



VIA EMAIL AND FEDEX

April 17, 2018

Senator Edward J. Markey
255 Dirksen Senate Office Building
Washington, D.C. 20510

Senator Richard Blumenthal
706 Hart Senate Office Bldg.
Washington, DC, 20510

Dear Senators Markey and Blumenthal,

Thank you for your letter inquiring about Grindr's policies regarding the protection of the sensitive information of its users. We are grateful for this opportunity to continue setting the public record straight and to offer further clarity concerning Grindr's sharing of user information with certain trusted service providers. Grindr appreciates everyone's concerns surrounding the protection of sensitive information. Unfortunately, some of the stories that have circulated have been inaccurate.

First, and foremost, Grindr is a mobile dating application that serves the gay, bi, trans, and queer community. Given the discrimination, abuse, and safety concerns that our community faces around the world, our goal remains to provide our users with a safe online platform to connect and thrive. Grindr for Equality, our global social impact platform, was created to promote health, safety, and human rights for LGBTQ individuals around the world. This desire to serve the wellbeing of our community led Grindr to give its users the option to share their HIV status to help fight that deadly epidemic. That decision was reached only after considerable deliberation. After consulting with HIV prevention specialists around the world, Grindr determined that allowing users to share HIV status information would help reduce the barriers and stigma that frequently deter people from important conversations about sexual health.

We want to make abundantly clear that Grindr has never sold, nor will it ever sell, personally identifiable user information.

With all of that said, by its very nature, Grindr is a platform for connecting, and part of this search for connection may include, at the user's choice, the sharing of personal information, including a profile picture, relationship status, ethnicity, HIV status, last tested date, and other information that a user voluntarily provides. That is an affirmative decision left to each individual user. Indeed and as noted above, Grindr added the "HIV status" and "last tested date" fields and implemented related functions recently in response to feedback from its users and health organizations requesting that Grindr take proactive steps to promote sexual health awareness among its users. Health researchers have suggested that Grindr's participation in HIV prevention can help curb the epidemic.

Again, ultimately, individual users determine what, if anything, to include about themselves in their profile.

Some of the recent news reports concerning Grindr's sharing HIV status information with two trusted service providers – Aptimize and Localytics – have focused on the perceived invasiveness of providing this type of information to service providers. What these reports fail to explain consistently is that Aptimize and Localytics were hired by Grindr to provide analytics services to Grindr, to help

improve the platform's performance and to help Grindr communicate with users, including facilitating a new feature which helps remind Grindr users to get HIV testing done periodically. Neither company shares Grindr data with third party advertisers. Indeed, under the terms of their agreements with Grindr, neither company was permitted to share or sell Grindr user data. Grindr retained ownership of all Grindr user information under the terms of its agreements with both companies. Both companies agreed to keep Grindr user data confidential.

Nonetheless, with this background, and in response to user feedback, Grindr no longer shares the HIV status of its users with these two companies.

In addition, recognizing the importance of these matters, Grindr is launching an initiative designed to elicit industry-wide protocols for the handling of sexual health information across social network and dating apps. We hope that other platforms will join Grindr and be part of the global effort to end the spread of the HIV epidemic.

Answers to your specific questions follow below.

- 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.**

As a threshold matter, Grindr has never sold personally identifiable user information; and Grindr will never sell personally identifiable user information.

As to using or sharing such information, yes, Grindr obtains users' consent to use or share their information within the Grindr app. Specifically Grindr users are presented with a copy of Grindr's privacy policy. Unlike most other online applications, they are not simply provided with a link to the privacy policy or have access to it within the application. Users are shown the actual privacy policy. Grindr users are then asked to acknowledge/agree to Grindr's privacy practices twice. First they click that they would like to "proceed" forward with the use of the Grindr application given its privacy practices; they are then asked a second time to "opt-in" by clicking that they "accept" the privacy practices.

