June 8, 2018

Chairman Chuck Grassley
Ranking Member Dianne Feinstein
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Dear Chairman Grassley, Ranking Member Feinstein, and Members of the Committee:

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 extra 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

Questions from Senator Booker

1. **In 2016, ProPublica revealed that advertisers could use "ethnic affinity" marketing categories to potentially discriminate against Facebook users in the areas of housing, employment, and credit, in violation of federal law. While you committed in November 2016 to "build tools to detect and automatically disable the use of ethnic-affinity marketing for certain types of ads," a year later ProPublica found that the system you built was still letting housing ads through without applying the new restrictions. It was chalked up to a "technical failure." You then opted for system where advertisers self-certify that they are complying with federal law and Facebook's antidiscrimination policy, but in fact just last month, several fair housing organizations filed a lawsuit against Facebook in the S.D.N.Y. alleging discrimination in housing advertising based not just on race, but also on disability, gender, and familial status. According to the lawsuit, the most recent ad buys were still occurring just weeks ago in late February 2018.**

    a. **Is a self-certification model the strongest way to safeguard against discrimination?**

Our Terms and Advertising Policies have long emphasized our prohibition on the use of Facebook's platform to engage in wrongful discrimination. Starting in late 2016, we began implementing additional protections for the people who use Facebook. Specifically, we set out to help better educate advertisers about our policies against discrimination and relevant federal and state laws, and to help prevent the abuse of our tools. First, we updated our Advertising Policies applicable to all advertisers and advertisements to strengthen our prohibition against discrimination, and we added a section to provide advertisers with antidiscrimination educational resources from government agencies and civil rights groups. Second, we implemented technical measures aimed at better protecting users from wrongful discrimination by advertisers that offer housing, employment and credit opportunities. Specifically, when we identify one of these types of ads, we require the advertiser to certify that it is complying with our anti-discrimination policy and with applicable law. We reject thousands of ads a day where the advertiser fails to certify.

    b. **Would it be better to not serve ads in certain categories (housing/credit/employment) at all?**

We have heard concerns about third party advertisers misusing these tools to engage in wrongful discrimination with respect to ads for housing, credit, and employment by targeting people based on the protected characteristics outlined in your questions. Based on feedback we have received from our community, and from policymakers, regulators, civil rights experts, and consumer advocates, we have limited the targeting options we offer for such advertisements that relate to protected classes as follows:

- We do not offer targeting based on race, religion, disability, sexual orientation, or gender identity.

- We do not offer targeting based on national origin, but we do have segments composed of "ex-pats"—people who used to live in particular countries (and may or may not be from these countries originally).

- We do permit some targeting based on family status (e.g., people who are parents), but we generally do not permit advertisers to exclude people from their audiences based on family status. Please note, however, that in limited cases and for the purpose of running ads that are not related to housing, employment or credit, we are re-enabling the ability of advertisers to exclude people from their audiences based on family status but are reviewing this as a targeting option.

- Like other major ad platforms, we enable targeting based on age and gender.

- We offer targeting options—called "interests" and "behaviors"—that are based on people's activities on Facebook, and when, where and how they connect to the Internet (such as the kind of device they use and their mobile carrier). These options do not reflect people's personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them. For example, we do not create interest or behavior segments that suggest the people in the segment are members of sensitive groups such as particular races, ethnicities, or religions. We therefore would not create an interest segment called "Muslims," because it could be misunderstood to enable an advertiser to reach people based on their religious beliefs.

- We also offer what we call the multicultural affinity segments, which are groups of people whose activities on Facebook suggest they may be interested in content related to the African American, Asian American, or Hispanic American communities. (For example, if a person "likes" Facebook Pages with the words "African American" in them or likes Pages for Historically Black Colleges and Universities, that person may be included in the African American multicultural segment.) As we explain to advertisers in our tools, these segments are based on people's activities on Facebook, not on race or ethnicity (which categories Facebook does not enable people to even include on their profiles).

- We have gone even further when it comes to using the "exclude" feature in our ads tools. This feature is designed to help advertisers refine their audiences by, for example, excluding people who are already interested in their products. But we recognize that permitting exclusions could, in some circumstances, raise the risk that an advertiser would engage in wrongful discrimination. For that reason, many of the targeting audiences that advertisers can choose to include in the group eligible to see their ad are not available for exclusion. For example, while we believe it is important that organizations be able to affirmatively reach people in the multicultural affinity segments, advertisers are not able to exclude people from their audiences based on the multicultural affinity segments.

- We also recently added a notice below the "exclude" field that reminds advertisers of their obligations under our non-discrimination policy as well as under relevant

applicable law in a persistent manner when they create their advertisements and define their audiences.

- In early 2017, we launched machine learning tools (called "classifiers") that were intended to automatically identify, once an ad was entered into our systems, employment, credit, and housing ads. We built these classifiers so that when one of these kinds of ads was identified, we could take two actions that would make it harder for advertisers to misuse our tools.

c. Given your inability to fix something as straightforward as discriminatory housing ads, why should Congress trust Facebook's ability to target and reduce suspicious election activity?

These industry-wide problems are not easy to solve, but we are committed to doing better by implementing the steps outlined throughout this document.

d. How does Facebook prevent advertisers from using their own data to segment users by race or other protected categories using Facebook's Custom Audiences feature?

See Response to Question 1, part c.

2. In responding to a November 2016 class action lawsuit against Facebook for discrimination in housing, employment, and credit, Facebook moved to dismiss the complaint on the basis that the plaintiffs were not injured.

a. Do you believe that people of color who are not recruited for various economic opportunities are harmed by not hearing about those opportunities?

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running a housing ad—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

3. A 2016 investigation by the ACLU of California revealed that another app developer, Geofeedia, was using data from Facebook and other platforms to help law enforcement monitor the activities of peacefully protesting civilians of color. In response, Facebook changed its policy to prohibit any developers from facilitating the surveillance of Facebook users.

a. You have endorsed Black Lives Matter and expressed sympathy after Philando Castile's killing, which was broadcast on Facebook Live. Despite this, why should communities of color trust Facebook has sufficiently addressed this surveillance issue?

b. Is simply changing the language of your terms of service enough? Have you taken any other steps to prevent another Geofeedia from attempting something similar?

In March 2017, we added language to our Facebook and Instagram platform policies to more clearly explain that developers cannot use data obtained from us to provide tools that are used for surveillance. Our previous policy limited developers' use of data but did not explicitly mention surveillance. We found out that some developers created and marketed tools meant for surveillance, took action, and we clarified our policy.

Questions from Senator Coons

1. **In 2015, Facebook learned that Aleksandr Kogan sold users' data he obtained from an application to the political consulting firm Cambridge Analytica in violation of Facebook's terms of service. Facebook did not publicly disclose that Cambridge Analytica obtained this user data until 2018, after public reports that Kogan had improperly sold the data to Cambridge Analytica.**

    a. **Why did you fail to tell the public until March 2018 that Kogan sold the data to Cambridge Analytica?**

    b. **Who specifically at Facebook made the decision not to tell the public that millions of users' data was obtained by Cambridge Analytica without their consent?**

    c. **Your announcement that at least 87 million users had their privacy violated came out only recently. In 2015, did you try to determine the universe of users whose privacy was violated?**

    d. **How long have you known the number of affected users was in the millions?**

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their newsfeed.

2. **In your testimony for the hearing, you noted, "In 2015, we learned from journalists at *The Guardian* that Kogan had shared data from his app with Cambridge Analytica."**

    a. **Prior to learning this from *The Guardian*, what steps was Facebook taking to ensure that developers were not selling data to third parties in violation of the site's terms of service?**

Since 2014, Facebook has proactively reviewed any app seeking to obtain extended permissions to data beyond a basic set of data, and it has rejected more than half of the apps seeking these permissions. Before we learned about the *Guardian* allegations and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals.

b. Why did Facebook wait until eight months after *The Guardian*'s report about Cambridge Analytica to send a letter asking for certification that the data was deleted?

Facebook did not wait until eight months after *The Guardian*'s report about Cambridge Analytica to seek assurance that the data was deleted. Facebook contacted Cambridge Analytica the day the article was released. About one month later, on January 18, 2016, Cambridge Analytica assured Facebook in writing that it had deleted the data received from Kogan/GSR and that their server contained no backups of the data.

c. If it were not for *The Guardian*'s reporting, would you have learned that Kogan sold the data to Cambridge Analytica? If yes, how?

We learned from journalists at *The Guardian* that Kogan may have shared data from his app with Cambridge Analytica. We would have acted in response to any external report, user report, or other signal to investigate these allegations and take appropriate action.

d. It is likely that there will not always be a newspaper reporting on every application developer that improperly sells user data. Has Facebook ever proactively (i.e., without being alerted by another party) learned about a similar violation of its terms of service – selling or transferring user data without consent to a third party – and if so, how? How many other such instances have you discovered?

We regularly take enforcement action against apps. For example, in 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform.

As part of the app investigation and audit we announced in March, we have suspended 200 apps, 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.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

3. Why did Facebook only recently suspend Cambridge Analytica's and Aleksandr Kogan's Facebook accounts when you knew about the illicit transfer of user data back in 2015?

a. Why did Facebook fail to take legal action back in 2015 when it learned from *The Guardian* that Kogan sold the data to Cambridge Analytica?

b. After Cambridge Analytica's acquisition of data came to Facebook's attention in 2015, did any policy or process change within your company in response? Please describe any such changes and when they occurred.

See Response to Question 1.

4. In 2014, Facebook stopped allowing applications access to the profiles of a user's friends, but for applications like Aleksandr Kogan's, you still allowed access to friends' data for another year. Why did Facebook permit other applications continued access to that data for another year?

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. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs.

5. Can you now confirm that Cambridge Analytica and its partners, AggregateIQ and Strategic Communications Laboratories, have deleted the Facebook data they received from Aleksandr Kogan? If not, why not?

a. Has Facebook ever attempted to prevent Cambridge Analytica from offering products or services that rely on or use the data it improperly obtained from Kogan?

b. Is there anything that will prevent Cambridge Analytica from offering products or services that rely on or use the illicitly acquired Facebook data in the 2018 and 2020 elections?

Facebook obtained written certifications from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all data they had obtained, and any derivatives, was accounted for and destroyed. Based on recent allegations, we have reopened our investigation into the veracity of these certifications and have hired a forensic auditor to conduct a forensic audit of Cambridge Analytica's systems. We are currently paused on the audit at the request of the UK Information Commissioner's Office request, which is conducting a regulatory investigation into Cambridge Analytica (based in the UK), and we hope to move forward with that audit soon.

We have suspended SCL/Cambridge Analytica from purchasing advertising on Facebook as well as removed the personal accounts of some of their officers.

6. You wrote in your testimony that, in March 2018, Facebook hired a firm to conduct a forensic audit of Cambridge Analytica and Kogan. Why did Facebook wait until March of 2018 to conduct an audit of Cambridge Analytica's and Kogan's systems to

ensure the data was destroyed, when the company has known for three years that the data was misappropriated?

Facebook knew about Cambridge Analytica in 2015, when Facebook banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed.

We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned that questions had been raised concerning the accuracy of the certifications. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook (and there was no intention of considering its reinstatement). Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future.

Facebook, and Mr. Zuckerberg, became aware from media reporting in March 2018 that the certifications we received may not have been accurate. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers.

