June 29, 2018

Senator Maggie Hassan
U.S. Senate Committee on Commerce, Science, and Transportation
330 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Hassan:

Thank you for your questions for the record from the April 10, 2018 Hearing titled Facebook, Social Media Privacy, and the Use and Abuse of Data. Per your request, attached are the answers for the record for your questions.

Please note that we received over 2,000 questions from the Senate and House Committees before which we testified on April 10 and 11, 2018. We appreciate the time you gave us to respond to these questions. We did our best to review and answer them in the available timeframe. We respectfully request an opportunity to supplement or amend our responses if needed.

Sincerely,

Facebook, Inc.

facebook

Address: 1601 Willow Road
Menlo Park, CA 94025

Committee on Commerce, Science, and Transportation

"Facebook, Social Media Privacy, and the Use and Abuse of Data."

Senator Maggie Hassan

April 10, 2018

Questions for the Record

Question 1.
During the hearing, you stated that you "don't know" whether Facebook employees actively coordinated with Cambridge Analytica as a result of the support Facebook provided directly to the Trump campaign. Representatives from the Trump campaign have extensively detailed how Facebook provided "hands-on" support to the campaign, embedding Facebook employees at the campaign's digital operation center in San Antonio.[1] Cambridge Analytica appears to have had employees nearby, in the same office, at the same time that Facebook employees were embedded there.

- **Was Facebook aware that Cambridge Analytica personnel would be working out of the same Trump campaign office before Facebook agreed to provide support to the campaign at this location? If not, when did someone at Facebook become aware, and what disclosure process was followed internally?**
- **Would Facebook have still provided support if it knew beforehand that it would be working alongside Cambridge Analytica? Once Facebook found out it would be working alongside Cambridge Analytica, what actions did Facebook take?**
- **Have you conducted an internal investigation into the vetting process behind this arrangement with the Trump campaign?**

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

In general, political data firms working on the 2016 campaign had access to Facebook's advertising support services, including technical support, and best practices guidance on how to optimize their use of Facebook. Everyone had access to the same tools, which are the same tools that every campaign is offered.

[1] https://qz.com/1233579/facebook-and-cambridge-analytica-worked-side-by-side-at-a-trump-campaign-office-in-san-antonio/

Question 2.
You stated that Facebook only collected text/call data when people opted-in from Facebook Messenger. Some reports[2] seem to contradict that, with users who reportedly did not download the Messenger app onto a given device seeing their message data from those devices in their Facebook files. Can you clarify this discrepancy?

You also stated that this was done to improve the user experience. Can you explain why it would be necessary to collect not only the contact data from a user's phone, but also the date, time, and length of calls and store that data for years?

Call and text history logging is part of an opt-in feature that lets people import contact information to help them connect with people they know on Facebook and Messenger. We introduced the call and text history component of this feature for Android users several years ago, and currently offer it in Messenger and Facebook Lite, a lightweight version of Facebook, on Android.

Contact importers are fairly common among social apps and serve as a way to more easily find the people users want to connect with. They help users find and stay connected with the people they care about and provide them with a better experience across Facebook.

Before we receive call and text history from people, they specifically grant us permission to access this data on their device and separately agree to use the feature. If, at any time, they no longer wish to use this feature they can turn it off, and all previously shared call and text history shared via that app is deleted. People can also access information they previously imported through the Download Your Information tool.

We've reviewed this feature to confirm that Facebook does not collect the content of messages—and will delete all logs older than one year. In the future, people will only upload to our servers the information needed to offer this feature—not broader data such as the time of calls.

Question 3.
You stated that information sent via WhatsApp is not seen or collected by Facebook, and is never used to inform advertisements. WhatsApp features end-to-end encryption, meaning Facebook has no access to those messages. But other Facebook services such as Messenger or messages on Instagram are not encrypted this way, meaning Facebook does have access to them. Are the content of messages sent through Facebook Messenger or Instagram ever used, or have they ever been used, to inform the placement of advertisements?

Facebook does not analyze the content of photos or text in users' posts or messages to target ads to them using AI or otherwise. Instead, there are a few primary ways that we personalize the ads and sponsored content for people on Facebook, based on:

[2] https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/

- Information from people's use of Facebook. When people use Facebook, they can choose to share things about themselves like their age, gender, hometown, or interests. They can also click or like posts, Pages, or articles. We use this information to understand what users might be interested in and hopefully show them ads that are relevant. If a bike shop comes to Facebook wanting to reach female cyclists in Atlanta, we can show their ad to women in Atlanta who liked a Page about bikes. People can always see the "interests" assigned to them in their ad preferences, and if they want, remove them.

- Information that an advertiser shares with us (or "custom audiences"). In this case, advertisers bring us the customer information so they can reach those people on Facebook. These advertisers might have people's email address from a purchase users made, or from some other data source. If we have matching email addresses, we can show those people ads from that advertiser (although we cannot see the email addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match). In ad preferences people can see which advertisers with their contact information are currently running campaigns—and they can click the top right corner of any ad to hide all ads from that business.

- Information that websites and apps send to Facebook. Some of the websites and apps people visit may use Facebook tools to make their content and ads more relevant, if people consent to let Facebook show them ads based on data from third-party partners. For example, if an online retailer is using Facebook Pixel, they can ask Facebook to show ads to people who looked at a certain style of shoe or put a pair of shoes into their shopping cart. If users don't want this data used to show them ads, they can turn it off in ad preferences.

- Facebook also offers Lookalike Audiences. Advertisers creating a Lookalike Audience choose a source audience (which could include a custom audience as described above, people who have opened or completed a form in lead ads on Facebook, people who have interacted with the advertiser's Facebook page or its Instagram profile). Facebook then identifies common qualities of the people in the source audience (e.g., demographic information or information about their interests), and then identifies people who are similar to them (on the basis of the common signals identified in the source audience), without sharing this information with the advertiser.

Question 4.
What research have you done relating to users' understanding of your policies and/or procedures relating to privacy and/or security of user data?

We do extensive research around our privacy controls, including focus-groups and on-platform surveys. Our research overwhelmingly demonstrates that, while "up front" information like that contained in the terms of service are useful, in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts, a menu

where people can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams", bringing together experts in design, privacy, law, and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design, and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

Question 5.
What percentage of users change their default privacy settings?

There is no single number that measures how much time people spend understanding how Facebook services work, in large part because Facebook seeks, as much as possible, to put controls and information in context within its service.

We've heard loud and clear that privacy settings and other important tools are hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

Question 6.
What types of data or information does Facebook collect and store about non-Facebook users? For what purpose does Facebook collect this data and information?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in – such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an

account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

Question 7.
Some reports have indicated that private messages sent via Facebook may have been accessible to Cambridge Analytica and other third party developers via the first version of the Graph API.[3] Is there merit to those reports? If so, how many users' private messages would have been available through this mechanism?

At the outset, we do not know what data Kogan may have shared with Cambridge Analytica. Our investigation into these matters is ongoing, and we are paused on investigating Cambridge Analytica directly (or conducting a forensic audit of its systems) due to the request of the UK Information Commissioner's Office, which is separately investigating Cambridge Analytica, a UK entity. The best information to date also suggests only US user data was shared by Kogan with Cambridge Analytica.

Approximately 300,000 Facebook users worldwide installed Kogan's app. For the majority of these users, the app requested consent to access the following data fields associated with the user and with the friends of the user: Public profile data, including name and gender; Birthdate; "Current city" in the "About" section of the user's profile, if provided; and Facebook Pages liked.

For a small subset of users, it appears that the app also requested consent to access users' Facebook messages (fewer than 1,500 individuals, based on current information) and to posts that appeared in the user's News Feed or Timeline (approximately 100 individuals, based on current information)—but only for users who installed the app. For a small subset of users (fewer than 1,500 individuals, based on current information), it appears that the app also requested consent to access the hometowns that the users' friends had specified in the "About" section of their profiles. And for a handful of people (fewer than 10) who appear to be associated with Kogan/GSR, the app requested consent to email address and photos.

Question 8.
What steps is Facebook taking to combat the opioid crisis (such as efforts to crack down on the sale of illicit drugs or identify users at risk of addiction)?

Thank you for highlighting this important issue. We have an iterative, proactive process to help prevent opportunities for—and respond quickly to—illicit drug sales on our platforms:

- Our Community Standards make it very clear that buying, selling or trading non-medical or pharmaceutical drugs is not allowed on Facebook. Any time we become

[3] https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747

aware of content on Facebook that is facilitating activity like drug sales, we remove it and have taken numerous measures to minimize the opportunity for these activities to take place on our platform.

- We make it easy for people to flag content for us so that we can quickly review and remove it if it violates. That's why people can report any piece of content on Facebook—profiles, Pages, Groups, individual content and even comments.

- If we identify violating content, we are able to look for associated profiles, Pages, groups, and accounts and remove them.

- We have also made it harder for people to find content that facilitates the sale of opioids on our platform.

- We have removed content that violated our policies that was surfaced in Search.

- We have blocked hundreds of terms associated with drugs sales from being able to surface results on Facebook or only returning links to news about drugs shared for awareness.

- We have removed thousands of terms from being suggested in search—meaning that our systems won't recognize the beginning of the word as it is being typed and suggest what the completed term to search is.

- We continue to look for ways to get faster at finding and removing this content, working across our policy, operations, product, and partnerships team. We also update our detection methods as bad actors work to game the system and bypass our safeguards.

We recently launched a new feature on Facebook so that now, when people search for help with opioid misuse—as well as attempt to buy opioids—they are prompted with content at the top of the search results page that will ask them if they would like help finding free and confidential treatment referrals. This will then direct them to the Substance Abuse and Mental Health Services Administration National Helpline.

The same resources will be available on Instagram in the coming weeks. This is one of a number of ways we are helping connect people with resources and communities to support them.

Question 9.
What process does Facebook use to vet third parties before granting them access to user data?

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to

make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- Review our platform. We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- Tell people about data misuse. We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app for misusing data, we will tell everyone who used it.

- Turn off access for unused apps. If someone has not used an app within the last three months, we will turn off the app's access to their data.

- Restrict Facebook Login data. We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to

control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- Reward people who find vulnerabilities. We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- Update our policies. We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

Question 10.
What steps does Facebook take to monitor third parties who have access to user data?

See Response to Question 9.

Question 11.
Which third parties have improperly accessed or inappropriately used user data, or violated signed agreements with Facebook regarding data? What steps has Facebook taken to remedy these events?

Facebook is in the process of investigating all the apps that had access to large amounts of information, such as extensive friends data (if those friends privacy data settings allowed sharing), before we changed our platform policies in 2014—significantly reducing the data apps could access. Where we have concerns about individual apps, we are investigating them—and any app that either refuses or fails an audit will be banned from Facebook. As of early June 2018, thousands of apps have been investigated and around 200 have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these apps also appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Question 12.
You stated that Facebook is an "idealistic company." Facebook has reportedly sought to build a censorship-friendly app to help enter the Chinese market.[4] Are those reports true? If so, do you consider those actions to be consistent with Facebook's idealism?

Because Facebook has been blocked in China since 2009, we are not in a position to know exactly how the government would seek to apply its laws and regulations on content were we permitted to offer our service to Chinese users. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out

[4] https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html

in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis.

In keeping with these commitments, rigorous human rights due diligence and careful consideration of free expression and privacy implications would constitute important components of any decision on entering China.

Question 13.
We are all grappling with the ability of foreign nations to exploit technology platforms like Facebook to spread propaganda and misinformation. While Facebook does not operate within China, reports have shown that the Chinese government advertises extensively on Facebook to spread propaganda in the U.S. and throughout Southeast Asia. Reports indicate that the Chinese government is the largest advertiser Facebook has in Asia. Do you believe Facebook should be a platform for allowing foreign nations to spread propaganda? Are the Chinese government's propaganda efforts consistent with Facebook's goal of cracking down on misinformation?

Entities can maintain a presence on Facebook as long as they comply with Facebook's policies, including complying with applicable law. We hold all accounts to the same standards, including standards related to authenticity, and we remove accounts and content that violate our policies. For content that does not violate our policies but that is false or misleading, we have begun to work with third-party fact-checking organizations to provide additional information to people who see or share this kind of content. Posts that don't violate Facebook's policies but that are determined to be false or disputed may also appear lower in News Feed and become less likely to be widely distributed. If we become aware that our policies are being violated, we will take action.

We've made important changes to prevent bad actors from using misinformation to undermine the democratic process. Here is a list of the 10 most important changes we have made:

1. Ads transparency. Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

2. Verification and labeling. Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

3. Updating targeting. We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our

principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

4. Better technology. Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

5. Action to tackle fake news. We block millions of fake account attempts each day as people try to create them thanks to improvements in machine learning and artificial intelligence. We are also working hard to stop the spread of false news. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights.

6. Significant investments in security. We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

7. Industry collaboration. Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

8. Information sharing and reporting channels. In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

9. Tracking 40+ elections. In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

10. Action against the Russia-based IRA. In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the

world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

Question 14.
You have stated that users are able to download all of the data that Facebook has about them. Does this include data that Facebook has obtained through means such as cross-web tracking, purchasing data from brokers, and inferential data created with that user data? If not, how can a user access this data?

Every user has a dedicated section in their settings which enables them to access or download their information at any time. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently expanded the tools we provide people for accessing their information, which will now allow people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Question 15.
Before the hearing, Facebook announced an independent election research commission to solicit research on the effects of social media on elections and democracy. Does Facebook plan to solicit similar research on the effects of social media on other important aspects of society, including privacy, mental health and wellbeing, inequality, etc.?

Facebook employs social psychologists, social scientists, and sociologists, and collaborates with top scholars to better understand well-being. Facebook has also pledged $1 million towards research to better understand the relationship between media technologies, youth development and well-being. Facebook is teaming up with experts in the field to look at the impact of mobile technology and social media on kids and teens, as well as how to better support them as they transition through different stages of life. Facebook is committed to bringing people together and supporting well-being through meaningful interactions on Facebook.

Question 16.
Many large institutions have set up independent systems to ensure transparency and internally check bad decisions. Federal agencies have inspectors general and offices to encourage whistleblowing. Many companies have ombudsmen, and some media companies have public editors to help publicly examine and evaluate their choices. Hospitals have ethics boards. What kinds of independent systems does Facebook have? Have you considered setting up an independent entity to help publicly examine and explain your decision-making?

Facebook's Board of Directors acts as the management team's adviser and monitors management's performance. The Board also reviews and, if appropriate, approves significant transactions and develops standards to be utilized by management in determining the types of transactions that should be submitted to the Board for review and approval or notification. The Board of Directors also has an Audit and Risk Oversight Committee with an oversight role.

In addition to the Board's role, Facebook works with outside groups on these issues. For example, Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process—getting feedback directly from civil rights groups, like The Leadership Conference on Civil and Human Rights, and help advise Facebook on the best path forward.

Moreover, Facebook recently announced a new initiative to help provide independent, credible research about the role of social media in elections, as well as democracy more generally. It will be funded by the Laura and John Arnold Foundation, Democracy Fund, the William and Flora Hewlett Foundation, the John S. and James L. Knight Foundation, the Charles Koch Foundation, the Omidyar Network, and the Alfred P. Sloan Foundation. At the heart of this initiative will be a group of scholars who will:

- Define the research agenda;
- Solicit proposals for independent research on a range of different topics; and
- Manage a peer review process to select scholars who will receive funding for their research, as well as access to privacy-protected datasets from Facebook which they can analyze.

Facebook will not have any right to review or approve their research findings prior to publication. More information regarding the study is available at https://newsroom.fb.com/news/2018/04/new-elections-initiative/.

Question 17.
When Facebook comes across terrorist-related content—such as ISIS or al-Qaeda propaganda—does Facebook proactively alert federal law enforcement to the terrorist content? If not, under what circumstances will Facebook alert federal law enforcement about terrorist propaganda on your platform?

We reach out to law enforcement if we learn of content that we believe reflects a credible threat of imminent harm. We have been able to provide support to authorities around the world that are responding to the threat of terrorism, including in cases where law enforcement has been able to disrupt attacks and prevent harm. Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have strict processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We publish more information in our Law Enforcement Guidelines at https://www.facebook.com/safety/groups/law/guidelines/ and Transparency Report at https://transparency.facebook.com/.