JOSH HAWLEY
MISSOURI

KYLE PLOTKIN
CHIEF OF STAFF

212 RUSSELL SENATE OFFICE BUILDING
TELEPHONE: (202) 224-6154
FAX: (202) 228-0526

WWW.HAWLEY.SENATE.GOV

United States Senate

WASHINGTON, DC 20510-2509

COMMITTEES
JUDICIARY
ARMED SERVICES
HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
SMALL BUSINESS
AND ENTREPRENEURSHIP
AGING

May 13, 2019

Mr. Mark Zuckerberg
Chief Executive Officer
Facebook
1 Hacker Way
Menlo Park, California 94025

Dear Mr. Zuckerberg:

I wish I could congratulate you on the launch of the latest version of the Facebook platform. But in the same week that you told the world that this time, finally, you are serious about a privacy-first future for Facebook, you were also letting your investors know that you expect to pay the largest fine ever in the United States for falsely pretending to be a company that cares about privacy.

In your F8 speech, you promised to shift Facebook from a "town square" platform into one focused on encrypted messages between smaller groups. But we both know that your business model is monetizing private data, not promoting privacy. And we both know that platforms that tout encrypted messaging can still engage in unscrupulous data harvesting.

While I hope that you and your platform can play a role in building the privacy-first future, I worry that your recent announcements indicate a different intention. To be blunt, I fear that your new platform's aim is to capture and subvert the privacy revolution that threatens your business model and claim an empty public relations victory. You claim your goal is to limit Facebook's window into users' lives, but your future profits demand that you expand that window.

The American people deserve to know how you plan to do that before they sign on to your new vision of supposedly private social engagement.

Messaging Privacy

At your F8 keynote, you promoted your vision of a "privacy focused social platform" with "private interactions" featuring end-to-end encryption. Yet this raises the question of how you can possibly monetize an encrypted platform. News reports suggest that this question has long been a source of frustration for your executive team, contributing to the departures of the founders of WhatsApp from Facebook.

As you have observed, privacy-oriented consumers are shifting from open and monetizable data sharing on unencrypted platforms like yours to encrypted private messaging apps. These kinds of apps, like iMessage and Signal, are distinct from Facebook Messenger in a central respect: they are not connected to a broader ad-based social network infrastructure. Whatever metadata they collect is not fed into a broader platform aimed at the erosion of user privacy for profit.

Encrypted messaging on Facebook, presumably, would be another matter. If you succeed in capturing the encrypted messaging market, I fear that the net effect would be erosion rather than expansion of user privacy. A dominant Facebook messenger could mean a transfer of information about users' most sensitive contact lists – the people to whom users are closest and in whom they confide their deepest secrets, as well as the dates and times of those interactions – from platforms with no interest in monetizing such information to a platform whose business model relies on such data exploitation.

Moreover, as you well know, data related to messaging is not limited to the text of messages. Facebook knows when its users are interfacing with its messaging products, and it knows through browser cookies and integration with publisher websites when users have clicked links to read articles. What features you offer to allow erasure of "off platform" web activity are off by default – a strange design decision for a privacy-focused platform. In combination, these data sources might tell Facebook when its users share links clicked by others through its encrypted messaging platform and which links receive the most traffic through the messaging platform, therefore enabling Facebook to extrapolate the content of users' conversations and add such insights to users' advertising profiles. A digital living room that transmits information to those outside it about which people discuss which subjects with each other within it is not a living room; it's a human aquarium.

- *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?*

- *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?*

- *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?*

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

Commerce and Payments

One form of monetization your company provides is advertising that places advertisers into direct, soon-to-be encrypted chats on the messaging platform. Such a monetization scheme complements your stated intent to expand Facebook's role in the payment ecosystem, including through direct payments within the messaging platform.

Both this approach to connecting ads to your ostensibly privacy-protective messaging platform and your focus on payments raise only further questions about privacy within the messaging platform. A payment system operated by Facebook as an intermediary within an encrypted messaging app is a potential vector for the transmission of sensitive information outside of the supposedly private ecosystem. Facebook touts the privacy and encryption of payment information related to credit cards, and I hope that this encryption will protect users from the leakage of any personal information relating to payments into Facebook's user profiles. Whether it will depends on what, exactly, is encrypted.

Facebook's knowledge of which businesses interact with which users and the conversion of advertisements into encrypted chats between users and advertisers is, itself, sensitive information even in the absence of information transmitted through the content of the encrypted messages occurring within an app. If Facebook knows which businesses its users choose to communicate with through encrypted private messaging and whether such communications are initiated through ads on its non-private platform, it can extrapolate from such conversations information about user preferences that users presume to be private due to Facebook's public presentation of its encrypted chat as a private online space. If Facebook has any knowledge of user transactions thanks to its control of the payment architecture, such extrapolation may be even more precise.

