master documentation. Hyperledger Fabric. Retrieved April 10, 2021, from <https://hyperledger-fabric.readthedocs.io/en/release-1.3/idemix.html#what-is-idemix>

<sup>46</sup> Microsoft. (2021, April 5). U-Prove. Microsoft Research. <https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A%2F%2Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove>

**Mitigation 3:** Alter Bumble’s matching algorithm to deemphasize completeness of profiles as a factor in matching (Technological)

Currently Bumble’s algorithm prioritizes more complete profiles<sup>47</sup>. Bumble could update its algorithm to be more inclusive to users who choose not to complete their profiles with detailed, sensitive information, if they are concerned about sharing sensitive personal information publicly on the app. For example, Bumble could show all users as potential matches equally, regardless of profile completion, or use data that is not publicly visible to other users to factor into match frequency, such as implementing Mitigation 1 in conjunction with this mitigation strategy.

### ***Risk: Collection & Disclosure of Location Data***

**Mitigation 1:** Do not collect users’ geographical information (Technological, Procedural)

Currently Bumble is rendered nearly useless if a user does not give Bumble access to their location<sup>48</sup>. While location is an important part of dating services, Bumble can consider alternative methods like allowing users to input their own location, as is the case with other dating apps like Hinge.

**Mitigation 2:** Allow users to hide their specific location or adjust their location manually (Technological)

If Bumble wants to continue tracking a user's geo-location, then they should provide users with the option to hide their location or adjust their location. Competitive products like Hinge give users the ability to manually input their location and allows them to change locations often. Bumble, on the other hand, uses geolocation to display where a user is. Some users may not feel comfortable disclosing their exact location, so allowing them to input the location that is displayed to others will help give them more control over the information they are sharing. Bumble can also give users the ability to hide their location if they do not feel comfortable sharing this information. If this policy is enacted, Bumble can employ several tactics to ensure that users are not misusing the location field. One such tactic could be to send notifications to users that the location they input manually is not the same as their actual location (checked via geolocation).

---

<sup>47</sup> Bumble - 6 Ways to Get More Matches on Bumble. (2021). Retrieved April 10, 2021, from Bumble Buzz website: <https://bumble.com/the-buzz/how-to-get-more-matches>

<sup>48</sup> <https://bumble.com/en/help/can-i-use-bumble-without-location-permissions>

### ***Risk: Screenshotting & Screen-recording***

**Mitigation 1:** Notify users when another user screenshots/screen records their profile or chat messages (Technological, Procedural)

Social media apps like Snapchat and Instagram have screenshot/screen-record notification alerts to notify the user when someone else takes a screenshot of the app. Although having an alert cannot prevent people from taking screenshots and sharing them, it could deter them. It could also encourage more dialogue between users about data sharing; a notification that says “[username] took a screenshot of your photo” can open up a conversation about what they intend to do with that snap, or allow a user to just block someone who consistently engages in this behavior.

**Mitigation 2:** Allow an easy way to filter and/or block subsequent unwanted interactions with users who screenshot or screen-record (Technological, Procedural)

To do this, the Bumble app may design an algorithm that flags the user who has been continuously screenshotting and screen recording other user profiles, private chat, and video chat and use this mitigation method in combination with Mitigation 1 and/or 3.

**Mitigation 3:** Institute strike policy for screenshotting for serial-screenshotters (Technological, Procedural)

To deter users who frequently screenshot other people’s profiles, Bumble can consider enacting a strike policy for screenshotting. With such a policy, each user will be allowed a certain number of strikes before their profile is banned or removed for frequent screenshotting.

### ***Risk: Users Creating False Identities for Catfishing***

**Mitigation 1:** Require users to verify their identity through (1) photo identification (2) matching public records (Technological, Procedural)

To mitigate the risk of catfishers creating false identities on the platform, Bumble could enhance their user verification process. For instance, a good starting point would be to make the current photo verification feature in which users upload a selfie to have it checked by Bumble personnel *required* instead of recommended. This option would be easy to implement in the short term. For a more thorough background check, Bumble could also follow the tactics that some pharmacies distributing COVID-19 vaccinations are using for user verification. CVS gives users a short quiz about their address, vehicle records, and voting records based on public documents. While photo verification is useful to nudge users to be truthful about their appearance, this would nudge them to be truthful about their names and birthdates.

### ***Risk: Surveillance of User Messaging/Chat***

**Mitigation 1:** Clearly state how the chat moderation process is conducted in the Privacy Policy (Organizational)

To better communicate what the company does with users' private chat data, the company can be more clear on explaining how their algorithms and real person moderators monitor the user's private chat and video calling experience. Therefore, the user can better understand when they should report and what is appropriate/inappropriate to share on the platform.

**Mitigation 2:** Provide a link to the relevant Privacy Policy section in the private chat to provide the more user with easy access to more information (Procedural)

To better communicate with privacy policy related with the private chat, Bumble could provide quick on-boarding screens for their privacy policy related with private chat when the user first uses the chat function. These on-boarding screens for the chat can use animation and clear language to explain what and how data has been collected or monitored and for what purpose.

