

ONE HUNDRED TWELFTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

February 23, 2012

Joel Simkhai
Founder and CEO
Grindr LLC and Blendr LLC
6725 Sunset Blvd., Ste. #430
Los Angeles, CA 90028

Dear Mr. Simkhai:

On January 20, 2012, the *Sydney Morning Herald* reported that a hacker breached the accounts of Grindr users in Australia. According to the report, the hacker was able to “log in as another user, impersonate that user, chat and send photos on their behalf.”¹ In addition, a security expert who replicated the breach for the newspaper asserted that both of your mobile location-based social networking apps – Grindr and Blendr – have “‘no real security’ and were ‘poorly designed.’”²

As the company boasts, Grindr is “the largest all male location-based mobile network tool”³ with more than three million users in 192 countries, including more than 800,000 users in the United States.⁴ Blendr, a similar social networking mobile application targeting a broader audience, was launched in September 2011.⁵

Much of the debate about data security in Congress has focused on the harm of identity theft, which is generally understood to involve the unauthorized use of certain narrow types of personally identifying information – like a social security number or financial account numbers. Some members of Congress have argued that only these types of data need to be secured. However, the failure by online services to secure chats, location information, photographs, and

¹ Ben Grubb, *Love Online: 100,000 Grindr Users Exposed in Hack Attack*, *Sydney Morning Herald* (Jan. 20, 2012) (available at www.smh.com.au/technology/security/love-online-100000-grindr-users-exposed-in--hack-attack-20120119-1q7pf.html).

² *Id.*

³ Grindr, LLC, *What is Grindr?*, Grindr.com (accessed Feb. 22, 2012).

⁴ Grindr Press Release, *Grindr Surpasses Three Million Users in 192 Countries* (Nov. 3, 2011).

⁵ Blendr Press Release, *Social Networking Just Got Social with Debut of Blendr* (Sept. 8, 2011).

other information people would want to keep private also could lead to economic harms as well as reputational harms, so we believe such information should also be protected.

This incident raises questions about the steps your company takes to protect the privacy and security of your users' information. The web pages containing the privacy policies for both of your mobile apps claim that they are "all about your privacy."⁶ Yet an independent security expert found there were security vulnerabilities in your apps that could have been mitigated, but were not.⁷ Every online service that asks its users to trust it with the transmission or collection of their information – whether it is a social network, a dating service, a retailer, or a financial institution – has an obligation to its customers to properly secure that information. Ensuring adequate security for users' information is an essential element of protecting their privacy.

In order to more fully understand this incident, and to help inform Congress's ongoing efforts to develop data security legislation, we request that you answer the following questions. As you develop your responses to this request, we want to be clear: Our only interest is in assessing the security measures taken by online services to guard their users' information. We are *not* asking for, nor are we interested in, any personally identifiable information about your users. That information is personal and private, and our efforts are aimed at keeping it that way.

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. 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 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?
 - 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?
 - 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*?

⁶ Grindr Privacy Policy (available at www.grindr.com/privacy-policy); Blendr Privacy Policy (available at blendr.com/privacy-policy) (accessed Feb. 22, 2012).

⁷ Grubb, *Love Online: 100,000 Grindr Users Exposed in Hack Attack*.

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?

- d. What security features were included in the versions of Grindr, Grindr Xtra, and Blendr that preceded the latest updates?
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?
 - 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?⁸
 - 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?
 - 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.⁹ 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.

⁸ See Jennifer Valentino-DeVries, *Privacy Risk Found on Cellphone Games*, Wall Street Journal (Sept. 19, 2011) (available at <http://blogs.wsj.com/digits/2011/09/19/privacy-risk-found-on-cellphone-games/>).

⁹ Kim-Mai Cutler, *Apple Steps Up Outreach to Developers Over Moving Away from UDIDs*, Inside Mobile Apps (Feb. 16, 2012) (available at www.insidemobileapps.com/2012/02/16/apple-steps-up-outreach-to-developers-over-moving-away-from-udids/).

- 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?
 - 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?
 - g. Have you ever conducted a privacy impact assessment concerning your information collection and use practices?
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."
 - 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?
 - 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.
 - d. Please explain why you had not included these security features in previous versions of Grindr, Grindr Xtra, and Blendr.
 - e. Does Grindr Xtra, the paid version of your app, include any additional security features not included with the free version?

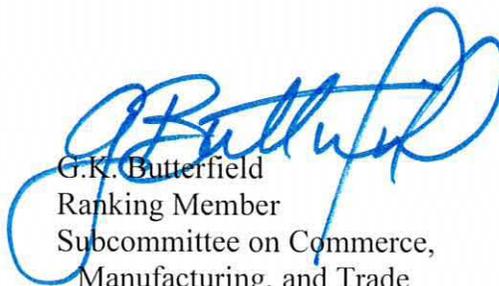
Please provide the information requested in writing no later than March 8, 2012. If you have any questions regarding this request, contact Felipe Mendoza with the Energy and Commerce Committee Staff at 202-226-3400.

Mr. Joel Simkhai
February 23, 2012
Page 5

Sincerely,



Henry A. Waxman
Ranking Member



G.K. Butterfield
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade