

Dating App Parallels

Tangentially to the design and proposal for CP, I want to know how particular aspects of other systems work. I'm thinking particularly about dating apps. First, refresh my memory. What are the top three dating apps in the US?

As of February 2025, the top three dating apps in the United States are:

1. **Tinder:** Launched in 2012, Tinder remains a dominant force in the online dating scene. It popularized the “swipe” feature, allowing users to quickly express interest or pass on potential matches. With a vast user base, Tinder caters to a wide range of relationship types, from casual encounters to serious commitments.
2. **Bumble:** Introduced in 2014, Bumble differentiates itself by requiring women to initiate conversations in heterosexual matches, promoting a more balanced and respectful interaction. Beyond dating, Bumble offers modes like Bumble BFF for finding friends and Bumble Bizz for professional networking, making it a versatile platform for various social connections.
3. **Hinge:** Marketed as the app “designed to be deleted,” Hinge focuses on fostering meaningful relationships. It encourages users to create detailed profiles with prompts and photos, facilitating more engaging conversations. Hinge’s algorithm emphasizes compatibility, aiming to connect users seeking serious, long-term relationships.

These platforms have maintained their popularity by continually evolving and adapting to user preferences, incorporating features like video chats, advanced matching algorithms, and enhanced safety measures to improve the online dating experience.

Do these applications use their own identity systems or do they leverage those of other social media companies? Do they allow you to login and register with federated IDs like Facebook or Google?

As of February 2025, the login and registration options for the top three dating apps in the U.S. are as follows:

1. **Tinder:** Tinder offers multiple sign-up methods, including using your phone number, Facebook account, or Google account. This flexibility allows users to choose between creating a standalone Tinder profile or leveraging existing social media identities for quicker registration and login.
2. **Bumble:** Bumble provides options to sign up with a phone number, Facebook account, or Apple ID. By allowing these federated identity providers, Bumble streamlines the onboarding process, enabling users to quickly set up profiles using information from their existing accounts.
3. **Hinge:** Hinge primarily requires users to sign up using their phone number or Facebook account. This approach allows users to either create a new identity specific to Hinge or utilize their existing Facebook profile to populate their dating profile.

In summary, all three platforms offer the convenience of registering and logging in through federated identity providers like Facebook, Google, or Apple, in addition to the option of using a phone number to create a unique account within the app.

Are you aware of their technical architecture with regard to identity? Are they using Okta or Cognito for example?

The specific technical architectures regarding identity management for Tinder, Bumble, and Hinge are not publicly disclosed. Therefore, it's unclear whether these platforms utilize third-party identity services like Okta or Amazon Cognito. However, it's worth noting that these dating apps offer users the option to register and log in using federated identities from providers such as Facebook, Google, or Apple, in addition to using phone numbers. This approach suggests that they have implemented systems capable of handling multiple identity providers, but the exact technologies or services employed remain proprietary information.

Are you aware of any identity fraud scandals involving these or any other dating services? If so what were the implications? Are users on their own? How are these services indemnified for relationships that don't work out, or any kind of abuse initiated from meetups?

Yes, there have been several instances of identity fraud and related scandals involving dating services:

Notable Incidents:

- **Ashley Madison Data Breach (2015):** Ashley Madison, a platform facilitating extramarital affairs, suffered a significant data breach in 2015. Hackers exposed personal information of millions of users, including real names, email addresses, and sexual preferences. This breach led to public shaming, blackmail attempts, and even reports of suicides among affected users.
- **The Tinder Swindler Case:** Simon Leviev, known as the “Tinder Swindler,” used the dating app Tinder to connect with women, building trust and then deceiving them into lending him substantial amounts of money under false pretenses. His actions led to significant financial and emotional harm to his victims.

Implications for Users:

Users often find themselves vulnerable in such situations. While dating platforms implement measures to enhance security, the responsibility largely falls on individuals to protect themselves. It's crucial for users to exercise caution, verify the identities of potential matches, and avoid sharing sensitive personal information early in interactions.

Liability of Dating Services:

Dating platforms generally have limited legal liability for misconduct occurring between users. Under the Communications Decency Act, these services are typically not held responsible for harm resulting from third-party user actions. Additionally, tort law requires a special relationship to establish a duty of care, which is often not present between users and platforms.

However, if a platform is aware of a user's predatory behavior and fails to take appropriate action, it could potentially be held liable for negligence. For instance, if a user creates fake profiles to lure victims and the platform does not address reported concerns, it might bear some responsibility.

Protective Measures:

To mitigate risks, users should:

- **Verify Profiles:** Look for inconsistencies in profiles and be cautious of users who avoid sharing verifiable information.
- **Report Suspicious Behavior:** Utilize the platform's reporting features to flag inappropriate or suspicious activities.
- **Limit Personal Information Sharing:** Avoid disclosing sensitive details until a trustworthy relationship is established.
- **Meet in Public Places:** For initial in-person meetings, choose public settings and inform a friend or family member of your plans.

While dating platforms offer opportunities to connect, users must remain vigilant and proactive in safeguarding their personal safety and information.