**Mitigation 3:** Provide system notification to users when sensitive words/money transactions/abuse are mentioned in chat (Technological)

To do this, Bumble can come up with a list of sensitive keywords, whenever money, harassment, or other sensitive vocabulary is mentioned, the system sends a system message to the user and reminds them about the community guidelines.

### ***Risks: Linked Accounts & Default Sharing Data with Third-Party Advertisers***

**Mitigation 1:** Increase transparency of third party advertising and accessibility of opt-out feature (Technological, Procedural)

Make it easier for users to opt-out of third party advertising. For instance, when they are onboarding the app, the app could display a screen with the question of whether they want to opt-in to third party advertising.

**Mitigation 2:** Inform users in the app if their friends list will be or already has been shared as a result of linking accounts (Technological, Procedural)

Users should not have to read the Privacy Policy or access their settings in a linked social media account to receive notice of what data is being shared between accounts, especially if the data involves unknowing users who are not consenting to Bumble's Terms & Conditions or acknowledging their Privacy Policy. Before a social media account is linked, a Bumble user could receive a just-in-time notification of the information that will be shared with third parties if the

user proceeds with the linking. A section in the user's settings should also exist to track and list the data that any third parties are receiving.

### ***Risk: Zombie Accounts***

**Mitigation 1:** Send users mobile notifications reminding them to delete their profile if they have not actively used Bumble in the past 30 days (Technological, Procedural)

For those users that leave Bumble on their mobile phone but do not use it, Bumble still has access to their profile information. As a result, after 30 days of inactivity Bumble should remind users to either return to using the app or recommend them to delete their account.

**Mitigation 2:** Remind users who only deleted the Bumble app that their Bumble account remains undeleted (Procedural)

As is noted in Bumble's Privacy Policy, deleting the Bumble app does not delete a user's profile. For those users that have deleted the app on their device but did not delete their profile, notify them via email that their account is still active and provide instructions within that email on how to delete the account.

**Mitigation 3:** Clarify or remove misleading and unclear information in the Privacy Policy about deactivating accounts (Organizational)

Currently, the Privacy Policy mentions that users can deactivate their account, however there are no instructions on how to deactivate an account or what deactivating means. There are instructions on how to delete accounts<sup>49</sup>; however, if deactivation is something different there should be information about it. If Bumble is using deactivate and delete interchangeably, then one word should be picked and used consistently.

### ***Risk: Privacy Settings Exist Behind Paywall***

**Mitigation 1:** Provide more privacy features by default and reject monetization of privacy measures (Technological, Organizational)

Current paid features like Backtrack and Incognito Mode that specifically impacts a user's ability to control who sees their profile should be provided in the free version of Bumble, rather than monetized behind a paywall. This mitigation strategy is based on the concepts of privacy by design and privacy by default.

---

<sup>49</sup> <https://bumble.com/en/help/how-do-i-delete-my-profile>

## Recommendations

To prioritize the mitigation measures that we recommend Bumble implement, our team members individually ranked all 18 mitigation measures based on (1) **feasibility** in terms of resources (time and money) required, (2) **impact on user experience** in terms of how it will enhance the utility, usability, and enjoyment of engaging with the app, (3) **urgency** (legal and financial consequences of not implementing the measure). These individual rankings were then tallied to produce a final prioritization order, listed below (Figure 8).

|                |                                                                                                                                                              | Points | Average Rank |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------|
| 1.             | Allow increased user control over Bumble badge visibility (Technological)                                                                                    | 55     | 5.25         |
| 2.             | Provide more privacy features by default and reject monetization of privacy measures (Technological, Organizational)                                         | 53     | 5.75         |
| 3.             | Inform users in the app if their friends list will be or already has been shared as a result of linking accounts (Technological, Procedural)                 | 49     | 6.75         |
| 4.             | Allow users to hide their specific location or adjust their location manually (Technological)                                                                | 47     | 7.25         |
| 5.             | Send users mobile notifications reminding them to delete their profile if they have not actively used Bumble in the past 30 days (Technological, Procedural) | 45     | 7.75         |
| 6.             | Strike policy for screenshotting for serial-screenshoters (Technological, Procedural)                                                                        | 43     | 8.25         |
| 7.             | Increase transparency of third party advertising and accessibility of opt-out feature (Technological, Procedural)                                            | 42     | 8.5          |
| 8.             | Minimize the amount of personal data collected (Technological/Procedural)                                                                                    | 39     | 9.25         |
| 9.             | Allow an easy way to filter and/or block subsequent unwanted interactions with users who screenshot or screen-record (Technological, Procedural)             | 39     | 9.25         |
| 10.            | Notify users when another user screenshots/screen records their profile or chat messages (Technological, Procedural)                                         | 37     | 9.75         |
| 11.            | Do not collect users' geographical information (Technological, Procedural)                                                                                   | 35     | 10.25        |
| 12.            | Remind users who only deleted the Bumble app that their Bumble account remains undeleted (Procedural)                                                        | 35     | 10.25        |
| 13.            | Require users to verify their identity through (1) photo identification (2) matching public records (Technological, Procedural)                              | 33     | 10.75        |
| 14.            | Provide system notification to users when sensitive words/money transactions/abuse are mentioned in chat (Technological)                                     | 33     | 10.75        |
| 15.            | Provide a link to the relevant Privacy Policy section in the private chat to provide the more user with easy access to more information (Procedural)         | 31     | 11.25        |
| 16.            | Alter Bumble's matching algorithm to deemphasize completeness of profiles as a factor in matching (Technological)                                            | 24     | 13           |
| 17.            | Clarify or remove misleading and unclear information in the Privacy Policy about deactivating accounts (Organizational)                                      | 24     | 13           |
| 18.            | Clearly state how the chat moderation process is conducted in the Privacy Policy (Organizational)                                                            | 20     | 14           |
| Total Votes: 4 |                                                                                                                                                              |        |              |

