



**Grindr LLC.**  
**6725 W. Sunset Blvd.**  
**Suite #430**  
**Los Angeles, CA 90028**  
**310 776-6690**

March 8, 2012

Honorable Henry A. Waxman  
Ranking Member  
Committee on Commerce and Energy  
U.S. House of Representatives  
2125 Rayburn House Office Building  
Washington, DC 20515-6115

Honorable G.K. Butterfield  
Ranking Member  
Subcommittee on Commerce,  
Manufacturing and Trade  
U.S. House of Representatives  
2125 Rayburn House Office Building  
Washington, DC 20515-6115

Dear Congressmen Waxman and Butterfield:

Thank you for your letter of February 23, 2012, inquiring into our practices regarding information security. We are grateful for your inquiry, which offers us an opportunity to set the record straight on this issue of significant public interest. As you note in your letter, your inquiry was generated by a report in the Australian press about the Grindr application (“Grindr”), which was triggered by allegations of an anonymous “expert” giving the false impression that Grindr is fundamentally insecure. Before dealing with your specific questions, please allow me to describe our business and tell you what it does and does not do.

### **What Grindr Is**

Grindr is an all male location-based mobile network tool. Grindr LLC is a Los Angeles based company that I launched in 2009 with an initial investment of \$5,000 from my own savings. The staff consisted of me and several others working on contract. With no outside funding, I ran it out of my house until July 2010. In the brief period since start-up, Grindr has exploded into a worldwide social network that has surpassed my wildest dreams. I immigrated

to the United States as a boy and I am proud of what my team and I have accomplished and of the economic growth and employment we have brought to Los Angeles, but there is no doubt that Grindr’s rapid growth has presented us with many challenges.

Grindr facilitates men meeting other men of like interest in their vicinity. Collecting location information about our users is therefore an essential part of what our users expect us to do. Our privacy policy is clear on this point. The policy says that Grindr “uses the GPS technology in [your device] to determine your exact location and instantly connect you with guys in your area.” It then explains that in order to do this, Grindr collects the user’s device id. The policy then states: “Please note that if you choose to show your location, the information that is provided to Grindr about your distance will be used within your profile and can be viewed and searched by other Grindr users. Even if you choose to hide your distance information, sophisticated users of Grindr may be able to determine your location.” I emphasize, however, that Grindr does not retain location information about its users other than the last known location.

Our users’ privacy is of utmost importance to us. Grindr users may remain anonymous and many do. The privacy policy states that users do not have to provide any information about themselves. “No photo or any details about yourself are required to start using Grindr . . . [T]he information you share is totally your choice.” However, the policy goes on to warn that “when you use Grindr, certain information you post or provide on Grindr may be shared with other users, including without limitation your profile, comments, photographs and locations.”

You have also inquired about our other applications. Grindr Xtra is a premium, fee-for-service version of Grindr. Blendr is a service like Grindr but aimed at a wider audience.

Our applications do not retain credit or debit card numbers, social security numbers, driver’s license numbers, or financial account numbers of any kind. Grindr Xtra uses a third-party to process payment information.

### **Responses to Your Questions**

- 1. According to the *Sydney Morning Herald* report, you initially claimed that Grindr had “never experienced a ‘major breach’ in which a large portion of users were affected” and that you were not aware of the chat function vulnerability.<sup>1</sup> However, in a subsequent conversation with the newspaper you said you were “aware of some vulnerabilities.”**
  - (a) Have Grindr, Grindr Xtra, or Blendr experienced any other breaches of any size in which any user provided information – including, but not limited to, chats, photos, linked social network accounts, and profile information – was**

---

<sup>1</sup> The comment made in the Australian press article was that Grindr is unaware of “the potential for text chats to be monitored.”

**compromised? If so, for each breach, how many users were affected? Where were they located? What information was compromised? How and when were affected users notified of the breach?**

Other than the vulnerability reported in the Australian press to which you referred, we are aware of only two instances where an intruder modified a small sub-set of our Grindr user profiles in Australia and the United Kingdom. These breaches affected 720 profiles, or .024%, of a total of 3 million users worldwide. To our knowledge, none of these incidents involved an intercepted chat session or the compromise of personal information; rather an intruder gained access to our system and posted the electronic equivalent of public graffiti on a user's profile. Grindr discussed the breach with affected users who contacted customer service and removed the offensive content.

