May 27, 2019

The Honorable Josh Hawley
United States Senate
212 Russell Senate Office Building
Washington, DC 20510

Dear Senator Hawley,

Thank you for your letter of May 13, 2019, regarding privacy and data use by Facebook, Instagram, and WhatsApp. The people who use Facebook—and lawmakers—should have a clear understanding of the kinds of data we collect and how we use that data, and we appreciate your interest in this area. As Mark Zuckerberg recently wrote in a Facebook post (and reiterated in his F8 keynote), the shift to a privacy-focused platform will focus around several key principles: creating spaces for private interactions, reducing permanence, encryption, safety, interoperability, and secure data storage. This is a work in progress that we expect to take several years, and it is still in its early stages.

As he noted further in his post, we plan to consult widely on the challenges this approach presents.

> *The decisions we'll face along the way will mean taking positions on important issues concerning the future of the internet. We understand there are a lot of tradeoffs to get right, and we're committed to consulting with experts and discussing the best way forward. This will take some time, but we're not going to develop this major change in our direction behind closed doors. We're going to do this as openly and collaboratively as we can because many of these issues affect different parts of society.*

As part of that consultative effort, we welcome the opportunity to engage with your office around this effort.

With that context in mind, below, please find answers to your specific questions.

Messaging Privacy

What metadata will Facebook maintain related to user messaging interactions, and for how long? How will it use such data? Will such data supplement other data in user profiles to enhance ad targeting?

There are still many open questions about what metadata we will retain. An important element of our privacy-focused messaging is to collect less personal data in the first place, which is the way WhatsApp, for example, was built from the outset. Another goal will be to limit the amount of time we store messaging metadata. We will use this data primarily to operate our services and to run our spam and safety systems, but we are open to evaluating the amount of time we need to retain data in the interest of reducing permanence. We've

Address: 575 7th Street NW
Suite 700
Washington, DC
20004

committed to consult privacy and safety experts, law enforcement, and governments on the best way forward, which we have already begun doing.

Will Facebook make any attempt to determine, by comparing such metadata with other data sources, anything about the content of users' conversations, such as which articles Facebook users have likely shared with each other via encrypted messenger?

As described above, there are still many open questions about what metadata we will retain and how it may be used. We've committed to consult safety and privacy experts, law enforcement, and governments on the best way forward. With the shift to end-to-end encryption, our goal is to ensure that message content can only be seen by the intended recipients—not hackers, criminals, or even Facebook.

Will it commit to establishing a firewall between data related to user messaging, including metadata related to links shared through the platform, and the rest of its data infrastructure?

As described above, there are still many outstanding questions around our plans to use metadata, or even what metadata will be maintained. However, it is worth noting that data related to user messaging is integral to how our products currently work (such as receiving a notification within Facebook.com when you receive a Facebook message) and to our ability to conduct investigations that help make the platform safer, reduce SPAM and fraud, and cooperate with law enforcement requests. This data will be even more integral to our safety and integrity efforts once the content of messages is end-to-end encrypted.

If not, will Facebook cooperate with inquiries by Congress and the FTC regarding whether its public representations about this messaging platform are misinforming consumers?

Facebook will of course cooperate fully with any Congressional or agency inquiries.

<u>Commerce and Payments</u>

What metadata will Facebook collect and retain relating to commercial interactions through its messaging platform and payments more generally? How does Facebook define "non-public personal financial information," and does such information include the names of participants in payment transactions? What metadata categories are excluded from this definition?

Today, payment transactions take place on Facebook either through Facebook Payments Inc. (which processes P2P payments in the U.S. over Messenger, donations to U.S. charities onboarded to our fundraising platform, and payment for digital goods on games within Facebook on the web) or a commercial partner (e.g. PayPal powers transactions for certain U.S.-based Shops on Pages and Instagram Checkout in the US).

Address: 575 7th Street NW
Suite 700
Washington, DC
20004

Facebook Payments Inc. is a financial institution and subsidiary of Facebook Inc. with its own Privacy Policy. Facebook Payments Inc. collects non-public personal financial information data necessary for payment transactions (e.g. payment credentials) in accordance with GLBA, and it is PCI-DSS compliant. Payment card information is stored in a separate PCI-DSS compliant environment.