Figure 8: Team Rankings for Mitigation Strategies

Our top six recommendations, which we believe that Bumble should prioritize first, were as follows:

1. Allow increased user control over Bumble badge visibility (Technological)<sup>50</sup>
2. Provide more privacy features by default and reject monetization of privacy measures (Technological, Organizational)
3. Inform users in the app if their friends lists will be or already has been shared as a result of linking accounts (Technological, Procedural)
4. Allow users to hide their specific location or adjust their location manually (Technological)
5. Send users mobile notifications to delete their profile if they have not actively used Bumble in the past 30 days. (Technological, Procedural)
6. Strike policy for screenshotting for serial-screenshotters (Technological, Procedural)

### ***Recommendation 1: Control over badge visibility***

Increasing user control over Bumble badge visibility is a low-hanging fruit because it is a relatively straight-forward software fix. The company may consider updating current users about the new flexible badge requirements with a simple pop-up modal and communicating the new badge flexibility feature in the onboarding process for new users. This recommendation enhances the usability of the product by increasing user control and freedom for what data to display about themselves on the interface.

### ***Recommendation 2: Privacy features by default***

When it comes to providing privacy features by default, Bumble already has two paid privacy features that exist so there should not be much technical development that goes in to offer those services to everyone. They will have to amend their offerings for Premium members to replace the two features that will now become available to all users. This mitigation measure requires Bumble, as an organization, to embrace an even stronger privacy-centered culture and it may potentially result in a loss of revenue with a decrease in users who will opt for the paid Bumble membership. Despite these obstacles, we believe that demonetizing privacy-centered design features will have a net positive impact by increasing user trust in the company and its application -- which can be a competitive differentiator and a revenue generator on its own.

### ***Recommendation 3: Inform of friend's list linking***

Informing users that their friends list will be shared if they link accounts can take many forms, some of which are relatively simple fixes. These fixes include a pop-up before authorizing linking. This will require Bumble to create notifications and/or pop-ups, both of which should

---

<sup>50</sup> See Figures 2-3 on page 10 for a snapshot of the data that goes into a user badge on Bumble.

not require too much effort. However, this will help users understand what the consequences are of linking various accounts. The impact of this recommendation is that it impacts not only the primary user of the app, but also protects the secondary users. Furthermore, this recommendation was ranked high because of the potential legal consequences of collecting user data without consent.<sup>51</sup>

#### ***Recommendation 4: Location control***

Allowing users to hide their location or change their location manually will require software work; however, we ranked it highly because of the risks of location disclosure. Users should be afforded the opportunity to hide information that makes it easier to identify them in real life. This is especially important because of how the geographic data can be used in conjunction with other sensitive information people share on the platform, such as their company or school. Ultimately, this technological change can help prevent instances of stalking and harassment.

#### ***Recommendation 5: Account deletion reminders***

Sending users a mobile notification after inactivity will require minimal work for Bumble while the impact for users will be great. Reminding users that their profile is still active and having them take action empowers them to have more control over their personal information. In this case, providing feedback about system *inactivity* is just as important as providing feedback about system activity.

#### ***Recommendation 6: Screenshotting Policy***

Developing a strike system for screenshotting will help deter users from capturing other users' personal information. This helps ensure that information on Bumble stays within Bumble and that a user's personal information is not transmitted without consent. This will require work on Bumble's part to develop a policy and a strike system, however, it's worthwhile in the long run if it helps users feel secure while using Bumble.

---

<sup>51</sup> Facebook was heavily criticized for allowing Cambridge Analytica to collect the data of users' friends without their consent.