Grindr's privacy policy clearly indicates that the information that a user chooses to provide about their HIV status, geolocation, relationships, and other information in their profile is displayed to other Grindr users and may be used for other purposes such as to provide the user with reminders to get tested for sexually transmitted infections. It also indicates that the information may be shared with service providers that help provide technical support to Grindr and that in such a situation Grindr contractually prohibits those service providers from using the information for other purposes.

- 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?**

Grindr requires service providers who receive its data to abide by appropriate contractual terms, including terms that prevent the service provider from sharing or selling Grindr user data. How long a service provider may retain Grindr user data varies from contract to contract, but in no instance is a service provider allowed to keep Grindr user data longer than is necessary for the service provider

to fulfill its contractual and legal obligations. By contract, service providers are not permitted to share Grindr user data for any purpose other than to provide service to Grindr, nor are they permitted to sell such data.

If Grindr were to learn of a service provider's improper sharing or selling of Grindr user data, Grindr would take immediate, appropriate actions, which may include, but are not necessarily limited to, the termination of the relationship with the service provider, the cessation of providing Grindr user data to the service provider, and the initiation of lawsuits seeking to enjoin the sharing or selling of Grindr user data.

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

Grindr takes data security seriously and takes steps to protect its users' personal data from unauthorized access, use, or disclosure, including the use of electronic, logical and physical access controls, and extensive logging of its network systems to identify, block and address potential threats. Additional information about Grindr's public statements on its data security practices can be found in Grindr's privacy policy: www.grindr.com/privacy-policy/.

Because public disclosure of specifics concerning data security measures can inadvertently weaken the effectiveness of security measures (by providing information to bad actors that may be used to circumvent the security), as a policy matter, Grindr does not publicly discuss details concerning its security program.

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?

Yes. Grindr requires service providers with whom it shares Grindr user information to adhere to data security practices to protect Grindr user information.

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?

By design Grindr only requires that users provide an email address when creating a Grindr account. No other information about the user is required. A user's email address is not shared with the public or other users within the App.

All users have control over what, if any, data they publish on Grindr. Users supply the majority of data to Grindr – and all of the sensitive data that they provide to Grindr – on a completely voluntary basis, *i.e.*, users have control over the information they supply in their Grindr profiles. Additionally, Grindr's Privacy Policy explains to users how they may opt-out of behavioral advertising.

In keeping with current industry standard practices, Grindr does not offer its users the opportunity to opt-out of sharing with Grindr's service providers.

In the case of analytics and operational service providers, it is important to provide robust user experience data in order for these types of service providers to provide Grindr with the services

requested by Grindr. Allowing segments of our user base to opt-out of including their data in these datasets would create inaccurate pictures of what is occurring in Grindr's systems.

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?

There is no single standard for what constitutes the de-identification or anonymization of data.

Grindr takes steps to allow users to make their personal data non-attributable without the use of additional information, although it does not make the data within its system impossible to associate to a person. Specifically, users are not required to provide their name, address, or telephone number, when they join Grindr, and they are not required to provide that information in their user profile. Although users are requested to provide an email address, that email address is not shared with the public. Users can, of course, voluntarily include information within their profile which would identify them. Storing personal data in a manner that does not permit easy identification without the use of additional research or information is sometimes referred to as data pseudonymization.

Grindr is now also analyzing the feasibility of using additional de-identification and anonymization practices to better secure its users' privacy. Grindr does not yet have an estimate on when that analysis will be completed.

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?

Again, Grindr has never sold personally identifiable user information; and Grindr will never sell personally identifiable user information.

When Grindr does share personal information with service providers, such service providers are authorized only to use such information in connection with providing services to Grindr, so any attempt to identify a particular user, or to connect a user's data provided by Grindr with data from another source, would be prohibited (except in the hypothetical circumstance where re-identification was somehow a part of the services provided – Grindr has no intention of ever directing or authorizing a vendor to re-identify any data). As noted in response to Question 6, Grindr is investigating the feasibility of using additional de-identification and anonymization practices in the future.