**(b) Did you provide *any direct* notice to any of your users regarding the breach reported by the *Sydney Morning Herald*? If so, how and when? If not, why not?**

We promptly notified users of the breach through public relations statements and official statements on our blog. As an anonymous application, Grindr does not require users to provide email addresses, phone numbers, or other identifying information. We therefore did not have the means to notify individually impacted users directly unless they contacted us.

**(c) What Grindr, Grindr Xtra, or Blendr security vulnerabilities were you or your staff aware of at the time of your interview with the *Sydney Morning Herald*? When and how did you or your staff become aware of each of these vulnerabilities? What steps had you taken at that time to deal with the vulnerabilities of which you and your staff were aware?**

At the time of the interview you inquired about, we were aware that our Grindr Application Programming Interface (API) could be vulnerable. We first became aware of this in 2011 when we learned that a third-party developed an infringing application called "Grindroid," a clone of Grindr for the Android platform, and, without our authorization, the third-party briefly offered it for sale to the public. We contacted the developer of Grindroid, who agreed to refrain from selling the application.

Later in 2011, through our own analysis and from user reports, we learned of <http://rdnirg.info>, a site that exposed the vulnerability of our API. We immediately blocked the [rdnirg.info](http://rdnirg.info) site to protect information which could be vulnerable if an intruder accessed our API. We also decided to develop a completely new, secure architecture for all of our applications.

When the Australian press article was published we knew that the chances hackers would target our vulnerabilities would increase. Because we had by that time built an in-house technical team that was already in the process of developing a new, secure architecture, we were

able to accelerate our security efforts. The team worked around the clock to develop the security enhancements that we were ultimately able to implement in February 2012.

**(d) What security features were included in the versions of Grindr, Grindr Xtra, and Blendr that preceded the latest updates?**

Prior to the latest updates, our versions included the following security features:

- A Secure Hash Algorithm (“SHA-1”) of a device id was used to log-in users.
- The Chat server required a password.
- Grindr chat history and delivered messages were not stored online.
- We used a third-party to collect and process payments for Grindr Xtra and did not retain financial information of any kind on Grindr Xtra servers.

**2. According to the report, Grindr uses a personalized string of numbers known as a hash to log in users, rather than requiring a username and password. Your privacy policy states: “In order for Grindr to work with your iPhone, iPod touch, iPad, BlackBerry, or other mobile device, we must collect your Device Identification Code.”**

**(a) Do you access, transmit, or collect any other information from or about a user’s device – including, but not limited to, the user’s phone number, email account information, or address book?**

Other than the device id, software and hardware versions, and relative location information, Grindr does not access, transmit, or collect any other information from or about a user’s device.

**(b) Is the hash used to log in any of your users the Unique Device Identifier (UDID); a Media Access Control (MAC) address; any other identifier unique to a specific device? If so, do you use any type of encryption or take other measures to protect against privacy and security vulnerabilities known to be associated with the use of device-specific identifiers to log in mobile app users?**

We use a SHA-1 of a device’s unique id to log-in users. In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States National Institute of Standards and Technology as a U.S. Federal Information Processing Standard.

**(c) Do you store UDIDs, MAC addresses, or any other identifier unique to a specific device with any other information provided by users – including, but**

**not limited to, photos, linked social network accounts, and other user provided profile information? If so, what information?**

An id that is unique to a user's device is stored with the user's profile information. The user determines the contents of the profile.

- (d) **With the release of iOS 5.0, Apple Inc. began phasing out access by app developers to UDIDs, and some reports suggest that more recently the company has started reaching out to some developers to hasten this phase out. Please explain what steps you have taken to phase out the use of UDIDs, MAC addresses, or any other identifier unique to a specific device.**

We will phase out the use of UDIDs and introduce account user names and passwords in a new version that we expect to release in mid-2012.

- (e) **Do the latest versions of Grindr, Grindr Xtra, and Blendr continue to rely on hash to log in users? If so, please explain why you use hash to log in users rather than requiring a username and password. Also, what additional security enhancements have you implemented to protect users from vulnerabilities associated with this log in method?**

The current versions of our applications use hashed ids to log-in users. Hashed ids are important because they protect the anonymity of our worldwide users by preventing the need to collect and store account information.

We have instituted secure encryption of all traffic to our servers, as well as new cryptographic ciphers to protect users' data.

- (f) **Have you at any time conducted any assessment of the security risks to your users' accounts and information from relying on hash to log in users? Have you at any time conducted a security risk assessment regarding any features of your app?**

We have assessed the security risks that may arise from relying on hashed ids to log-in users. On one hand, a sophisticated attacker may be able to spoof an id. On the other hand, hashed ids are important to our users to protect their anonymity. Now that Apple is moving away from UDIDs as a log-in method, we have decided to follow suit.

We have also conducted internal security assessments of our overall application. We retained a security consultant to conduct a security review of our application, and we continue to capitalize and grow new internal resources to implement recommended changes for our applications.

- (g) Have you ever conducted a privacy impact assessment concerning your information collection and use practices?**

Our legal counsel evaluates our policies and procedures to ensure we are in compliance with privacy requirements.

- 3. You claimed that you would rush to release a security update for your applications in a “few days.” However, it took you up to three weeks to release those updates.**

- (a) Please explain why it took you two weeks to release the security updates for Grindr and Grindr Xtra, and three weeks for Blendr, when a security expert claimed that securing your application “wouldn’t be too hard.”**

I initially believed it would require only a few days to implement security updates to our applications. My technical staff informed me, however, that typically it would take weeks just to get an application through reviews and approvals (by Apple and Blackberry, e.g.) and deployment. We had to add cryptography against server side and five client platforms, test that the changes would not bring the network down, get release approvals, and phase out all existing clients. The opinion of an anonymous security “expert” about the ease of implementing these changes should be read with caution, to say the least.

- (b) What measures did you take to protect your users’ information from breach in the period between when the Australian breach became public on January 20 and when you released the security updates on February 3 for Grindr and Grindr Xtra and February 10 for Blendr?**

While we worked to implement the security updates we maintained heightened vigilance for unusual network traffic. Our customer service agents evaluated unusual customer activity and reports. This allowed us to block access when unusual activity was detected.

- (c) Please describe each security enhancement included in the latest versions of Grindr, Grindr Xtra, and Blendr and the vulnerabilities they are meant to address.**

The security enhancement was an extensive operation that involved major updates to all elements of our architecture and was designed to address the vulnerabilities described above. It included a combination of introducing a client side cryptographic cipher in Grindr iOS, Grindr iOS Xtra, Grindr Android, Grindr Blackberry, Blendr iOS, Blendr Facebook, and multiple server updates. We updated all the API endpoints on the clients and on the server side to use Hypertext Transfer Protocol Secure (“HTTPS”), which provides encrypted communication and secure identification of our network web server. We wrote code for a new chat authentication mechanism that has been deployed on new servers in our infrastructure. We worked with Google (one of our hosting providers) to add HTTPS to encrypt traffic at our endpoints to prevent simple sniffing of the data. Ultimately, we forced all users to upgrade to the new secured clients by rendering all previous versions inoperable.

**(d) Please explain why you had not included these security features in previous versions of Grindr, Grindr Xtra, and Blendr.**

Security is an evolving challenge, not a fixed point. It involves a constant contest of wits between lawful online vendors and service providers like Grindr, on the one hand, and hackers, fraud artists, and criminals on the other. It also involves trade-offs with users' convenience that vendors and service providers must take into account.

We determined that developing a new, secure architecture was the best solution. But it took us time to build the technical capability to successfully implement our security enhancements. Please see the response to question 1(c).

**(e) Does Grindr Xtra, the paid version of your app, include any additional security features not included with the free version?**

No. There are no additional security features in any paid version of our applications.

In closing, let me say again that we are grateful for your interest in the evolving challenge of securing networks and applications against exploitation by unauthorized users and criminals. The privacy and security of our service and of our users' private information are of utmost importance to us, and we continue to upgrade our services in order to provide attractive and secure services to our users. To our knowledge, a user's identifying information – such as name, email, phone number, financial information, or social security number – has never been compromised on Grindr, Grindr Xtra, or Blendr.

Sincerely,



Joel Simkhai  
Founder and CEO  
Grindr LLC and Blendr LLC

Cc: Mr. Felipe Mendoza