United States Senate
WASHINGTON, DC 20510

April 3, 2018

Nancy Hua
CEO and Co-Founder Apptimize
330 Townsend St,
San Francisco, CA 94117

Dear Ms. Hua:

We write to inquire about Apptimize's policies for protecting the sensitive information of Grindr's millions of users. According to a press report, Grindr, a popular dating app tailored for the LGBTQ community, is sharing the most personal and sensitive information of its approximately 3.6 million active daily users without their informed consent.[1] The data includes personally identifiable and sensitive user information such as HIV status, email address, telephone number, precise geolocation, sexuality, relationship status, ethnicity, and "last HIV tested date."

Although the report suggests that Grindr shares profile information with third parties, including Apptimize, to optimize the app and send targeted advertisements, this sensitive information could be misused if appropriate protections are not in place. According to the report, this sensitive information could link specific individuals to their HIV status and sexual orientation. In the wrong hands, this information could lead to unlawful discrimination or worse. Further, according to the report, some of the data in question has been shared with third party advertising campaigns over unencrypted connections, which could leave this sensitive information vulnerable to cyberattack.

Grindr collects highly personal data about its users — information as sensitive as their health, sexual orientation, sexual preferences, and geolocation. Simply using an app should not give companies a license to carelessly handle, use, or share this type of sensitive information. Grindr and those with whom it shares its users sensitive information has an obligation to both protect this data and ensure users have meaningful control over it.

We therefore respectfully request that you respond to the following questions by April 17, 2018:

1. Do you obtain Grindr users' affirmative opt-in consent to use, share, or sell any of the following information: geolocation, email address, phone number, sexuality, relationship status, ethnicity, HIV status, and last HIV tested date? If yes, please detail your policy. If no, please explain why not, and identify the information you are sharing or selling and with whom you are doing so.

---

[1] Azeen Ghorayshi & Sri Ray, *Grindr Is Letting Other Companies See User HIV Status And Location Data*, BuzzFeed (Apr. 2, 2018), www.buzzfeed.com/azeenghorayshi/grindr-hiv-status-privacy?utm_term=.ey3Q0Ggo1O#.ptr5ZjoNPv.

2. What requirements do you impose on third parties with whom you share user data? How long are third parties able to keep user data? What prevents them from selling or sharing this data, or using it for an unapproved purpose?

3. Please identify the data-security practices to which you adhere and detail your data-security policy.

4. Do you require third parties with whom you have shared information to develop and adhere to data-security practices sufficient to protect your user information? If yes, please detail your policy. If no, why not?

5. If users do not want their information shared with a third party, do you provide them opt-out control over their information? If yes, please identify the types of information and detail your policy. If no, why not?

6. When sharing user information, do you practice strong de-identification or anonymization, such that de-identified personal information cannot be reasonably linkable to a person or device? If yes, please explain your process for de-identifying data. If no, why not?

7. Do you prohibit third parties with whom you share or sell sensitive user information from re-identifying de-identified information? If yes, please detail your policy. If no, why not?

8. Do you maintain information or data related to former users? If yes, what information do you keep, how is it maintained, and is it minimized? What are your data-security and privacy policies for the data and personal information of former users?

9. Do you ever notify users of the types of information collected, how and for what purposes you use and share this information, and with whom that information is shared or sold? If yes, please detail your policy. If no, why not?

10. Do you notify customers within 30 days if their information has been breached or accessed by unauthorized parties? If yes, do you also alert customers to any mitigating action they should take? If not, why not?

We thank you for your attention to this important matter.

Sincerely,

Edward J. Markey
United States Senator

Richard Blumenthal
United States Senator