7. In an interview with CBS's *60 Minutes*, Aleksandr Kogan estimated that "tens of thousands" of application developers had similar access to their participants' friends' profiles.

a. Approximately how many other application developers had access to their users' friends' profiles, like Kogan?

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. To date 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.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we changed our platform to reduce data access. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

b. Has Facebook ever learned of an application developer other than Kogan transferring or selling user data without user consent and in violation of Facebooks terms of service to a third party?

The ability for app developers to share data entrusted to them is an industry-wide challenge, which impacts every major app platform. We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and among other things, analyze potentially suspicious activity from our analysis of logs and usage patterns by these apps. Where we have concerns, we will conduct an audit using internal and external experts and ban any developer that refuses to comply. If we identify misuses of data, our enforcement actions may include banning the app from our platform and pursuing legal action if appropriate.

8. Have there been instances in which Facebook discovered misuse of user data by application developers in any way other than transferring or selling data without user consent?

a. If so, how many additional instances does Facebook currently know about?

b. Have you notified any users in these cases? If not, will you commit to doing so?

c. Will you commit to publicly announcing and notifying users of every future violation of Facebook's terms of service by application developers?

We are in the process of investigating every app that had access to a large amount of information before we changed our platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

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 suspensions include apps that 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.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

9. ***The Guardian*** **recently reported that Joseph Chancellor, former co-director of Aleksandr Kogan's company, Global Science Research (GSR), has been working as a quantitative social psychologist at Facebook since 2015. In an interview for CBS's *60 Minutes*, Kogan was asked whether Chancellor had anything to do with the study he did for Cambridge Analytica. He replied, "Yeah. I mean, we did everything together."**

    a. **Does Facebook continue to employ Chancellor, knowing since 2015 that he was involved in GSR's harvesting and sale of Facebook data to Cambridge Analytica? If so, why?**

    b. **Facebook banned Aleksandr Kogan's account and required that he certify the user data he harvested was deleted. Did Facebook take similar actions against Chancellor? If not, why not?**

We are investigating Mr. Chancellor's work with Kogan/GSR.

10. **Cambridge Analytica whistleblower Christopher Wylie testified to the U.K. House of Commons that Russian intelligence agencies easily could have put a key logger in Aleksandr Kogan's computer during his regular trips to Russia to get his psychological profiles of Americans. Is Facebook aware of whether Russia or other foreign governments accessed Kogan's data?**

We are not aware of any evidence to suggest that Kogan shared data obtained through his app with Russia or other foreign governments, but our investigation is ongoing.

    a. **Is Facebook aware of any instances in which foreign governments accessed user data from third-party application developers?**

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014.

    b. **What steps is Facebook taking to ensure that foreign governments cannot access the private information of U.S. citizens held by application developers?**

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. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. 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.

c. Is there a way for Facebook to affirmatively track Facebook data that application developers download from the platform such that you know when that data has been improperly accessed or transferred?

See Response to Question 10, part b.

11. Why did Facebook threaten *The Guardian* with legal action after it sought to publish an interview with former Cambridge Analytica employee Christopher Wylie? Has Facebook ever taken legal action against a current or former employee who attempted to, or did, expose violations of user agreements?

Facebook did not threaten to sue *The Guardian*. We sent *The Guardian* a letter to correct some facts in the article they sought to publish. Facebook supports vocal, independent journalism.

12. Facebook sends employees or affiliates to work as consultants with campaigns to help shape digital strategy, content, and execution. Do you plan to embed such Facebook consultant embeds in major political campaigns in the 2018 and 2020 elections? If yes, what will Facebook instruct such consultant embeds about their responsibility to monitor for improper uses of Facebook user data or breaches of the Facebook user agreement?

We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform.

a. Were any of Facebook's consultant embeds in 2016 aware of the user data improperly acquired by Cambridge Analytica?

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.

b. Did Facebook consultant embeds work with Cambridge Analytica in shaping strategy for any U.S. campaigns in 2016?

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.

13. In 2011, Facebook entered into a binding consent decree with the FTC, in which it promised to get users' consent before sharing their data with third parties. Yet, as late as 2015, app developers had access to the Facebook profiles of the friends of users who downloaded their apps, without the friends' knowledge or consent. Why did Facebook permit this even after entering into the consent decree with the FTC?

a. In the consent decree, Facebook further agreed to report any unauthorized access to data to the FTC. Did Facebook ever report to the FTC that Cambridge Analytica accessed the profiles of at least 87 million Facebook users without Facebook's authorization or those users' consent?

b. If not, why not, and who made the decision that this did not have to be reported to the FTC?

We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however.

Instead, and among other things, the consent order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook (i) accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers at all times; (ii) honored the restrictions of all privacy settings that covered developer access to data (including settings that allowed people to turn off the ability of their friends to share their data with apps); and (iii) implemented a comprehensive privacy program build on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

The Consent Order does not contain ongoing reporting obligations to the FTC of the sort suggested in this question. Moreover, Kogan was authorized to access all data that he obtained through Facebook's platform by the people who authorized his app, and no data was shared with Kogan relating to friends who had enabled settings preventing their data from being shared with apps by their friends.

14. Last year, Facebook generated almost $40 billion in advertising revenues. How much is Facebook spending on data privacy and security?

a. How much is Facebook spending to ensure compliance with civil rights laws?

We do not have a single budget line-item for these efforts.

b. The NAACP, Muslim Advocates, the Leadership Conference, the Southern Poverty Law Center, and over a dozen other civil rights organizations asked for a third-party civil rights audit of Facebook's policies in October 2017. Will you commit to hiring an independent third party to conduct an audit focused on civil rights and privacy?

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.

15. Does Facebook use artificial intelligence to analyze content posted by users in order to assist in the creation of targeted advertisements? How many individuals are involved in reviewing advertisements that are targeted using personal information?

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:

- **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.

We have thousands of people whose job it is to help review ads for compliance with our policies. We recently announced that we are hiring thousands of additional reviewers this year.

16. Would it be possible to create a one-click way for a Facebook user to opt out of targeted advertising?

a. Why did you decide not to offer that option to users?

b. Will you commit to offering that option in the future?

c. Have you considered creating a one-click way for a user to prevent Facebook from collecting and storing data beyond what individual users elect to post?

Users can't opt out of seeing ads altogether because selling ads are what keep Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads.

Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories."

17. What do Facebook and its subsidiary companies consider "private" information that is not collected or used for advertising purposes? Is there any content that users provide or post that Facebook does not analyze or review for advertising purposes?

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use data from each of the categories described above to obtain these interests and to personalize every aspect of our services, which is the core value we offer and the thing that makes Facebook services unique from other online experiences. This includes selecting and ranking relevant content, including ads, posts, and Page recommendations, to cite but a few examples.

For example, we use the data people provide about their age and gender to help advertisers show ads based on those demographics but also to customize the pronouns on our site and deliver relevant experiences to those users.

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, so we can rank posts relating to those interests higher in NewsFeed, for example, or enable advertisers to reach audiences—i.e., groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them organic posts from friends who have been in that location or we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of email addresses of people they would like to reach on Facebook. 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).

Again, for people who are new to Facebook, we may have minimal data that we can use to personalize their experience, including their News Feed, their recommendations and the content (organic and sponsored) that they see. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls.

In addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

18. If a user leaves Facebook and affirmatively deletes his/her account, do you destroy his/her data?

a. What, if any, information is retained after a user profile is deleted?

b. If any data is retained by Facebook, what is that data used for?

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

19. At your hearing before the House Committee on Commerce and Energy, when asked by Representative Gene Greene if you would "commit today that Facebook will extend the same protections to Americans that Europeans users will receive under the GDPR," you replied: "Yes Congressman, we believe that everyone around the world deserves good privacy controls. We've had a lot of these privacy controls in place for years, the GDPR requires us to do a few more things, and we're going to extend that to the world." However, *Reuters* recently reported that, before the GDPR becomes effective in the EU in May, you plan to move non-European users' data – including profile data on 1.5 billion users from Africa, Asia, Australia, and Latin America – from Ireland to Silicon Valley in order to "reduce exposure" to the GDPR (*available at* https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook- to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P).

a. Can you confirm that the reason you are moving 1.5 billon users' data is to avoid unnecessary exposure to the GDPR?

No, that is not the reason. The change referred to in this question involves the legal entity with which Facebook users contract when they use the service, which changed in some jurisdictions as a part of the most recent updates to our Terms of Service and Data Policy. This change did not impact people who live in the United States, who contract with Facebook, Inc. under both our new and old policies.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer (DPO) or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU.

We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

b. Do you agree that such a move fails to show your willingness to apply stronger privacy controls and practices to all of your users?

No. See the answer above. In addition, the controls and settings that Facebook is enabling as part of GDPR are already available to other users around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We also provide the same tools for access, rectification, erasure, data portability and others to users in the US and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

c. Is your response to Representative Greene at your hearing, that you were "going to extend [the things required by the GDPR] to the world," consistent with Facebook's actions to relocate massive amounts of user data outside of the EU following your hearings?

We are not relocating people's data. To enable people to access Facebook globally and communicate with people throughout the world, we maintain data centers in multiple locations around the world. We typically store people's information in multiple data centers, and that is not changing. We are instead changing the entity that provides the service for users outside of Europe and North America to Facebook, Inc., for the reasons set forth above. We are offering the same controls and settings to people everywhere.

20. Facebook continues to find Russian trolls operating on your platform. At your hearing, you stated, "just last week, we were able to determine that a number of Russian media organizations that were sanctioned by the Russian regulator were operated and controlled by this Internet Research Agency." Hate groups thrive on Facebook even though your policies prohibit hate speech and glorifying violence. Fake duplicate profiles of real users frequently appear on the site in spite of Facebook policy prohibiting them. This recently happened to me, and I had to alert Facebook in order to have this false profile taken down. Why does Facebook shift the burden to its users to flag inappropriate content—is it not Facebook's job to protect its users?

Facebook does not "shift the burden" to users to flag inappropriate content, though we encourage people to report posts to help us find and take action on inappropriate content. Advances in technology, including in artificial intelligence, machine learning, and computer vision mean that we can now remove bad content faster, get to more content, and increase the capacity of our review team. It has taken time to develop this software—and we're constantly pushing to improve it. We do this by analyzing specific examples of bad content that have been reported and removed to identify patterns of behavior. These patterns can then be used to teach our software to proactively find other, similar problems. But understanding the context of speech, for example, often requires human eyes—is something hateful, or is it being shared to condemn hate speech or raise awareness about it? We've started using technology to proactively detect something that might violate our policies, starting with certain languages such as English and Portuguese. Our teams then review the content so what's OK stays up, for example someone describing hate they encountered to raise awareness of the problem.

a. Is Facebook's artificial intelligence technology capable of automatically flagging fake profiles?

Claiming to be another person violates our Community Standards, and we want to make it harder for anyone to be impersonated on our platform. Users can also report accounts that are impersonating them. We've developed several techniques to help detect and block this type of abuse. At the time someone receives a friend request, our systems are designed to check whether the recipient already has a friend with the same name, along with a variety of other factors that help us determine if an interaction is legitimate. Further, we recently announced new features that use face recognition technology that may help detect when someone is using another user's image as their profile photo—which helps stop impersonation. This is an area we're continually working to improve so that we can provide a safe and secure experience on Facebook.

b. Is there currently any automated system in place for flagging fake profiles or fake news articles at Facebook?