## Solution Proposal

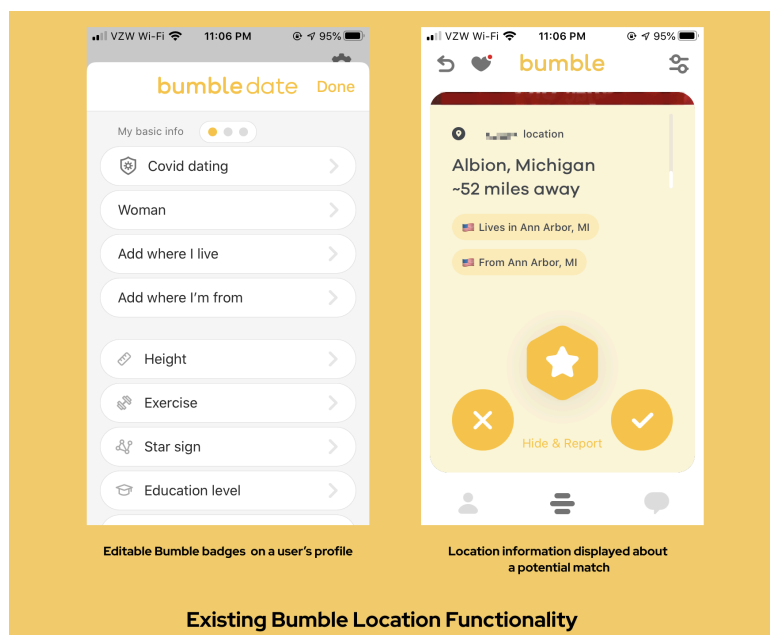
For our designs we decided to develop solutions for mitigation measures 4 and 6. We thought these measures would allow the most robust interactions and would also have a significant impact on Bumble users if implemented.

### ***Design Proposal 1: Location Control***

#### ***Rationale***

Bumble's decision to require the collection and display of a user's current location is a privacy invasive feature on a dating application. Many mobile apps, including competitor dating apps, have other less invasive tactics which could be implemented on Bumble. There are a variety of ways to make the collection and display of a user's location information less precise, and therefore less risky to the user's safety and privacy.

Currently, when a user registers for a Bumble account, they are presented with a popup modal on their phone asking them to grant the application access to use the phone's location. Although a user can later set and edit the Bumble badges "where I live" and "where I'm from" to display on their profile to prospective matches, a user is not able to edit or hide their phone's detected geolocation location and the distance of that location from other users viewing their profile. This design not only collects unnecessarily sensitive information, but it is also potentially dangerous, as it could inform bad actors of an individual's physical location.



**Figure 9: Bumble's current profile settings and location display UI**

## Prototype

Using the data-oriented privacy by design principle of minimization<sup>52</sup>, we propose an alternative onboarding process that allows the user more choice in location settings and provides better privacy notice about the visibility of their personal information. As shown in Figure 10: rather than allowing Bumble to access a user's phone location constantly or while the app is in use, during their onboarding process, users should be able to input an approximate location and select whether this information is visible to other Bumpers. Bumble could also allow users to specify the location they are looking for matches, and within what radius, to allow them to see matches in a more specific area than the location that they're willing to share they are located.

For example, imagine Alice is located in Ann Arbor, MI but sets her location as being within 50 miles of the Detroit Metro Area in order to maintain her privacy and not reveal a more precise location to anyone on Bumble. However, Alice is really more interested in finding matches right in downtown Detroit because she is planning to relocate for her new job. With the proposed design solution, Alice can indicate that she's looking for matches within a 10 mile radius of any city or zip code, including the metro Detroit area. This information will not be displayed publicly to other Bumpers, and she can still receive accurate matches while minimizing the amount of personal information she discloses about her own location.