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?

Grindr has instituted steps to erase much of the personal information that it collects from former users within a short period of time after a user deletes the information or leaves Grindr. Grindr's privacy by design approach also seeks to minimize the amount of information Grindr collects, or maintains, about the user. For example, when a user engages in a conversation with another user (e.g., a chat session) the text exchanged between two users is not stored by Grindr, and after delivery exists only on the end-users' local devices. As a result, Grindr maintains no copies, or history, of text exchanged between or among its users.

Grindr applies the privacy and security practices described in its privacy notice to both current and former users.

9. When updating privacy policies, must current users agree to the new terms in order to continue service? Please detail your policy.

Grindr's policy on revisions to its privacy policy is contained within the Grindr Privacy Policy:

***"Changes To This Privacy Policy.** If we make a material change to this policy we will, at a minimum, attempt to notify you of that change either by sending an e-mail to the last e-mail address that you provided to us (if any) or by notifying you when you log into the Grindr Services. Continued use of the Grindr Services indicates your agreement that any information relating to you, regardless of when it was collected, will be governed by Grindr's current policy."*

In addition to notifying users concerning changes to its privacy policy, when Grindr last updated its privacy policy in August 2017, it asked each of its users to affirmatively agree or "opt-in" to the change.

10. 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?

Yes. Users of the Grindr app are notified of the types of information collected, how and for what purposes Grindr uses and shares this information, and with whom that information is shared within the Grindr Privacy Policy available at: www.grindr.com/privacy-policy/. Users are also notified when Grindr makes a material change to its privacy policy either via email or when the user accesses the Grindr Services.

In addition, users are provided with in-time contextual notice concerning the health related information that is being collected by Grindr as Grindr only collects such information directly from the user when they manually submit it while deciding to publish such information on their public profile page.

11. 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?

Grindr complies with applicable data breach notification laws and would notify users as soon as practicable if Grindr believed that user information was breached or accessed by unauthorized parties. Grindr would also advise users of potentially mitigating actions they could take following such an incident.

12. Do you notify customers when you make material changes to your privacy policies? If yes, please detail your customer-notification policy. If no, why not?

Yes, Grindr notifies its users when it makes material changes to its privacy policy. Grindr's policy on notifying users of revisions to its privacy policy is contained within the Grindr Privacy Policy:

***"Changes To This Privacy Policy.** If we make a material change to this policy we will, at a minimum, attempt to notify you of that change either by sending an e-mail to the last e-mail address that you provided to us (if any) or by notifying you when you log into the Grindr Services. Continued use of the*

Grindr Services indicates your agreement that any information relating to you, regardless of when it was collected, will be governed by Grindr's current policy."

When Grindr last updated its privacy policy in August of 2017 in addition to notifying each user when they logged into their Grindr account, it also asked the user to affirmatively opt-in to the new policy.

13. Do you have a clear, user friendly, easily accessible, and responsive complaint process for users who have evidence or reason to believe their privacy has been violated? If yes, please detail your policy. If no, why not?

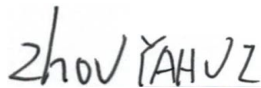
Yes. Grindr allows users to contact it via email or postal mail to report any complaints or concerns that they might have regarding the privacy of their information. We have systems in place to review and respond to such inquiries promptly. As Grindr's privacy policy explains:

Contact Information. *Grindr welcomes your comments or questions regarding this Privacy Policy. Please contact us at the following:*

privacy@grindr.com
Mailing Address:
Grindr LLC
PO Box 69176
West Hollywood, CA 90069

Thank you for the opportunity to address your concerns and questions about Grindr's privacy and security practices. If you wish to discuss any of these responses, or other matters, further, we are happy to make members of the Grindr team available for a call or a meeting with you and your staffs.

Sincerely,



Zhou Yahui
Interim CEO of Grindr