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.

c. If yes, do Facebook employees review every such potentially fake profile or news article that these systems flag?

Not every fake account that has been disabled is reviewed as the volume is simply too great (Facebook took action on approximately 583 million fake accounts in the first three months of 2018). But our engineers carefully test and retest the accuracy of the policies and rules they implement to identify and disable fake accounts.

d. Do Facebook employees manually search for fake content, or is the function of flagging fake or inappropriate content left solely to users and automated systems?

See Response to previous question (Question 20, part c).

21. Special Counsel Robert Mueller's indictment of 13 Russian individuals and three Russian companies states that the Russians have engaged in "'information warfare against the United States of America' through fictitious U.S. personas on social media platforms," including Facebook. As a U.S. company, do you have an obligation to prevent your platform from being used as a weapon against our democracy?

a. What are you doing to prevent Facebook from being used for information warfare in the 2018 election and beyond?

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative, and well-funded adversaries. But we are making steady progress. 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 can already see all the ads that a Page is running on Facebook—and we're launching this globally in June.

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.

b. Have you made any attempt to identify Russian political advertisements or troll accounts that are not associated with the Internet Research Agency?

Facebook has conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by using Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite efforts by these accounts to mask the provenance of their activity. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

22. Do you have the technology or capability to detect when a foreign entity is attempting to buy a political ad?

Now all election and issue ads on Facebook and Instagram in the US must be clearly labeled—including a "Paid for by" disclosure from the advertiser at the top of the ad. This will help ensure that people can see who is paying for the ad—which is especially important when the Page name doesn't match the name of the company or person funding the ad. This also meets the commitments we made back in October 2017 to increase the transparency of the election-related ads people see on Facebook.

When people see that label, it means the person running the ad went through the authorization process and verified his or her identity and location. We believe this new level of

transparency is good for people, and it will allow journalists, researchers, NGOs and others to hold campaigns, candidates and organizations accountable for the ads they create. And all people on Facebook, no matter where they live, will also be able to access and review a searchable archive that will house these ads for seven years from the day they run. More information about our transparency efforts can be found at our recent Newsroom post here: https://newsroom.fb.com/news/2018/05/hard-questions-political-ads.

Moreover, Facebook's Statement of Rights and Responsibilities (the terms that govern all use of our services) prohibit using Facebook to do anything that is unlawful, misleading, or malicious. In addition, advertisers must comply with Facebook's Advertising Policies, including acknowledging that they are responsible for understanding and complying with all applicable laws and regulations. Therefore, violating the Federal Election Campaign Act also violates our terms.

We also have processes designed to identify inauthentic and suspicious activity and we also maintain a sanctions compliance program to screen advertisers and paid app developers. Facebook's denied party screening protocol involves checking paid app developers and advertisers against applicable denied party listings. Those screened remain in an on-going monitoring portfolio and are screened against changes to applicable denied party listings. Moreover, our payments subsidiaries file Suspicious Activity Reports on developers of certain apps as appropriate. However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer. In addition, the general challenge of attributing online activities to specific governments or organizations is widely recognized in the intelligence and law enforcement communities.

a. If so, do you have any procedures to inform U.S. enforcement agencies when a foreign entity is attempting to buy a political ad or when it may be taking other steps to interfere in an election?

In general, we have a long history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform. We deeply respect and value the seriousness, diligence, and support of those organizations, and we would welcome their partnership as we work to address this specific threat. We are particularly encouraged by the FBI's creation of a task force dedicated to addressing election interference and we are actively working with that newly-formed body. This is a new kind of threat, and we believe that we will need to work together—across industry and between industry and government—to be successful.

b. What trends have you discovered with respect to the rate at which foreign entities are attempting to interfere in our elections? Is this tactic becoming more prevalent over time?

See Response to Question 21, part b.

Questions from Senator Cruz

I. Directions

Please provide a wholly contained answer to each question. A question's answer should not cross-reference answers provided in other questions.

If a question asks for a yes or no answer, please provide a yes or no answer first and then provide subsequent explanation. If the answer to a yes or no question is sometimes yes and sometimes no, please state such first and then describe the circumstances giving rise to each answer.

If a question asks for a choice between two options, please begin by stating which option applies, or both, or neither, followed by any subsequent explanation.

If you disagree with the premise of a question, please answer the question as-written and then articulate both the premise about which you disagrees and the basis for that disagreement.

If you lack a basis for knowing the answer to a question, please first describe what efforts you undertook as Chief Executive Officer of Facebook order to ascertain an answer to the question and then provide your tentative answer as a consequence of its reasonable investigation. If even a tentative answer is impossible at this time, please state what efforts you and Facebook intend to take to provide an answer in the future and give an estimate as to when the Committees shall receive that answer.

If it is impossible to answer a question without divulging confidential or privileged information, please clearly state the basis for confidentiality or privilege invoked and provide as extensive an answer as possible without breaching that confidentiality or privilege. For questions calling for answers requiring confidential information, please provide a complete answer in a sealed, confidential form. These materials will be kept confidential. For questions calling for privileged information, please describe the privileged relationship and identify the privileged documents or materials that, if disclosed, would fully answer the question.

If the answer to a question depends on one or more individuals' memory or beliefs and that individual or those individuals either do not recall relevant information or are not available to provide it, please state the names of those individuals, what efforts you undertook to obtain the unavailable information, and the names of other individuals who may have access to that information.

To the extent that an answer depends on an ambiguity in the question asked, please state the ambiguity you perceive in the question and provide multiple answers which articulate each possible reasonable interpretation of the question in the light of the ambiguity.

To the extent that a question inquires about you or Facebook's actions, omissions, or policies, the question also asks about any entities that you or Facebook owns or controls, including any subsidiaries and affiliates. If context suggests that a question may ask

about Facebook as a service rather than as an entity, please answer the question as applied to both Facebook as a service as well as all of Facebook's affiliated entities or platforms.

II. Questions

1) **Please attach a copy of each and every formal or informal policy, whether presently written or otherwise, regarding the moderation, promotion, evaluation, or alteration of users or content on Facebook. These include, for example, Facebook's Terms of Service, its Community Guidelines, and similar policies.**

Facebook's Terms and Policies are available here: https://www.facebook.com/policies. Facebook's Community Standards are available at https://www.facebook.com/communitystandards/.

2) **Yes or no: Are Facebook's decisions to permit users access to its services or to permit content to remain displayed on its services, or the prominence or accessibility of that content, including its order, visibility, duration visible, inclusion in searches or order within search results, inclusion within "Trending" lists or analogous suggestions of content to users, determined in whole or part by Facebook's corporate values, beliefs, priorities, or opinions?**

   a) **Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of the social value or social desirability of that content?**

   b) **Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of that content's truth or falsity?**

   c) **Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of the content's agreement or disagreement with Facebook's corporate values, beliefs, priorities, or opinions?**

The conversations that happen on Facebook reflect the diversity and free expression of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.

With regard the order and visibility of content, a user's News Feed is made up of stories from their friends, Pages they've chosen to follow and groups they've joined. *Ranking* is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available *inventory* of stories; the *signals*, or data points that can inform ranking decisions; the *predictions* we make, including how likely we think they are to comment on a story, share with a friend, etc.; and a *relevancy score* for each story.

Misleading or harmful content on Facebook comes in many different forms, from annoyances like clickbait to hate speech and violent content. When we detect this kind of content in News Feed, there are three types of actions we take: remove it, reduce its spread, or inform people with additional context.

Our Community Standards and Ads Policies outline the content that is not allowed on the platform, such as hate speech, fake accounts, and praise, support, or representation of terrorism/terrorists. When we find things that violate these standards, we remove them. There are other types of problematic content that, although they don't violate our policies, are still misleading or harmful and that our community has told us they don't want to see on Facebook—things like clickbait or sensationalism. When we find examples of this kind of content, we reduce its spread in News Feed using ranking and, increasingly, we inform users with additional context so they can decide whether to read, trust, or share it.

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

(1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.

(2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and

(3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

3) Yes or no: Have Facebook's decisions to permit users access to its services or to permit content to remain displayed on its services, or the prominence or accessibility of that content, including its order, visibility, duration visible, inclusion in searches or order within search results, inclusion within "Trending" lists or analogous suggestions of content to users, ever been determined in whole or part by Facebook's corporate values, beliefs, priorities, or opinions?

See Response to Question 2.

a) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of the social value or social desirability of that content?

See Response to Question 2.

b) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of that content's truth or falsity?

See Response to Question 2.

c) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of the content's agreement or disagreement with Facebook's corporate values, beliefs, priorities, or opinions?

See Response to Question 2.

4) Yes or no: Does Facebook employ its corporate values, beliefs, priorities, or opinions when deciding what content Facebook removes, republishes, moderates, promotes, or otherwise increases or decreases access to content?

The conversations that happen on Facebook reflect the diversity of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.

We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. That's why we have developed a set of Community Standards that outline what is and is not allowed on Facebook. Our Standards apply around the world to all types of content. They're designed to be comprehensive—for example, content that might not be considered hate speech may still be removed for violating our bullying policies.

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

(1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.

(2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and

(3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

5) **Yes or no: Has Facebook ever employed its corporate values, beliefs, priorities, or opinions when deciding what content Facebook removes, republishes, moderates, promotes, or otherwise increases or decreases access to content?**

See Response to Question 4.

6) **It has become a common position on colleges and universities that statements which a listener disagrees with severely either can constitute violence or can rise to the moral equivalent of violence. According to this position, statements may rise to the level of violence even without a threat, reasonable or otherwise, of imminent violence, the use of "fighting words," or either a subjective intent or reasonably understood objective attempt to harass a listener.**

    a) **Yes or no: Does Facebook believe that speech neither advocating for physical violence against, threatening physical violence against, nor undertaken with either the subjective purpose or objective indicia of harassing a listener, may constitute violence?**

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture.

On the subject of credible violence, our Community Standards are explicit in what we don't allow. We aim to prevent potential real-world harm that may be related to content on Facebook. We understand that people commonly express disdain or disagreement by threatening or calling for violence in facetious and non-serious ways. That's why we try to consider the language, context and details in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, we may also consider additional information like a targeted person's public visibility and vulnerability. We remove content, disable accounts, and work with law enforcement when we believe there is a genuine risk of physical harm or direct threats to public safety.

    b) **Yes or no: Has Facebook ever believed that speech neither advocating for physical violence against, threatening physical violence against, nor undertaken with either the subjective purpose or objective indicia of harassing a listener, may constitute violence?**

See Response to Question 6(a)

7) **Regardless of Facebook's answer to Question 7, have any of Facebook's policies ever required removal of content not described in Question 7 from Facebook? If so, what categories, and based on what policies?**

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

(1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.

(2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and

(3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

8) **Yes or no: Does Facebook consider itself a publisher or speaker entitled to First Amendment protection when supervising its services, designing or implementing its policies, altering, reposting, promoting or demoting content, including through results displayed by a user search, their order or presence in a "Trending" list or similar suggestions to users regarding content?**

Facebook does not create the content that users share on its Platform, although it does take steps to arrange, rank and distribute that content to those who are most likely to be interested in it, or to remove objectionable content from its service. These activities are protected functions under Communications Decency Act Section 230 and the First Amendment.

9) **Aside from content clearly marked as coming from Facebook or one of its officers or employees, under what circumstances does Facebook consider itself as acting as a First- Amendment-protected publisher or speaker in its moderation, maintenance, or supervision over its users or their content?**

We are, first and foremost, a technology company. Facebook does not create or edit the content that users publish on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content according to published community standards in order to keep users on the platform safe, to reduce objectionable content and to make sure users participate on the platform responsibly.

10) **Yes or no: Does Facebook provide access to its services on a viewpoint-neutral basis? For this question and its subparts, please construe "access to its services" and similar phrases broadly, including the position or order in which content is displayed on its services, the position or order in which users or content show up in searches (or whether they show up at all), whether users or content are permitted to**

purchase advertisements (or be advertised), the rates charged for those advertisements, and so on.

We are committed to free expression and err on the side of allowing content. When we make a mistake, we work to make it right. And we are committed to constantly improving our efforts so we make as few mistakes as humanly possible.

Decisions about whether to remove content are based on whether the content violates our Community Standards.

Discussing controversial topics or espousing a debated point of view is not at odds with our Community Standards, the policies that outline what is and isn't allowed on Facebook. We believe that such discussion is important in helping bridge division and promote greater understanding.

We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available here: https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

a) Yes or no: Has Facebook ever discriminated among *users* on the basis of viewpoint when determining whether to permit a user to access its services? If so, please list each instance in which Facebook has done so.

See Response to Question 10.

i) If so, does Facebook continue to do so today, or when did Facebook stop doing so?

See Response to Question 10.

ii) If so, what viewpoint(s) has Facebook discriminated against or in favor of? In what way(s) has Facebook done so?

See Response to Question 10.

iii) If so, does Facebook act only on viewpoints expressed on Facebook, or does it discriminate among users based on viewpoints expressed elsewhere? Has Facebook ever based its decision to permit or deny a user access to its services on viewpoints expressed off Facebook?

See Response to Question 10.

b) Yes or no: Excluding content encouraging physical self-harm, threats of physical violence, terrorism, and other content relating to the credible and imminent physical harm of specific individuals, has Facebook ever discriminated among *content* on the basis of viewpoint in its services? If so, please list each instance in which Facebook has done so.

See Response to Question 10.

c) Yes or no: Has Facebook ever discriminated against American users or content on the basis of an affiliation with a religion or political party? If so, please list each instance in which Facebook has done so and describe the group or affiliation against which (or in favor of which) Facebook was discriminating.

See Response to Question 10.

d) Yes or no: Has Facebook ever discriminated against any American users or content on its services on the basis of partisan affiliation with the Republican or Democratic parties? This question includes advocacy for or against a party or specific candidate or official. If so, please list each instance and the party affiliation discriminated against.

See Response to Question 10.

e) Yes or no: Has Facebook ever discriminated against any American users or content on its services on the basis of the user's or content's advocacy for a political position on any issue in local, State, or national politics? This question includes but is not limited to advocacy for or against abortion, gun control, consumption of marijuana, and net neutrality.

See Response to Question 10.

f) Yes or no: Has Facebook ever discriminated against any American users or content on its services on the basis of the user's or content's religion, including advocacy for one or more tenets of that religion? If so, please list each such instance in which Facebook has done so and identify the religion, religious group, or tenet against which Facebook discriminated.

See Response to Question 10.

11) Yes or no: Has Facebook ever discriminated between users in how their content is published, viewed, received, displayed in "trending" or similar lists, or otherwise in any function or feature, based on the user's political affinity, religion, religious tenets, ideological positions, or any ideological or philosophical position asserted? If so, please list each such incident as well as the basis on which Facebook discriminated against that user or content.

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do.

Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

When allegations of political bias surfaced in relation to Facebook's Trending Topics feature, we immediately launched an investigation to determine if anyone violated the integrity of the feature or acted in ways that are inconsistent with Facebook's policies and mission. We spoke with current reviewers and their supervisors, as well as a cross-section of former reviewers; spoke with our contractor; reviewed our guidelines, training, and practices; examined the effectiveness of operational oversight designed to identify and correct mistakes and abuse; and analyzed data on the implementation of our guidelines by reviewers.

Ultimately, our investigation revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature. In fact, our analysis indicated that the rates of approval of conservative and liberal topics are virtually identical in Trending Topics. Moreover, we were unable to substantiate any of the specific allegations of politically-motivated suppression of subjects or sources, as reported in the media. To the contrary, we confirmed that most of those subjects were in fact included as trending topics on multiple occasions, on dates and at intervals that would be expected given the volume of discussion around those topics on those dates.

Nonetheless, as part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.

We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.

We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

We have launched an appeals process to enable people to contest content decisions with which they disagree.

We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

12) Except for accidental instances, has Facebook ever removed, downgraded, concealed, or otherwise censored content associated with any of the following? If yes, please describe the content that was removed, downgraded, concealed, or otherwise censored and the circumstances under which it was removed, downgraded, concealed, or otherwise censored.

a. Any individuals employed by Facebook?

b. Any elected official or candidate seeking elected office who self-identifies or is registered as a Democrat or a "Democratic Socialist"?

c. Any group who self-identifies as being part of the "Anti-Trump Resistance Movement"?

d. Any individuals employed by MSNBC?

e. Any individuals employed by CNN?

f. Any blogs that self-identify as "liberal" or "progressive"?

g. Any Facebook groups that self-identify as "liberal", "progressive", or being part of the "Anti-Trump Resistance Movement"?

h. Open Society Foundation?

i. Planned Parenthood?

j. Indivisible?

k. Sierra Club?

l. The American Civil Liberties Union?

m. The Anti-Defamation League?

n. The Council on American-Islamic Relations (CAIR)?

o. Emily's List?

p. NARAL Pro-Choice America?

q. The National Association for the Advancement of Colored People (NAACP)?

r. NextGen Climate Action?

s. The Southern Poverty Law Center?

t. The Union of Concerned Scientists?

u. Everytown for Gun Safety?

v. Amnesty International?

w. Priorities USA Action?

x. Media Matters for America?

y. Human Rights Watch?

z. Every Voice?

aa. NowThis?

bb. The Women's March?

cc. Organizing for America?

dd. Organizing for Action?

When content that violates our policies is brought to our attention, we remove that content—regardless of who posted it. We have removed content posted by individuals and entities across the political spectrum.

On April 24, 2018, we published the detailed guidelines our reviewers use to make decisions about reported content on Facebook. These guidelines cover everything from nudity to graphic violence.

We published these guidelines because we believe that increased transparency will provide more clarity on where we draw lines on complex and continuously evolving issues, and we hope that sharing these details will prompt an open and honest dialogue about our decision making process that will help us improve - both in how we develop and enforce our standards. We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

We do not typically comment on specific cases of content removal for privacy reasons.

13) In your testimony before the committees, you stated several times that Facebook prohibits content based on its status as "hate speech." How have you and Facebook defined "hate speech" today and at any other stage in Facebook's existence?

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of

inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available here: https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

Our Community Standards make an important distinction between targeting people and targeting particular beliefs or institutions. We believe that people should be able to share their views and discuss controversial ideas on Facebook.

14) Did or does Facebook collaborate with or defer to any outside individuals or organizations in determining whether to classify a particular statement as "hate speech?" If so, please list the individuals and organizations.

Hate speech has no place on our platform. Our Community Standards prohibit attacks based on characteristics including race, ethnicity, religion, and national origin.

Facebook has partnerships with academics and experts who study organized hate groups and hate speech. These academics and experts share information with Facebook as to how organizations are adapting to social media and give feedback on how Facebook might better tackle these problems. We recently hosted several of these academics at Facebook for multiple days of observation and assessment, during which the academics attended substantive meetings on our content policies and the guidance we provide to our reviewers. Further, in the area of hate speech, there are very important academic projects that we follow closely. Timothy Garton Ash, for example, has created the Free Speech Debate to look at these issues on a cross-cultural basis. Susan Benesch established the Dangerous Speech Project, which investigates the connection between speech and violence. These projects show how much work is left to be done in defining the boundaries of speech online, which is why we will keep participating in this work to help inform our policies at Facebook. We are committed to continuing our dialogue with third parties to ensure we can have the widest possible expression of ideas, while preventing abuse of the platform.

Facebook works with organizations from across the political spectrum around changes to our content standards including hate speech. While we do not share individual pieces of content from users with these organizations out of concerns for user privacy, we do provide in-depth examples and explanations of what the policy changes would entail.

15) Did or does Facebook collaborate with or defer to any outside individuals or organizations in determining whether a given speaker has committed acts of "hate speech" in the past? If so, please list the individuals and organizations.

In an effort to prevent and disrupt real-world harm, we do not allow any organizations or individuals that are engaged in organized hate to have a presence on Facebook. We also remove content that expresses support or praise for groups, leaders, or individuals involved in these activities.

In developing and iterating on our policies, including our policy specific to hate speech, we consult with outside academics and experts from across the political spectrum and around the world. We do not, however, defer to these individuals or organizations in making decisions about

content on our platform. Content that violates our Community Standards is removed when we are made aware of it, and content that doesn't violate is left on the platform.

Designating hate organizations and/or individuals is an extensive process that takes into account a number of different signals. We worked with academics and NGOs to establish this process and regularly engage with them to understand whether we should refine it. Among the signals we consider are whether the individual or organization in question has called for or directly carried out violence against people based on protected characteristics.

16) Did or does Facebook ban or otherwise limit the content of individuals or organizations who have spoken "hate speech" on its platform aside from the offending content? If so, under what circumstances?

See Response to Question 15.

17) Yes or no: Did or does Facebook ban or otherwise limit the content of individuals or organizations on its platform based on hate speech or other behavior conducted outside of Facebook's platform?

See Response to Question 15.

18) Yes or no: Do you believe that "hate speech" is not protected under the First Amendment from government censorship?

The goal of our Community Standards is to encourage expression and create a safe community for our 2 billion users, more than 87% of whom are located outside the United States.

We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

We do not allow hate speech on Facebook because it creates an environment of intimidation and exclusion and in some cases may promote real-world violence.

Our current definition of hate speech is anything that directly attacks people based on what are known as their "protected characteristics"—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease. However, our definition does allow for discussion around these characteristics as concepts in an effort to allow for and encourage expression and dialogue by our users.

There is no universally accepted answer for when something crosses the line.

Our approach to hate speech, like those of other platforms, has evolved over time and continues to change as we learn from our community, from experts in the field, and as technology provides us new tools to operate more quickly, more accurately and precisely at scale.

19) Yes or no: Have you ever believed that "hate speech" is not protected under the First Amendment from government censorship?

See Response to Question 18.

20) Yes or no: Does Facebook believe that "hate speech" is not protected under the First Amendment from government censorship?

See Response to Question 18.

21) Yes or no: Has Facebook ever believed that "hate speech" is not protected under the First Amendment from government censorship?

See Response to Question 18.

22) Yes or no: Does Facebook's "hate speech" policy prohibit, exclude, remove, or censor content that, were Facebook a governmental entity, would be entitled to First Amendment protections?

See Response to Question 18.

23) Facebook states on its website that, per its community standards, Facebook will remove hate speech, which it describes as "including content that directly attacks people based on their: race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, or serious disabilities or diseases." Yes or no: Does Facebook limit its definition of hate speech only to content that "directly attacks" people based on the aforementioned characteristics?

We define "attack" under our hate speech policy as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. We allow discussion of issues related to characteristics like race, gender, ethnicity, and immigration status. We do not permit attacks against people based on these characteristics. Context matters in making what can be a difficult determination in some cases.

Specific details on the type of content that is prohibited under our hate speech policies are available here: https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

24) What standard or procedure has Facebook applied now and in the past in determining whether content "directly attacks" an individual or group based on a protected characteristic under Facebook's community standards?

See Response to Question 23.

25) Yes or no: Has Facebook ever removed content for hate speech that did not directly attack a person on the basis of his or her race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, or serious disabilities or diseases? If so, what criteria did Facebook use to determine that the content violated Facebook's policy?

We define "attack" under our hate speech policy as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation.

Sometimes, it's obvious that something is hate speech and should be removed—because it includes the direct incitement of violence against people possessing protected characteristics, or degrades or dehumanizes people. Sometimes, however, there isn't a clear consensus—because the words themselves are ambiguous, the intent behind them is unknown, or the context around them is unclear. Language also continues to evolve, and a word that was not a slur yesterday may become one today.

Here are some of the things we take into consideration when deciding what to leave on the site and what to remove.

- Context: Regional and linguistic context is often critical in deciding whether content constitutes hate speech, as is the need to take geopolitical events into account. In Myanmar, for example, the word "kalar" has benign historic roots, and is still used innocuously across many related Burmese words. The term can however also be used as an inflammatory slur, including as an attack by Buddhist nationalists against Muslims. We looked at the way the word's use was evolving, and decided our policy should be to remove it as hate speech when used to attack a person or group, but not in the other harmless use cases.

- Intent: There are times someone might share something that would otherwise be considered hate speech but for non-hateful reasons, such as making a self-deprecating joke or quoting lyrics from a song. People often use satire and comedy to make a point about hate speech. In other cases, people may speak out against hatred by condemning someone else's use of offensive language, which requires repeating the original offense. This is something we allow, even though it might seem questionable since it means some people may encounter material disturbing to them. But it also gives our community the chance to speak out against hateful ideas. We revised our Community Standards to encourage people to make it clear when they're sharing something to condemn it, but sometimes their intent isn't clear, and anti-hatred posts get removed in error.

On April 24, 2018, we announced the launch of appeals for content that was removed for hate speech. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

26) Has Facebook ever removed content for hate speech that was posted by an individual employed by Facebook? If so, please describe each instance.

Our policies apply equally to all of our users. If a Facebook employee posted content that was reported to us and violated our policies, the content would be removed.

27) Recording artist Taylor Swift recently released a cover of Earth, Wind & Fire's "September."

a) In response, Nathaniel Friedman, an author at GQ magazine, stated that "Taylor Swift's cover of 'September' is hate speech." Does Facebook agree?

b) In response, Monique Judge, an author at The Root, stated that "Taylor Swift needs her * whooped." Is this statement hate speech?**

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

We generally do not assess whether content violates our policies (including our hate speech policy) unless it is part of our normal content review process. Context matters in making what can be a difficult determination in some cases. Sometimes, it's obvious that something is hate speech and should be removed—because it includes the direct incitement of violence against people possessing protected characteristics, or degrades or dehumanizes people. Sometimes, however, there isn't a clear consensus—because the words themselves are ambiguous, the intent behind them is unknown or the context around them is unclear. Language also continues to evolve, and a word that was not a slur yesterday may become one today.

28) It was reported that Democratic D.C. Councilman Trayon White posted a video on his Facebook page blaming a recent snowstorm on wealthy Jewish families. According to USA Today, White said: "It just started snowing out of nowhere this morning, man. Y'all better pay attention to this climate control, man, this climate manipulation," which White attributed to "the Rothschilds controlling the climate to create natural disasters they can pay for to own the cities, man."

a) Yes or no: Does Facebook consider this video or this quote hate speech?

See Response to Question 27.

b) Yes or no: Did Facebook remove this video from its platform? If so, when? If not, why not?

See Response to Question 27.

29) Multiple authors for the website Vox, including its founder, Ezra Klein, have described Charles Murray's book, *The Bell Curve*, as "hate speech." Similarly, the left-wing Southern Poverty Law Center perplexingly describes Murray as a "white nationalist," largely relying on its depiction of *The Bell Curve*.

a) Does *The Bell Curve* qualify as "hate speech" for purposes of Facebook's policies?

See Response to Question 27.

i) If so, what portions of *The Bell Curve* qualify as "hate speech?" Please provide quotations with page numbers for these portions.

See Response to Question 27.

ii) If not, do Facebook's content policies prohibit a false claim that someone has engaged in "hate speech?"

See Response to Question 27.

iii) What procedures or penalties does Facebook employ, if any, to discourage false claims that someone has engaged in hate speech?

See Response to Question 27.

30) Are any portions of the Bible, quoted verbatim and with citation, subject to removal as:

a) "Hate speech?" If so, please list the quotations and under which translation Facebook considers the quote "hate speech."

See Response to Question 27.

b) Harassment? If so, please list the quotations and under which translation Facebook considers the quote harassment.

We do not tolerate harassment on Facebook because we want people to feel safe to engage and connect with their community. Our harassment policy applies to both public and private individuals and includes behavior like repeatedly contacting a single user despite that person's clear desire and action to prevent that contact and repeatedly contacting large numbers of people with no prior solicitation. It also applies to calls for death, serious disease or disability, or physical harm aimed at an individual or group of individuals in a message thread. Context and intent matter, however, and we allow people to share and re-share posts if it is clear that something was shared in order to condemn or draw attention to harassment. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available at https://www.facebook.com/communitystandards/safety/harassment.

We released our updated Community Standards—which reflect the guidelines our reviewers use to evaluate content that is reported to us—in order to better demonstrate where we draw lines on complex and continuously evolving issues. We also simultaneously launched an appeals process for content that has been removed for nudity/sexual activity, hate speech, and graphic violence. With this launch, we are giving people an opportunity to request review of our decisions and provide additional context that will help our team see a more complete picture as they review the post

again. This type of feedback allows us to continue improving our systems and processes so we can prevent similar mistakes in the future.

31) **On April 19, 2018, the California State Assembly voted in favor of a bill, AB 2943, which would make it an "unlawful business practice" to engage in any transaction for a good or service that seeks "to change an individual's sexual orientation" The bill clarifies that this includes efforts to "change behaviors or gender expressions, or to eliminate or reduce sexual or romantic attractions or feelings toward individuals of the same sex." Multiple legal experts have observed that the bill's language, reasonably interpreted, could be read to outlaw the sale and purchase of books, such as the Bible, the Torah, and the Koran, which advocate for traditional sexual ethics.**

    a) **Yes or no: Does Facebook believe that books, such as the Bible, the Torah, and the Koran, which advocate for traditional sexual ethics, constitute hate speech?**

    See Response to Question 27.

    b) **Yes or no: Does Facebook consider any part of the Bible, the Torah, and/or the Koran hate speech? If so, what parts of the Bible, the Torah, and/or the Koran qualify? Please provide quotations with page numbers for each part identified as hate speech.**

    See Response to Question 27.

    c) **Yes or no: Does Facebook believe that the messages contained in books, such as the Bible, the Torah, and the Koran, which advocate for traditional sexual ethics (*i.e.* that sex should be had only within a marriage between one man and one woman), should be discouraged from public dissemination?**

    See Response to Question 27.

    d) **Yes or no: Does Facebook agree with the California State Assembly that goods or services that seek to change behaviors or gender expressions deserve to be discouraged, muted, or banned?**

    See Response to Question 27.

    e) **Yes or no: Does Facebook agree with the California State Assembly that goods or services that seek to eliminate or reduce sexual or romantic attractions or feelings toward individuals of the same sex deserve to be discouraged, muted, or banned?**

    See Response to Question 27.

    f) **Yes or no: In the event AB 2943 is fully enacted into law, will Facebook comply with its provisions by removing, denying, downgrading, concealing, or otherwise censoring content and advertisements restricted by the bill? If so,**

does Facebook intend to remove, deny, downgrade, conceal, or otherwise censor content and advertisements that pertain to the Bible, the Torah, the Koran, and other books which advance traditional sexual ethics.

See Response to Question 27.

32) If an individual posted any of the following statements, standing alone and not directed to any Facebook user in particular, would that statement violate Facebook's "hate speech" policy? To the extent that the decision would depend on additional facts, please describe whether the statement would prompt an investigation to determine whether it constitutes "hate speech," and whether the decision would involve algorithmic or human decision making.

a) There are only two sexes or two genders, male and female.

b) Bathroom segregation based on sex is similar to segregation based on race.

c) God created man in his image, male and female.

d) Gender is a social construct.

e) A person's sex or gender are immutable characteristics.

f) Sex reassignment surgery is a form of bodily mutilation.

g) The abortion of an unborn child is murder.

h) It should be a crime to perform or facilitate an abortion.

i) It should be a crime to prevent someone from performing or obtaining an abortion.

j) No person of faith should be required to assist a same-sex wedding by providing goods or services to a same-sex marrying couple.

k) When an individual enters the marketplace, he gives up the right to choose whether to support a same-sex marriage.

l) Islam is a religion of peace.

m) Islam is a religion of war.

n) All white people are inherently racist.

o) All black people are inherently racist.

p) Black lives matter.

q) Blue lives matter.

r) All lives matter.

s) Donating to the NRA funds the murder of children, such as those slain in Parkland, Florida.

t) Donating to Planned Parenthood funds the murder of children, such as those dismembered by Kermit Gosnell.

u) Men should stop interrupting when women are talking.

v) Women should stop interrupting when men are talking.

w) DREAMers are Americans too and should be entitled to stay in this country.

x) Illegal aliens need to be sent back.

y) Religious beliefs are irrational and anti-science.

z) Non-believers have no path to eternal salvation.

aa) Affirmative Action policies discriminate on the basis of race and sex.

bb) America is a "melting pot."

See Response to Question 27.

33) Facebook states on its website that per its community standards, "organizations and people dedicated to promoting hatred" against protected groups are not allowed a presence on Facebook.

a) What standards or policies does Facebook apply in determining whether a group violates this policy?

See Response to Question 15.

b) Yes or no: Does Facebook contract with or in any way rely upon an outside party to determine what organizations and people are dedicated to promoting hatred against protected groups? If yes, please list the outside parties.

See Response to Question 15.

c) Yes or no: Has Facebook ever referenced, used, consulted, or in any way relied upon the left-wing Southern Poverty Law Center's list of designated hate groups in order to determine whether an organization or individual was dedicated to promoting hatred against protected groups?

See Response to Question 15.

d) Yes or no: Has Facebook ever denied an organization a presence on Facebook on account of the organization being dedicated to promoting hatred? If so, has Facebook ever reversed its decision to designate an organization a hate group under its community standards and reinstated the organization's privilege to post and have a presence on Facebook?

See Response to Question 15.

34) One group on Facebook, "TERMINATE the Republican Party," has over 10,000 followers, one of which was James T. Hodgkinson. In June 2017, Hodgkinson opened fire on Republican members of Congress at a baseball practice, seriously wounding Rep. Steve Scalise, a congressional staffer, and two heroic police officers. Quotes from this group's posts and comments include that "These people are all the same, criminals, rapists, racists, Republicans;" that, about Rep. Patrick McHenry, "who gives birth to sorry pieces of s* like him and allowed it to reach adulthood, truly needs a f*****g hammer to the head a few times;" and, referring to the President, "G*****n Russian roach traitor bastard . . . and his Republicanazi followers!" Each of these quotes took place long after Hodgkinson's shooting, though similar quotes are available from before it as well.**

a) Do these quotes constitute "hate speech?"

i) If so, why have they not been removed?

ii) If not, why do they not?

b) If applied to Democrats, would the quotes above constitute "hate speech?"

c) How has Facebook changed its platform in response to Hodgkinson's shooting? It has apparently not suspended or ended this group.

d) Does it concern Facebook that such rhetoric is being used in a group which had an attempted political assassin as a member?

e) Does Facebook permit threats of violence against the President?

f) Does Facebook permit threats of violence against members of Congress?

g) Does Facebook monitor its platforms for potential left-wing violence?

i) If so, what is Facebook doing to ensure that shooters like Hodgkinson do not coordinate using Facebook?

ii) If so, what is Facebook doing to ensure that shooters like Hodgskinson do not use Facebook to incite violence against Republicans or conservatives?

iv) If not, why is Facebook not doing so given that its platform was integral to at least one attempted political assassination?

The shooting at the Congressional baseball practice was a horrendous act. As a designated mass shooting, any praise for that conduct or the shooter is against Facebook policies. We also do not allow any pages or accounts representing the shooter. If we are made aware of such comments, we would take them down.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. Political-party affiliation is not included in our list of protected characteristics. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

Our credible violence policies prohibit posting credible statements of intent to commit violence against any person, groups of people, or place (city or smaller). We assess credibility based upon the information available to us and generally consider statements credible if the following are present:

- A target (person, group of people, or place) and:
  - Bounty/demand for payment, or
  - Mention or image of specific weapon, or
  - Sales offer or ask to purchase weapon, or
  - Spelled-out address or named building, or
- A target and 2 or more of the following details (can be 2 of the same detail):
  - Location
  - Timing
  - Method

We also prohibit calls for violence, statements advocating violence, or aspirational or conditional statements of violence targeting public individuals, provided those statements are credible, as defined above. Any calls for violence against heads of state, including the United States President, violate our policies.

There are times someone might share something that would otherwise be considered hate speech but for non-hateful reasons, such as making a self-deprecating joke or quoting lyrics from a song. People often use satire and comedy to make a point about hate speech. In other cases, people may speak out against hatred by condemning someone else's use of offensive language, which requires repeating the original offense. This is something we allow,

even though it might seem questionable since it means some people may encounter material disturbing to them.

35) In July 2012, Governor Mike Huckabee praised Chick-fil-A because of its support for traditional marriage and called on Christians to support Chick-fil-A in its position by purchasing its products. Facebook temporarily removed Governor Huckabee's post from its service before reinstating it.

a) Why was Governor Huckabee's post removed?

b) What Facebook rule was Governor Huckabee's post thought to have violated before it was reinstated?

c) Did Governor Huckabee's post violate Facebook's prohibition on "hate speech," either in 2012 or now?

d) Does a post opposing the Supreme Court's decision in *Obergefell v. Hodges*

violate Facebook's prohibition on "hate speech?"

e) Does a post opposing legalized same-sex marriage violate Facebook's prohibition on "hate speech?"

f) As of July 2012, had Facebook removed, downgraded, concealed, or otherwise censored any content created by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's support for same-sex marriage? If so, please include the removed content including identifying information indicating its author.

g) As of July 2012, had Facebook removed, downgraded, concealed, or otherwise censored any other content created by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's opposition to same-sex marriage? If so, please include the removed content including identifying information indicating its author.

h) Has, since July 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's (or that content's) opposition to same-sex marriage? If so, please include the removed post identifying information indicating its author.

i) Has, since July 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's (or that content's) support for same-sex

marriage? If so, please include the removed post identifying information indicating its author.

j) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, opposes same-sex marriage?

k) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, supports same-sex marriage?

In July 2012, our automated systems incorrectly removed an event page entitled "Chick-fil-A Appreciation Day." The page was restored within hours of coming to our attention. When we make mistakes on these important content decisions, we make every attempt to make it right as quickly as we can.

Our goal is to allow people to have as much expression as possible, including on the issue of same-sex marriage. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

See also Response to Question 27.

36) As described in the Washington Post, in October 2012, Facebook removed a post by a group called "Special Operations Speaks." The post said: "Obama called the SEALS and THEY got bin Laden. When the SEALs called Obama, they got denied," a reference to the failure of the Executive Branch to provide military support to Americans under assault, and later killed, in Benghazi. Facebook first warned the group that the post violated its rules and then subsequently removed the post as a violation of "Facebook's Statements of Rights and Responsibilities." Facebook further suspended Special Operations Speaks for 24 hours following the removal. Facebook later admitted error and permitted the content to remain on its platform.

a) Why was Special Operations Speaks' post removed?

b) What term of Facebook's then-extant 2012 Statement of Rights and Responsibilities was Special Operations Speaks' post thought to have violated before Facebook reversed its decision?

c) Yes or no: Did any member of the Obama Administration, including any administrative agency then-directed by an executive official appointed by the Obama administration, contact Facebook to request that the post be removed?

i) If so, whom?

ii) What was Facebook's response?

d) Yes or no: Did Facebook assure any government official or employee that this post would be removed? If so, whom?

e) Did Special Operations Speaks' post violate Facebook's prohibition on "hate speech," either in 2012 or now?

f) As of October 2012, had Facebook removed, downgraded, concealed, or otherwise censored any other content created by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

g) As of October 2012, had Facebook removed, downgraded, concealed, or otherwise censored any content created by a political action committee on the basis of that content's approval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

h) Has, since October 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

i) Has, since October 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on

U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

j) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, opposes the Obama Administration's handling of the attacks on U.S. diplomats and servicemen in Benghazi?

k) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, supports the Obama Administration's handling of the attacks on U.S. diplomats and servicemen in Benghazi?

In this particular case, we removed the content as a violation of our standards. The content was deleted for 29 hours. However, we realized that we made a mistake, and we restored the content and apologized for the error.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

Our Community Standards prohibit hate speech and celebrating graphic violence and allow people to use Facebook to raise awareness of and condemn violence. Drawing that line requires complex and nuanced judgments, and we carefully review reports that we receive from the public, media, civil society, and governments. We remove content that violates our policies, regardless of who posted the content.

37) In September 2017, Facebook deemed the videos of two African American Trump supporters, known as Diamond and Silk, as "dangerous." In a company email, Facebook stated that the decision was final and "not appealable in any way." Facebook then retracted this statement, explaining that the determination was inaccurate.

a) What about Diamond and Silk did Facebook initially determine to be "dangerous?"

b) What is Facebook's criteria for determining whether content that neither depicts nor advocates for violence as "dangerous?"

c) Aside from the illustration of or advocacy for violence, under what conditions is the discussion of non-classified speech "dangerous?"

d) Has Facebook implemented an appeals system by which users can challenge a determination of dangerousness?

e) How often does Facebook retract these determinations?

f) What is the internal review process for these types of determinations?

We mishandled communication with Diamond and Silk for months. Their frustration was understandable, and we apologized to them. The message they received on April 5, 2018 that characterized their Page as "dangerous" was incorrect and not reflective of the way we seek to communicate with our community and the people who run Pages on our platform.

As part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community.

- We continue to expand our list of outside organizations from across the political spectrum to provide feedback on potential changes to our content standards.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

See also Response to Question 27.

38) In October 2017, the social-media company Twitter refused to permit Representative Marsha Blackburn to pay to promote a campaign advertisement because Rep. Blackburn stated that she fought to stop the sale of children's body parts. Twitter's explanation was that Blackburn's critique of "the sale of baby body parts" was an "inflammatory statement" that Twitter refused to advertise.

a) Does Representative Blackburn's campaign advertisement (available readily on the internet) violate Facebook's policies regarding acceptable advertisements?

b) Does Representative Blackburn's campaign advertisement violate Facebook's policies against "hate speech?"

c) Would the statement, standing alone, that Planned Parenthood sells baby body parts qualify as "hate speech?"

d) Would Facebook censor or otherwise downgrade or make unavailable the statement that Planned Parenthood sells baby body parts for any other reason?

As Facebook indicated publicly in October 2017, Representative Blackburn's campaign advertisement, in which she mentioned "the sale of baby body parts" does not violate our Advertising Policies or our Community Standards.

We work to strike the right balance between enabling free expression around the globe and ensuring that our platform is safe. We currently define hate speech as anything that directly

attacks people based on protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease. We remove content that violates our policies, regardless of who posted the content, including the government.

Our policies allow content that may be controversial and at times even distasteful, but which does not cross the line into hate speech. This may include criticism of public figures, religions, professions, and political ideologies.

39) Louis Farrakhan presently employs Facebook to reach numerous individuals. At present, he has over a million followers.

a) On his Facebook page, Farrakhan links to an open letter of his which states: "We can now present to our people and the world a *true*, undeniable record of the relationship between Blacks and Jews from their own mouths and pens. These scholars, Rabbis and historians have given to us an undeniable record of Jewish anti-Black behavior, starting with the horror of the trans-Atlantic slave trade, plantation slavery, Jim Crow, sharecropping, the labor movement of the North and South, the unions and the misuse of our people that continues to this very moment."

i) Does this statement violate Facebook's policies against "hate speech?"

ii) If so, why has this post been permitted to remain?

iii) If not, why not?

b) On his Facebook page, Farrakhan links to a sermon in which he describes the "Synagogue of Satan" and its attempts to harm him.

i) Is the term "Synagogue of Satan" a violation of Facebook's policies against "hate speech?"

ii) If so, why has this post been permitted to remain?

iii) If not, why not?

We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to

assess whether content violates our hate speech policies are available at https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

40) In June 2013, Facebook blocked the following post written by Fox News Radio's Todd Starnes for violating Facebook's community standards, "I'm about as politically incorrect as you can get. I'm wearing an NRA ball cap, eating a Chick-fil-A sandwich, reading a Paula Deen cookbook and sipping a 20-ounce sweet tea while sitting in my Cracker Barrel rocking chair with the Gather Vocal Band singing 'Jesus Saves' on the stereo and a Gideon's Bible in my pocket. Yes sir, I'm politically incorrect and happy as a June bug." Although Facebook ultimately reversed its decision, for several hours, Todd Starnes could not access either his fan or person page.

a) Why was Todd Starnes' post removed?

b) What Facebook rule was Todd Starnes' post thought to have violated before it was reinstated?

c) Was any part of Starnes' statement "hate speech?"

d) Was any part of Starnes' statement considered harassment?

e) Yes or no: must posted content be "politically correct" to remain in accordance with Facebook's community standards?

f) Is a statement that something is not "politically correct" a violation of Facebook's standards?

The page where Todd Starnes posted the content was not unpublished. He was the administrator that made the post, and the action was taken on his profile. He posted the content at around 2 am on June 29, 2013, and it was restored shortly before 10 am the same day. During that time, he did not lose his ability to access either his profile or his page, just the post itself. When we reinstated the post, we sent him an apology the same day.

Our policies apply equally to individuals and entities across the political spectrum. We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

When we're made aware of incorrect content removals, we review them with team members so as to prevent similar mistakes in the future. We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

We hope that our recent decision to publicize our detailed Community Standards—which reflect our internal reviewer guidelines—and the introduction of appeals will aid in this process. By providing more clarity on what is and isn't allowed on Facebook, we hope that people will better understand how our policies apply to them. Where people believe we have made a mistake, they can request review of our decisions.

See also Response to Question 44.

41) How many individuals at Facebook have the ability to moderate, remove, downgrade, conceal, or otherwise censor content, ban, suspend, warn, or otherwise discipline users, or approve, price, review, or refuse advertisements on the platform? This question includes individuals with the power to alter search results and similar mechanisms that suggest additional content to users in order to to promote or demote content, whether individually or routinely through an algorithm or by altering any of the platform's search functions. (Please include all employees, independent contractors, or others with such ability at Facebook.)

a) Into what divisions or groups are those individuals organized?

b) Who are the individuals responsible for supervising these individuals as their conduct relates to American citizens, nationals, businesses, and groups?

c) We understand from your April 10 testimony that Facebook has approximately 15,000 to 20,000 moderators. How many individuals have the responsibility to moderate, remove, downgrade, conceal, or otherwise censor content, ban, suspend, warn, or otherwise discipline users, or approve, price, review, or refuse advertisements as a primary or significant function of their role at Facebook? This question includes individuals with the power to alter search results and similar mechanisms that suggest additional content to users in order to to promote or demote content, whether individually or routinely through an algorithm or by altering any of the platform's search functions. (Going forward, we will refer to these individuals, with a primary or significant responsibility for reviewing content, users, or advertisements, as "moderators.")

d) Who are the individuals responsible for supervising these moderators as their conduct relates to American citizens, nationals, businesses, and groups?

e) How many moderators has Facebook had on its platform for each of the calendar years 2006 to 2018? Please provide approximations if exact numbers are impossible to obtain.

f) How many moderators does Facebook intend to retain for the years 2019 and 2020?

g) On average, how many pieces of content (*e.g.*, a Facebook post, an Instagram photo, and so on) does a moderator remove a day?

h) On average, how many users does a moderator discipline a day?

i) On average, how many advertisements does a moderator approve, disapprove, price, consult on, review, or refuse a day?

Our content reviewers respond to millions of reports each week from people all over the world.

Our community of users helps us by reporting accounts or content that may violate our policies. Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in dozens of languages to review these reports. By the end of 2018, we will have doubled the number of people working on safety and security as compared to the beginning of the year—to a total of 20,000.

To help the Facebook community better understand our efforts to enforce the Community Standards, we recently published a Community Standards Enforcement Preliminary Report (https://transparency.facebook.com/community-standards-enforcement) describing the amount and types of content we take action against, as well as the amount of content that we flag for review proactively.

We are also committed to getting better at enforcing our advertising policies. We review many ads proactively using automated and manual tools, and reactively when people hide, block, or mark ads as offensive. We are taking aggressive steps to strengthen both our automated and our manual review. We are also expanding our global ads review teams and investing more in machine learning to better understand when to flag and take down ads, such as ads that offer employment or credit opportunity while including or excluding multicultural advertising segments. Enforcement is never perfect, but we will get better at finding and removing improper ads.

As to the questions regarding ranking and algorithmic changes, see Response to Question 47.

42) What percentage of Facebook's moderators:

a) Self-identify or are registered as Democrats?

b) Self-identify or are registered as Republicans?

c) Would identify themselves as "liberal?"

d) Would identify themselves as "conservative?"

e) Have donated to:

i) The Democratic Party?

ii) A candidate running for office as a Democrat?

iii) A cause primarily affiliated with or supported by the Democratic Party?

iv) A cause primarily affiliated with or supported by liberal interest groups?

v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

vi) The Republican Party?

vii) A candidate running for office as a Republican?

viii) A cause primarily affiliated with or supported by the Republican Party?

ix) A cause primarily affiliated with or supported by conservative interest groups?

x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

f) Worked on or volunteered for a Democratic campaign?

g) Worked on or volunteered for a Republican campaign?

h) Worked on, interned for, or volunteered for a Democratic legislator, State or federal?

i) Worked on, interned for, or volunteered for a Republican legislator, State or federal?

j) Worked on or interned for a Democratic administration or candidate?

k) Worked on or interned for a Republican administration or candidate?

We do not maintain statistics on these data points.

43) What percentage of Facebook's employees:

a) Self-identify or are registered as Democrats?

b) Self-identify or are registered as Republicans?

c) Self-identify as "liberal?"

d) Self-identify as "conservative?"

e) Have donated to:

i) The Democratic National Committee, the Democratic Congressional Campaign Committee, or the Democratic Senatorial Campaign Committee?

ii) A candidate running for office as a Democrat?

iii) A cause primarily affiliated with or supported by the Democratic Party?

iv) A cause primarily affiliated with or supported by liberal interest groups?

v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

vi) The Republican National Committee, the National Republican Senate Committee, or the National Republican Congressional Committee?

vii) A candidate running for office as a Republican?

viii) A cause primarily affiliated with or supported by the Republican Party?

ix) A cause primarily affiliated with or supported by conservative interest groups?

x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

f) Worked on, interned for, or volunteered for a Democratic candidate campaigning for elected office or an elected Democratic official or candidate?

g) Worked on, interned for, or volunteered for a Republican campaigning for elected office or an elected Republican official or candidate?

We do not maintain statistics on these data points.

44) What percentage of Facebook's management:

a) Self-identify or are registered as Democrats?

b) Self-identify or are registered as Republicans?

c) Self-identify as "liberal?"

d) Self-identify as "conservative?"

e) Have donated to:

i) The Democratic National Committee, the Democratic Congressional Campaign Committee, or the Democratic Senatorial Campaign Committee?

ii) A candidate running for office as a Democrat?

iii) A cause primarily affiliated with or supported by the Democratic Party?

iv) A cause primarily affiliated with or supported by liberal interest groups?

v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

vi) The Republican National Committee, the National Republican Senate Committee, or the National Republican Congressional Committee?

vii) A candidate running for office as a Republican?

viii) A cause primarily affiliated with or supported by the Republican Party?

ix) A cause primarily affiliated with or supported by conservative interest groups?

x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

f) Worked on, interned for, or volunteered for an elected Democratic official or candidate?

g) Worked on, interned for, or volunteered for an elected Republican official or candidate?

We do not maintain statistics on these data points.

45) What percentage of Facebook's executives:

a) Self-identify or are registered as Democrats?

b) Self-identify or are registered as Republicans?

c) Self-identify as "liberal?"

d) Self-identify as "conservative?"

e) Have donated to:

i) The Democratic National Committee, the Democratic Congressional Campaign Committee, or the Democratic Senatorial Campaign Committee?

ii) A candidate running for office as a Democrat?

iii) A cause primarily affiliated with or supported by the Democratic Party?

iv) A cause primarily affiliated with or supported by liberal interest groups?

v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

vi) The Republican National Committee, the National Republican Senate Committee, or the National Republican Congressional Committee?

vii) A candidate running for office as a Republican?

viii) A cause primarily affiliated with or supported by the Republican Party?

ix) A cause primarily affiliated with or supported by conservative interest groups?

x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

f) Worked on, interned for, or volunteered for an elected Democratic official or candidate?

g) Worked on, interned for, or volunteered for an elected Republican official or candidate?

We do not maintain statistics on these data points.

46) How many employees has Facebook hired that previously worked for 501(c)(3) or 501(c)(4) nonprofits? Please list the names of the 501(c)(3) and 501(c)(4) organizations employees have previously worked for and the number of employees for each.

We do not maintain statistics on these data points.

47) Based on your testimony, we understand that Facebook conducts many of its editorial and moderating decisions using one or more algorithms.

a) What editorial and moderating functions do these algorithms undertake?

b) List and describe the factors that the algorithm evaluates and considers.

c) Describe what if any human oversight or auditing is in place to review the algorithm's functions.

d) Do any of the factors in these algorithms associated with promoting, demoting, flagging, removing, suggesting, or otherwise altering the visibility of content correlate strongly (defined as meeting any generally accepted threshold for strong correlation using any generally accepted bivariate or multivariate analysis technique, including, but not limited to, chi-square, ANOVA, MANCOVA, Probit, Logit, regression, etc.) with any of the following traits (if so, please list which factor and its correlation):

i) Self-identification with the Democratic Party?

ii) Registration as a Democrat?

iii) Self-identification as a liberal?

iv) Self-identification with the Republican Party?

v) Registration as a Republican?

vi) Self-identification as a conservative?

e) Do any of these factors correlate significantly (p greater than or equal to .05) with any of the following traits (if so, please list which factor and its correlation):

i) Self-identification with the Democratic Party?

ii) Registration as a Democrat?

iii) Self-identification as a liberal?

iv) Self-identification with the Republican Party?

v) Registration as a Republican?

vi) Self-identification as a conservative?

A user's News Feed is made up of stories from their friends, Pages they've chosen to follow and groups they've joined. Ranking is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook.

Ranking has four elements: the available inventory of stories; the signals, or data points that can inform ranking decisions; the predictions we make, including how likely we think a user is to comment on a story, share with a friend, etc.; and a relevancy score for each story.

News Feed considers thousands of signals to surface the content that's most relevant to each person who uses Facebook. Our employees don't determine the ranking of any specific piece of content. To help the community understand how News Feed works and how changes to News Feed affect their experience on Facebook, we publish a regularly-updated News Feed FYI blog (https://newsroom.fb.com/news/category/inside-feed/) where our team shares details of significant changes.

48) What percentage of the individuals who design, code, implement, monitor, correct, or alter any of these algorithms:

a) Self-identify as Democrats?

b) Are registered as Democrats?

c) Self-identify as liberal?

d) Self-identify as Republicans?

e) Are registered as Republicans?

f) Self-identify as conservative?

We do not maintain statistics on these data points.

49) In 2016, in response to complaints about "fake news" during the 2016 Presidential campaign and following President Trump's election, Facebook procured the services of specific "fact-checking" outlets in order to flag certain stories or sources as disputed, challenged, or incorrect. Earlier this year, it additionally changed one or more of the algorithms that recommend websites to users, such as users' news feeds.

a) On what basis did Facebook select the fact-checking organizations that it enlisted to identify incorrect assertions of fact?

b) Numerous sources have cited the presence of political bias in many "fact-checking" organizations; for example, according to one 2013 study by George Mason University's Center for Media and Public Affairs, the site Politifact.com-- which Facebook employs to check facts on its platform--was between two and three times more likely to rate Republicans' claims as false (32%) than Democrats' claims (11%), and was between two and three times more likely to rate Democrats' statements as mostly or entirely true (54%) compared to Republicans' statements (18%). Indeed, the RealClearPolitics "Fact Check Review" notes that, in the last 120 days, approximately 1/6th of "facts" that Politifact.com claims to check aren't facts at all, but mere opinions.

i) What steps does Facebook take to counteract liberal or left-wing bias by fact-checking outlets?

ii) What steps does Facebook intend to take to bring political balance to its fact-checking review process?

iii) What mechanisms for appealing a determination that a statement is false or otherwise disagreed-with does Facebook make available to entities that Politifact (or others) accuse(s) of lying?

(1) If none exist, what mechanisms does Facebook intend to make available?

(2) If none exist, to what extent will Facebook make its review of these claims publicly visible?

iv) Has Facebook ever labeled claims or articles by any of the following entities as false? If so, please identify which claims and when.