As Facebook is the platform on which these transactions take place, Facebook Inc. also collects data related to the transaction (e.g. purchase made, merchant, transaction amount, date, time), similar to any other commerce platform. For example, Facebook collects information related to interactions on Marketplace, which is used to provide a better experience and to better suggest products.

How will data and metadata relating to commercial and other payment interactions--including data relating to the origin and conclusion of encrypted private chats with advertisers or Facebook contacts as well as data on payments occurring within such chats--be used by Facebook?

As noted above, there are still many open questions about what metadata we will retain and how it may be used. We've committed to consult safety and privacy experts, law enforcement, and governments on the best way forward.

Will such data inform Facebook's advertising and other data-based personalization algorithms?

Payment account information (e.g. credit card number or bank account information) is not used for Facebook advertising or personalization. Similar to other direct interactions users make on Facebook, information about transactions can be used for personalization on the Facebook platform in accordance with Facebook's data policy.

What commitments will Facebook make to wall off such data from the rest of its data collection and advertising algorithms to ensure user confidence in the ostensible privacy of its private messaging platform? Will any such data be exempted from such commitments?

As described above, Facebook Payments Inc. already stores payment card information in a separate PCI-DSS compliant environment. As for metadata, as previously noted, data related to user messaging is integral to how our products currently work (such as receiving a notification within Facebook.com when you receive a Facebook message) and to our ability to conduct investigations that help make the platform safer, reduce SPAM and fraud, and cooperate with law enforcement requests. We are committed to continuing to consult with safety and privacy experts, law enforcement, governments, and regulators on how best to comply with any applicable regulations and ensure user confidence in our platform.

<u>Groups and Events</u>

Address: 575 7th Street NW
Suite 700
Washington, DC
20004

Will encryption be available for private messages between more than two participants?

Yes. WhatsApp encrypts group conversations today, and we plan to use WhatsApp's privacy model as a starting place for the private messaging future.

Will Facebook commit to apply the same data encryption protocols used in private messenger to Facebook groups?

Facebook's encryption efforts are beginning with our messaging platforms, the most fundamental and private use case. This vision for messaging is a complement to our current products that are focused on the more public town square, such as Facebook Groups, which are well-suited for easily finding new communities of people with similar interests. We do not currently plan to end-to-end encrypt the content shared in Facebook Groups.

Will it make any privacy-protective distinctions with respect to its own data collection for user profiling and advertisement between data shared in open groups and data shared in closed and secret groups?

The Groups privacy model gives Group administrators the ability to choose who can see the content of the group and whether it is discoverable by non-members on Facebook. In order to give all Groups meaningful and relevant features, we use Facebook Group membership as one of many signals that can personalize your experience on the platform.

Will it allow advertisement targeted to groups, and will the advertising allowed differ between different categories of groups?
We currently do not allow targeting to groups. As we add monetization options across our products, we will continue to make sure those ads products reflect our existing advertising principles, including limiting categories advertisers can target based on.

<u>Changes to the Platform and Effect on Publishers</u>

What steps have you taken in recent months to prepare publishers dependent on your platform for the announcements made at F8? If you have not taken such steps, why not?

Facebook has multiple channels for communication with publishers about changes to our products that might impact them. Those communications may vary based on what kind of publisher we're reaching out to (a local small business, a multinational corporation that is a managed client, a news publisher, etc.), but in general that outreach includes, but is not limited to:

Address: 575 7th Street NW
Suite 700
Washington, DC
20004

- Announcements shared in our News Room and on our various properties, such as the Facebook for Business Page, the Facebook Politics and Government Page, and the News Feed FYI blog;
- Press outreach about product changes in national and trade publications;
- Special channels for particular types of publishers, such as the Facebook Journalism Project Community Network;
- Updates to the Facebook Help Center;
- Dedicated support channels for Facebook
- Outreach to certain partners who have managed relationships;
- Livestreaming events where announcements are made, such as F8;
- Local events, such as Facebook Boost Your Business, Community Boost, and pop-up events;
- Participation in trainings, conferences, and other large meetings, which might include Help Desks or information booths.

Thank you again for the opportunity to address these questions. As noted above, we are in the early stages of this process. We are committed to keeping members of Congress and their staff informed and engaged as we move forward, and we would be happy to brief you and your staff on these issues as requested.

Sincerely,

Kevin Martin
Vice President, U.S. Public Policy

facebook

Address: 575 7th Street NW
Suite 700
Washington, DC
20004