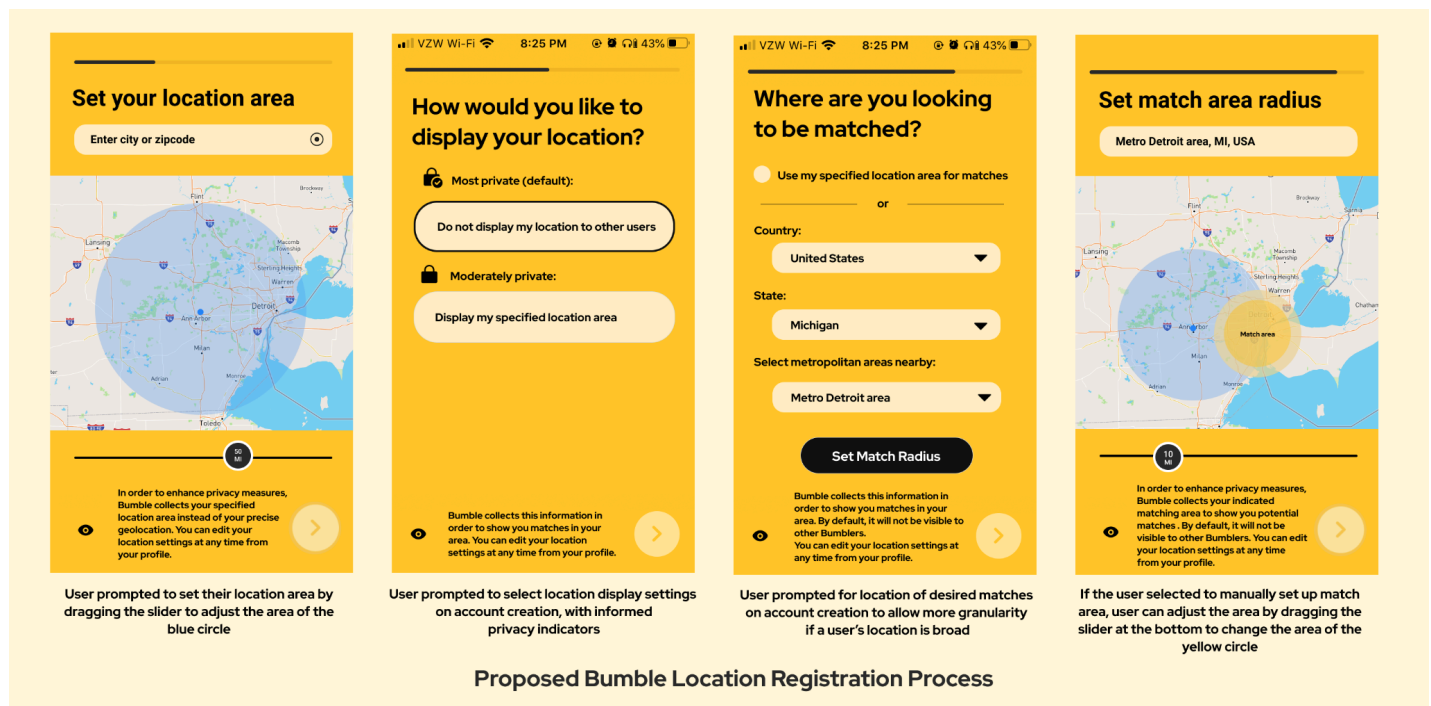


Figure 10: Proposed changes to Bumble's location settings during onboarding

<sup>52</sup> Hoepman, J. (2018). Privacy Design Strategies (The Little Blue Book). Retrieved April 10, 2021 from <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>

Both the user's location area and the desired match location area can be updated by the user at any time by editing their profile. Rather than non-optionally displaying a user's location and their miles away from a match, the profile will display a message if a user has set their profile information to private or show the approximate location area specified by the user, but only if they have opted to display the information using the toggle button at the bottom of the "Set my location area" screen.

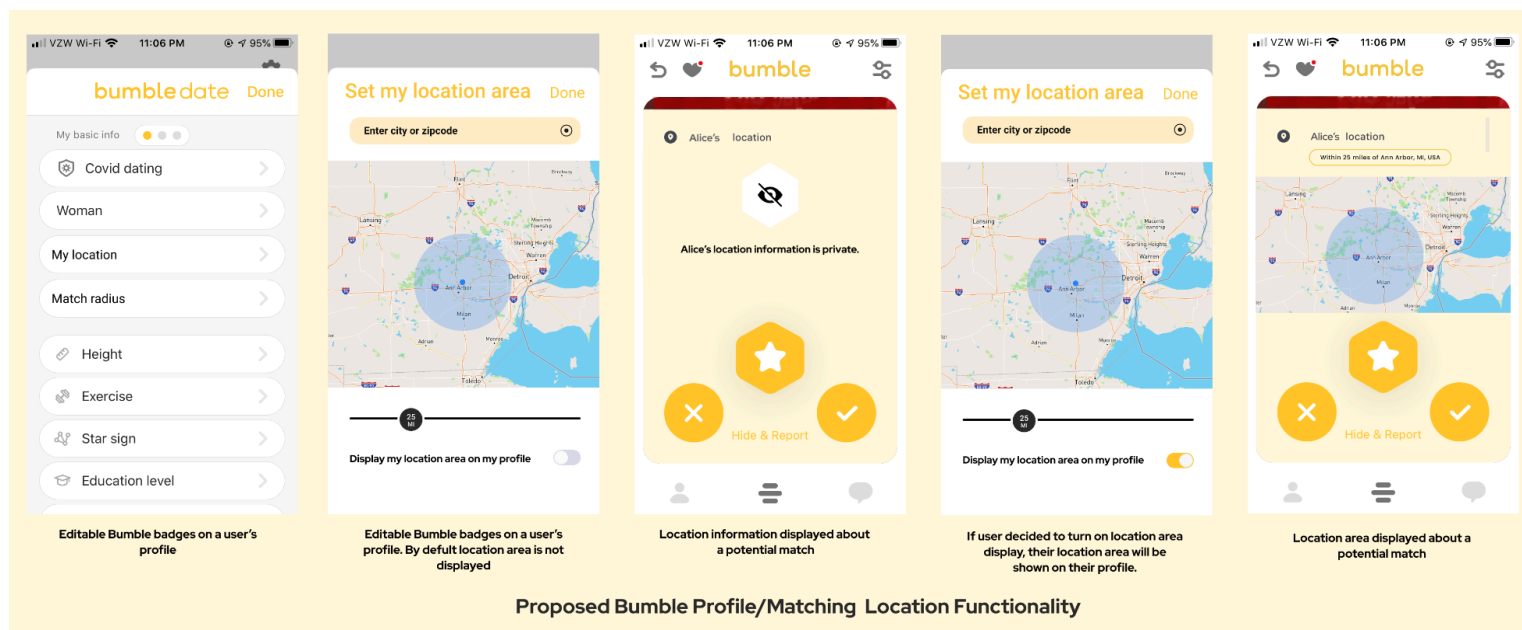


Figure 11: Proposed changes to Bumble's profile and location display UI

### Limitations

This proposed design is intended to minimize the amount of sensitive location information that an individual discloses to Bumble *and* displays to other Bumlbers by giving users more flexibility to abstract and to hide their location details. Overall, these changes are designed to increase a user's privacy and protect them from dangerous situations in which their physical location is non-optionally disclosed to strangers online. However, this change could also potentially introduce additional risk factors, such as an increased rate of catfishing due to all users being able to search for matches in a location other than their own. Currently, Travel Mode allows users to do this, but it is a paid Premium feature, so not all Bumble accounts have access to these capabilities or the ability to abuse them. To address the risk of increased catfishing, we suggest two potential mitigation methods:

1. On a potential match's profile, under the user's location (or, if their location is hidden, where their location *would* be displayed) provide a brief notice to the user viewing the profile that the location a user is searching for matching in is not nearby (within reason

-- for example within 100 miles) the area that a user has set as their location. This would not explicitly disclose the user's exact location, but it would make users aware of the situation if it is a cause for concern.

2. In order for a user to set a desired match area, require them to either use the same city or zip code as they input for their own location area. Only allow the user to adjust the radius of the match area from that location, rather than the location itself. Alternatively, require the user to approve location access on their device for a one-time verification that their location is within a reasonable distance of their match area; do not collect or store location data after that verification.

## ***Design Proposal 2: Screencapturing Policy***

### ***Rationale***

Currently there are no restrictions on how many screenshots a user can make on Bumble. Users have unfettered access to other people's profiles which includes personal information and pictures. Users cannot tell if their information has been screenshotted nor can they control who sees their profiles. This can be especially troubling in private chats, where users often disclose more personal information.

To our knowledge, Bumble is not the only company that allows users to screenshot information within their app. We could not find any other dating app that penalizes users for screenshotting or ones that place any limits/restrictions on screenshotting.

Within the realm of screenshotting disclosures, one of the most well known platforms that alerts users of captured information is Snapchat. Snapchat will notify a user when another user has taken a screenshot of their photo, video, chat conversation, or Snapchat story.<sup>53</sup>

### ***Prototype***

To deter people from repeatedly capturing permanent photos and videos of other users' profiles, we are proposing Bumble develop a Screencapturing Policy. The crux of this new policy would be a tiered strike system that keeps track of when users screenshot other people's information. With each screenshot (strike) that a user makes they would be given a specific consequence that escalates in severity with each consequent transgression. If users screenshot their *own* profile, they do not receive a strike.

---

<sup>53</sup> John, S. (2019, October 28). "Does Snapchat notify users when you take screenshots?": Here's what you need to know. Retrieved April 18, 2021, from Business Insider website: <https://www.businessinsider.com/does-snapchat-notify-screenshots>

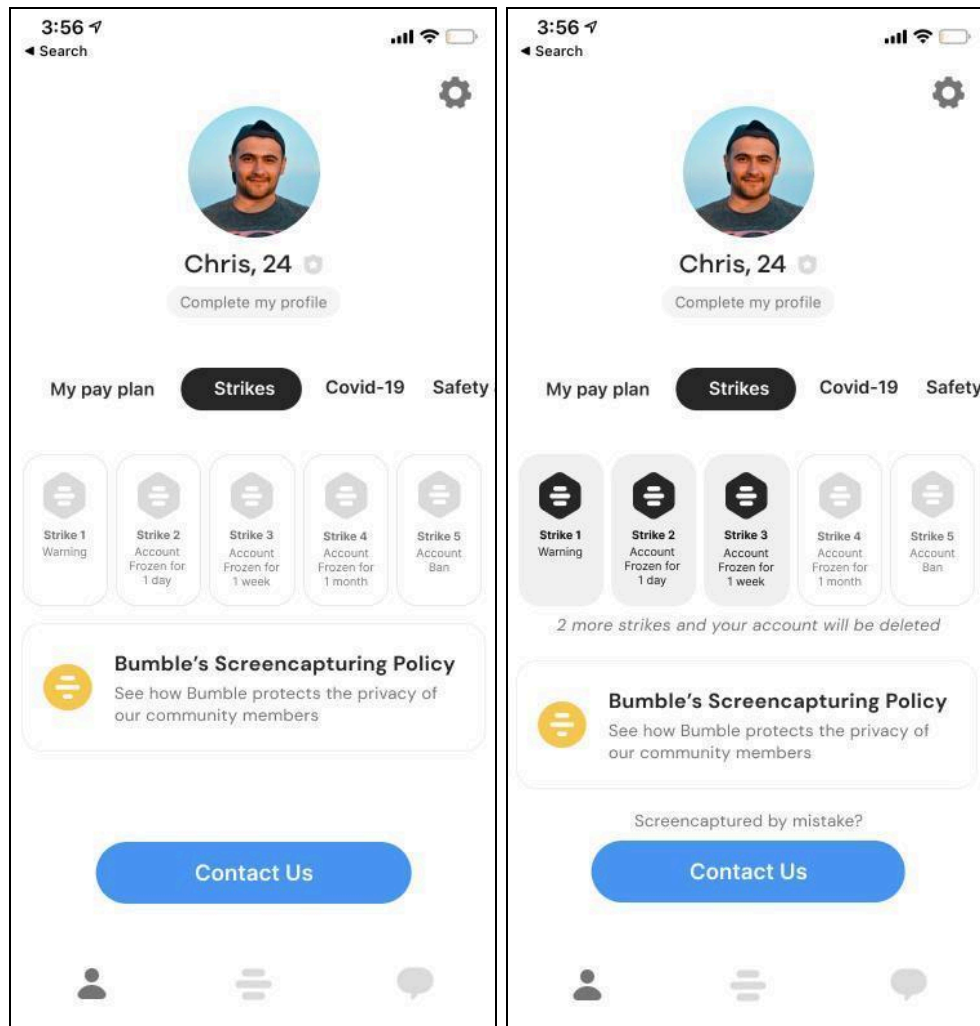
Our tiered strike system is as follows:

- **First strike:** a pop-up that informs the user of the strike policy and conditions.
- **Second strike:** the perpetrator's account is frozen for one day.
- **Third strikes:** the perpetrator's account is frozen for one week.
- **Fourth strike:** the perpetrator's account is frozen for 1 month.
- **Fifth strike:** the perpetrator is banned from Bumble.

The policy can also provide additional information on what constitutes screencapturing and the importance of the policy.

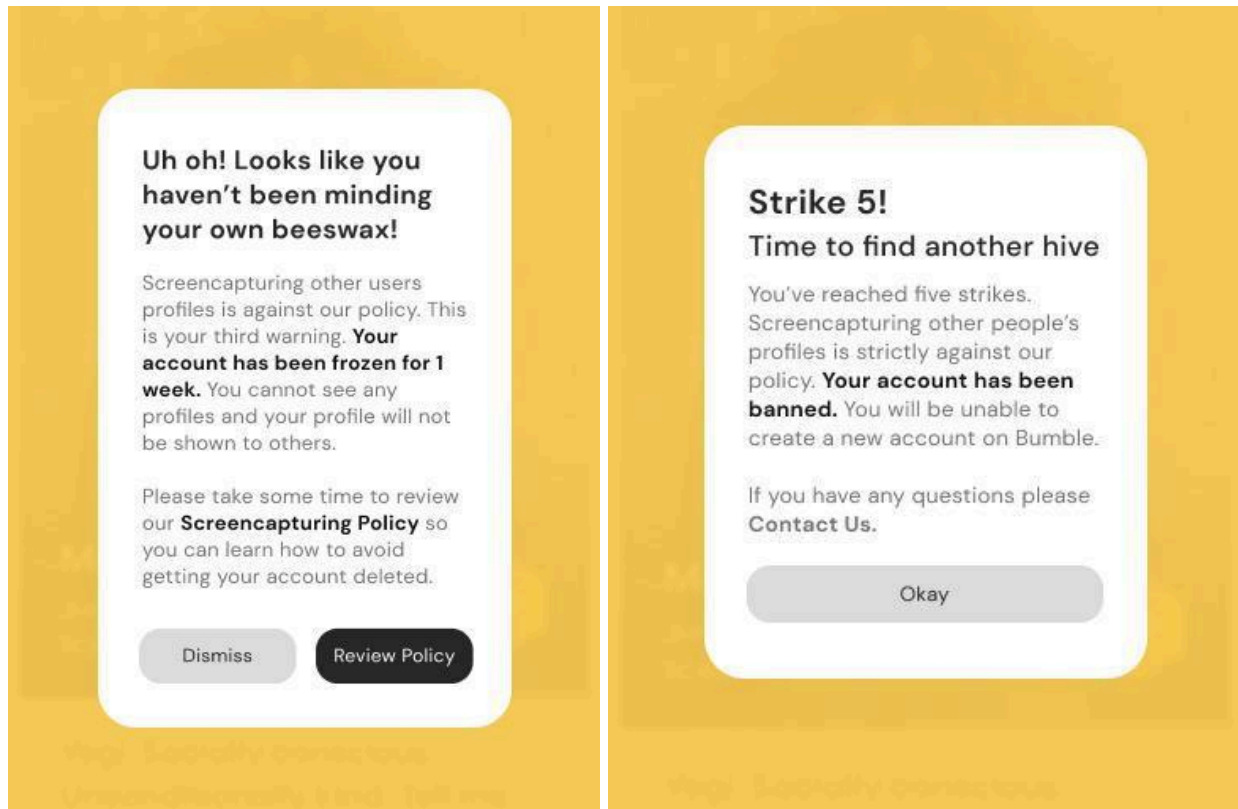
To implement our new strike system, we decided that it must contain two important components: a way for users to view the number of strikes they have left and a notification system to alert perpetrators that they have received a strike and to inform them of the consequence(s). To inform users about how many strikes they have accumulated, we developed a new page called "Strikes". This new page is located within the user's account settings (See Figure 12). The strike system takes the form of five "hives," in line with Bumble's bee theme. For each consecutive strike on the user's account, another gray hive turns black. Each hive also has a description alerting users of the consequence if they reach that strike. This page also contains a link to Bumble's Screencapturing Policy and a Contact Us button to provide users with the opportunity to contact team members with petitions for accidental screencaptures or general questions (See Figure 12)

In the future, Bumble could expand upon the strike system by including warnings about all inappropriate behavior on this page.