More troublingly, Facebook's effort to gain a share of the market for online payments may threaten to undermine the privacy of encrypted conversations between friends and their acquaintances. Users of other payment platforms use those mechanisms for some of their most sensitive interactions, from rent payments to ride sharing to shared costs for meals. A Facebook that knows which users transact with each other in these ways need not know the precise content of encrypted communication to determine sensitive details of users' lives – details it can further feed into its advertising infrastructure.

- *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?*

- *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?*

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

- *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?*

Groups and Events

In your F8 presentation, you emphasized a shift from the Facebook news feed to groups. You presented this shift in the context of a presentation emphasizing the value to users of private, secure spaces for more valuable and sensitive interactions.

The need for such spaces and the security you promise on your platform has become more apparent in recent months as we have learned more about Facebook's failure to protect sensitive information communicated through its existing group features. Last year, Facebook succumbed to public pressure to close loopholes in its closed group feature allowing membership lists for groups organized around sensitive interests such as shared genetic predisposition to cancer to be downloaded by non-members. At the time, such groups' only recourse was to classify as "secret," a remedy that would render them inaccessible by search and therefore limit users' ability to connect over sensitive shared interests.

Additionally, advertisers have long hoped to increase their ability to target such groups. As recently as this year, before the F8 announcement, industry observers have noted the presence of new options for Facebook advertisers to target such groups, suggesting imminent product changes. Such changes presumably relate to Facebook's greater emphasis on groups relative to the news feed.

Further questions remain about the extent to which Facebook plans to collect and utilize data about those groups, such as group membership, as well as more sensitive data shared within groups to target ads to members within group pages, or to supplement publicly shared information in users' advertising profiles.

Unacknowledged in your presentation is that the very logic that has informed your shift from the news feed to groups is the value of more personalized and private spaces. Users already assume such spaces, given their relative intimacy, provide them safer spaces in which to share sensitive information, even if they are not formally classified as "private messages." The principles that have led to your decision to encrypt private messages necessarily suggest that users of groups – certainly of closed or secret groups – deserve the same protections afforded to users of private messenger. Yet Facebook's suggestion that it will monitor the interactions in such groups for misinformation – just as it does in the public news feed – suggests it takes a different view of these interactions than it hopes its likely users will.

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

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

- *Will it allow advertisement targeted to groups, and will the advertising allowed differ between different categories of groups?*

- *Will data compiled through content shared in groups – especially closed or secret groups – be added to the user profiles compiled to target ads to users throughout the platform?*

- *If Facebook fails to make such guarantees, will it make clear to users of groups – including groups organized around sensitive, personal subjects – that it regards their interactions in such groups as analogous to interactions in its news feed "digital public square"? Or will it muddy the waters between the supposedly private spaces within its platform and the public ones?*

Changes to the Platform and Effect on Publishers

I would be remiss not to address a subject unrelated to the privacy concerns heretofore raised.

The changes Facebook announced recently will have a substantial effect on the flow of digital information. I hope those changes are for the good. Only time will tell. But already we know with certainty that these changes will be disruptive.

As a major online content platform, Facebook holds the fate of America's news publishers in its hands. It has not proven itself a worthy custodian. Publishers have in recent years been victimized by capricious changes to Facebook's algorithm, such as its "pivot to video," which prompted massive shifts in the media industry's productive capacity toward the development of video content at the expense of shoe-leather reporting. Such sudden shifts have led to the collapse of local newspapers and major digital news startups alike.

I hope that in planning these announced changes your platform has accounted for the possibility of its impact on media stakeholders. I fear that you have not – and that newsrooms across the country are already reeling from the launch of your new mobile product.

- *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?*

Your platform has earned immense power. It is unclear that you or your management team deserve the weighty responsibilities that come with it. I wish you the best if your intentions are as you suggest: to promote healthier, safer, more private interactions that enrich all our lives and improve the health of our civic culture. But you long ago lost the benefit of the doubt.

The burden to illustrate that Facebook's products and the changes you announced recently will in time make a positive contribution to American life is on you. The burden to protect the American people from forces parasitic on our national life and on our economy is on me and my colleagues. I take my responsibilities seriously. I hope you do the same for yours. If you do not, you should anticipate policy changes in the years to come to force behavior change on the part of your senior managers, including legislation holding you and your colleagues personally liable for conduct whose consequences currently fall on Facebook's shareholders.

I have copied WhatsApp cofounders Brian Acton and Jan Koum on this message. I suspect their insights about Facebook's approach to privacy and data monetization would be of special interest to the Senate Judiciary Committee, on which I sit, as well as to the public.

I would appreciate a response to this letter by May 27.

Sincerely,

Josh Hawley
United States Senator

CC:

Jan Koum and Brian Acton
Co-founders, WhatsApp