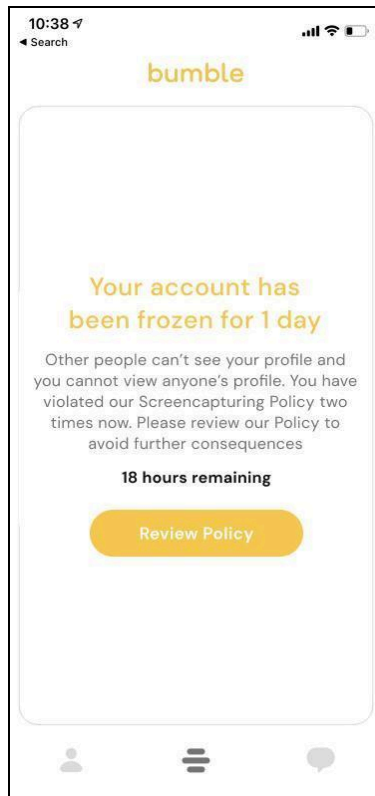
**Figure 12: The first screen shows what the strike page looks like when a user has no strikes. The second screen shows what the screen would look like when a user has already received 3 strikes.**

To alert users when they receive a strike, we developed a notification system. The primary notification would be a pop-up modal. The goal of the pop-up modal is to make the screenshotting behavior more salient to the user. The pop-up modal lets the user know they have gotten a strike and notifies them of the consequence associated with that strike. The user is also presented with two call-to-actions—they can choose to either dismiss the pop-up or review strike system policy. We intentionally made the Review Privacy Policy button more noticeable in order to nudge the user to review the policy. Throughout the new feature, we intentionally maintained a playful yet direct, forceful tone. For example, the language in the pop-up continues with the bee theme, “Uh oh! Looks like you haven’t minding your own beeswax!” (See Figure 13)



**Figure 13: Sample notifications. The pop-up message on the left is for a user who has received their third strike. The message on the right is letting a user know they have reached five strikes and have been banned from Bumble.**

Since three of our strikes involve a freeze to a user's account, we have also developed an additional notification to let users know that their account has been frozen. This notification will appear on the page a user goes to find matches. Users will be told that their account has been frozen, why it was frozen, and will tell them for how much longer their account will be frozen. It will also link back to the Screencapturing policy.



**Figure 14:** This screen shows what a frozen profile will look like. This message will appear when a user attempts to look for matches.

### **Limitations**

We recognize that users may accidentally take a screenshot, which is why we gave users a total of five strikes before they are permanently banned. For these users, we also included a Contact Us button so they can petition to remove a strike from their record. We believe that Bumble will be able to determine who is contacting them for mistakes versus who is contacting them to try to abuse the system by how frequently a user utilizes the Contact Us button.

Ultimately, we decided to only notify the perpetrator and not the victim of screencapturing behavior because we believed it could cause the victim too much emotional distress. Receiving notifications that someone has screenshotted your personal information may make the app less enjoyable for users who did nothing wrong. This type of disclosure may also cause them to leave the app entirely. Additionally, we discussed whether we should add a button to allow a perpetrator to delete the screencapture from their library. However, we believe that was outside of the capabilities of the Bumble app and could only be done through the phone's operating system.



We acknowledge that this feature will not stop all instances of screencapturing on the platform. However, the goal is that it significantly dissuades users from screencapturing. We also realize that developing a new screencapturing policy, such as the one we have designed, may be seen as too restrictive or punitive. However, we do not think there are any legitimate reasons why a user needs to have the option to save information about other users. For situations that involve harassment, violence, or criminal activities, the user can work with Bumble to capture any relevant information without incurring strikes. This one exception can be built into the policy.

## Conclusion

Bumble is a dating application that prides itself on putting the safety and security of women first. These values are reflected in some of Bumble's features. The most notable design feature is Bumble's matching policy that, in heterosexual matches, requires women to make the first move and initiate the conversation. Additionally, Bumble has implemented features such as profile verification, using machine learning to detect inappropriate photos, and offering paid features that enhance privacy.

While privacy by design is incorporated into some aspects of Bumble, the increasing popularity of dating applications and the increasing amount of online harassment suggest that Bumble would benefit from reviewing its privacy harms and addressing the risk of these harms by introducing additional mitigation measures and design solutions.

In this Privacy Impact Assessment, we have done the following:

- Presented a threshold analysis to justify the use of conducting a PIA on Bumble
- Identified the main stakeholders involved in the Bumble app (Bumble Users, Bumble Inc., and Third-Party Providers) and outlined their vested interest in privacy
- Identified the flow of information through the Bumble app, including points where user information is collected, stored, protected, and shared
- Conducted a privacy risk analysis to identify privacy harms on Bumble, classify their level of risk, and address the extent to which Bumble is compliant with modern privacy legislation
- Identified mitigation measures for each privacy risk and prioritized these mitigations in the form of recommended actions
- Proposed mockups of design solutions to two of the identified privacy risks

Ultimately, we hope that Bumble will innovatively address the privacy concerns associated with the dating application to improve trust and protect the safety of its consumers.