(1) Huffington Post

(2) Salon

(3) Slate

(4) ThinkProgress

(5) Media Matters for America

(6) ShareBlue

(7) The Daily Kos

(8) Vice

(9) Vox

(10) TalkingPointsMemo

v) Does Facebook consider the basis for a fact-checker's determination that something is "false" when choosing to label it as such? For example, as numerous media outlets have noted, some fact-checking outlets concede that the factual statement a public figure has made is true, but then condemn it for lacking "context" or spin favorable to a left-wing politician.

(1) If so, how does Facebook consider it?

(2) If not, does Facebook intend to do so in the future? And if so, how? If not, why not?

c) When one of Facebook's fact-checkers determines that a claim is false, how does Facebook determine what material to refer a user to in response? Please list all such sources and any method relied on for determining their priority.

d) Facebook's 2018 alteration of its algorithm has had a noted and outsized impact on traffic to conservative websites while not having a similar effect on liberal websites. At least one study by the Western Journal estimated liberal publishers' traffic from Facebook rose approximately 2% following the change, while conservative publishers' traffic declined approximately 14%.

i) In what way(s) did Facebook change its content-screening or news-suggesting algorithms, or any other feature of its website which suggests content to users, in this 2018 instance?

(1) Were any components of these changes intended to have a differential impact on conservative outlets versus liberal ones?

(2) Were any components of these changes expected to have a differential impact on conservative outlets versus liberal ones?

ii) Measured against pre-change traffic, how has the traffic of liberal publishers changed following this 2018 instance?

iii) Measured against pre-change traffic, how has the traffic of conservative publishers changed following this 2018 instance?

iv) Measured against pre-change traffic, how has this 2018 instance changed the traffic of the following publishers:

(1) The Washington Post

(2) The New York Times

(3) The Washington Times

(4) The New York Post

(5) The New York Daily News

(6) Fox News

(7) National Review

(8) The Daily Beast

(9) Huffington Post

(10) Buzzfeed

(11) Newsweek

(12) The Daily Wire

(13) Vice

(14) USA Today

(15) Salon

(16) Slate

(17) Vox

(18) The Daily Caller

(19) The Blaze

(20) PJ Media

(21) The Washington Free Beacon

(22) Reuters

(23) The Associated Press

(24) National Public Radio

(25) Bloomberg

v) Does Facebook intend to do anything to reduce the differential effect on its recent algorithmic changes on conservative publishers?

(1) If so, what?

(2) If not, why not?

To reduce the spread of false news, one of the things we're doing is working with third-party fact checkers to let people know when they are sharing news stories (excluding satire and opinion) that have been disputed or debunked, and to limit the distribution of stories that have been flagged as misleading, sensational, or spammy. Third-party fact-checkers on Facebook are signatories to the non-partisan International Fact-Checking Network Code of Principles. Third-party fact-checkers investigate stories in a journalistic process meant to result in establishing the truth or falsity of the story.

In the United States, Facebook uses third-party fact-checking by the Associated Press, Factcheck.org, PolitiFact, Snopes, and the Weekly Standard Fact Check.

Publishers may reach out directly to the third-party fact-checking organizations if (1) they have corrected the rated content, or if (2) they believe the fact-checker's rating is inaccurate. To issue a correction, the publisher must correct the false content and clearly state that a correction was made directly on the story. To dispute a rating, the publisher must clearly indicate why the original rating was inaccurate. If a rating is successfully corrected or disputed, the demotion on the content will be lifted and the strike against the domain or Page will be removed. It may take a few days to see the distribution for the domain or Page recover. Additionally, any recovery will be affected by other false news strikes and related interventions (like demotions for clickbait). Corrections and disputes are processed at the fact-checker's discretion. Fact-checkers are asked to respond to requests in a reasonable time period—ideally one business day for a simple correction, and up to a few business days for more complex disputes.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help.

As to the questions regarding ranking and algorithmic changes, see Response to Question 47.

50) Facebook's Help section explains that the posts that users see are influenced by their connections and activity on Facebook, including the number of comments, likes, and reactions a post receives and what kind of story it is. Some reporting suggests that Facebook's algorithm functions based on the content available (inventory), considerations about the content (signals), considerations about a person (predictions), and overall score.

a) How do Facebook employees determine how informative a post is or which interactions create a more meaningful experience?

b) Does a speaker's viewpoint determine in whole or part how informative or meaningful a post is?

c) Does a speaker's partisan affiliation determine in whole or part how informative or meaningful a post is?

d) Does a speaker's religious affiliation determine in whole or part how informative or meaningful a post is?

See Response to Question 47.

51) Facebook is entitled to contribute money to federal and State elections both as a function of the First Amendment as well as of federal and State law. Including all of its subsidiaries, affiliates, as well as political action committees, partnerships, councils, groups, or entities organized with either a sole or significant purpose of electioneering, making political contributions to issue advocacy, candidates, or political parties, or of bundling or aggregating money for candidates or issue or party

advocacy, whether disclosed by law or not, and during primary elections or general elections, how much money has Facebook contributed to:

a) All federal, State, and local candidates for office from 2008 to present?

b) All national party committees?

i) Of that amount, how much was to:

(1) The Democratic National Committee?

(2) The Democratic Senatorial Campaign Committee?

(3) The Democratic Congressional Campaign Committee?

(4) The Republican National Committee?

(5) The National Republican Senate Committee?

(6) The National Republican Congressional Committee?

c) All political action committees (or other groups outlined above in question 43) from 2008 to present?

d) All issue-advocacy campaigns, including initiatives, referenda, ballot measures, and other direct-democracy or similar lawmaking measures?

e) Candidates running for President:

i) In 2008?

(1) How much of that money was to the Democratic candidate?

(2) How much of that money was to the Republican candidate?

(3) How much of that money was to other candidates?

ii) In 2012?

(1) How much of that money was to the Democratic candidate?

(2) How much of that money was to the Republican candidate?

(3) How much of that money was to other candidates?

iii) In 2016?

(1) How much of that money was to the Democratic candidate?

(2) How much of that money was to the Republican candidate?

(3) How much of that money was to other candidates?

f) Candidates running for the U.S. Senate: (for special or off-year elections going forward, please group donation amounts with the next nearest cycle)

i) In 2008?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

ii) In 2010?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

iii) In 2012?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

iv) In 2014?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

v) In 2016?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

vi) In 2018?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

g) Candidates running for the U.S. House of Representatives:

i) In 2008?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

ii) In 2010?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

iii) In 2012?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

iv) In 2014?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

v) In 2016?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

vi) In 2018?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

h) Candidates running for Governor: i) In 2008?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

ii) In 2010?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

iii) In 2012?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

iv) In 2014?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates? v) In 2016?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

vi) In 2018?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

i) Political action committees or other groups mentioned in question 43 that:

i) **Contribute 75% or more of their money to Democratic candidates for office?**

ii) **Contribute 75% or more of their money to Republican candidates for office?**

iii) **Identify as liberal, progressive, or otherwise left-wing?**

iv) **Identify as conservative or right-wing?**

Facebook complies with all political contribution reporting requirements, and such reports are publicly available. For more information on Facebook's contributions, please see https://newsroom.fb.com/news/h/facebook-political-engagement/.

52) **How much has Facebook donated, either in the form of money or services (including free or discounted advertising or more prominent placements within the platform via searches and other suggested-content mechanisms), to the following not-for-profit organizations (or their affiliates or subsidiaries) in the last 10 years? (Please separate answers into cash and non-cash components.)**

a) **Planned Parenthood**

b) **NARAL**

c) **The Center for Reproductive Rights**

d) **The National Right to Life Committee**

e) **Americans United for Life**

f) **Everytown for Gun Safety**

g) **The Brady Campaign**

h) **The National Rifle Association**

i) **Gun Owners of America**

j) **Human Rights Campaign**

k) **Amnesty International**

l) **Lambda Legal**

m) **National Immigration Forum**

n) **Federation**

o) **GLAAD**

p) ACLU

q) UnidosUS (formerly "La Raza" or the "National Council of La Raza")

r) The Sierra Club

s) Greenpeace

t) The Heritage Foundation

u) The Cato Institute

v) The Institute for Justice

w) Southern Poverty Law Center

x) The Open Society Foundation(s)

y) Americans for Prosperity

We partner with various domestic and international non-governmental organizations, which span the political and ideological spectrum. We provide our partners with technical expertise, sponsorships, advertising credits, and trainings, among other support. Our partnerships are crucial to our mission of building community. More information about our partnerships is available at https://newsroom.fb.com/news/h/facebook-political-engagement/.

53) Facebook sells advertisements to political candidates and organizations. Multiple sources report that Facebook charged different rates to the Hillary Clinton and Donald Trump campaigns during the 2016 election. For the following questions, to the extent that geographic or local-market concerns significantly explain disparate rates between candidates, please explain how they do so and to what extent they do so, including calculations justifying that explanation.

a) Did Facebook charge the two campaigns different rates?

i) If so, on what basis?

ii) If so, what rates did Facebook charge:

(1) The Clinton Campaign?

(2) The Trump Campaign?

b) If these campaigns purchased advertising rates on Facebook or its platforms, what rates did Facebook charge each of the following campaigns?

i) Barack Obama's 2008 campaign

ii) John McCain's 2008 campaign

iii) **Barack Obama's 2012 campaign**

iv) **Mitt Romney's 2012 campaign**

c) **On average, and among campaigns that purchased advertisements, what rates did Facebook charge:**

i) **Democrats running for Senate in 2008?**

ii) **Republicans running for Senate in 2008?**

iii) **Democrats running for the House of Representatives in 2008?**

iv) **Republicans running for the House of Representatives in 2008?**

v) **Democrats running for Governor in 2008?**

vi) **Republicans running for Governor in 2008?**

vii) **Democrats running in State or local legislative races in 2008?**

viii) **Republicans running in State or local legislative races in 2008?**

ix) **Democrats running for Senate in 2010?**

x) **Republicans running for Senate in 2010?**

xi) **Democrats running for the House of Representatives in 2010?**

xii) **Republicans running for the House of Representatives in 2010?**

xiii) **Democrats running for Governor in 2010?**

xiv) **Republicans running for Governor in 2010?**

xv) **Democrats running in State or local legislative races in 2010?**

xvi) **Republicans running in State or local legislative races in 2010?**

xvii) **Democrats running for Senate in 2012?**

xviii) **Republicans running for Senate in 2012?**

xix) **Democrats running for the House of Representatives in 2012?**

xx) **Republicans running for the House of Representatives in 2012?**

xxi) **Democrats running for Governor in 2012?**

xxii) **Republicans running for Governor in 2012?**

xxiii) Democrats running in State or local legislative races in 2014?

xxiv) Republicans running in State or local legislative races in 2014?

xxv) Democrats running for Senate in 2014?

xxvi) Republicans running for Senate in 2014?

xxvii) Democrats running for the House of Representatives in 2014?

xxviii) Republicans running for the House of Representatives in 2014?

xxix) Democrats running for Governor in 2014?

xxx) Republicans running for Governor in 2014?

xxxi) Democrats running in State or local legislative races in 2014?

xxxii) Republicans running in State or local legislative races in 2014?

xxxiii) Democrats running in State or local legislative races in 2016?

xxxiv) Republicans running in State or local legislative races in 2016?

xxxv) Democrats running for Senate in 2016?

xxxvi) Republicans running for Senate in 2016?

xxxvii) Democrats running for the House of Representatives in 2016?

xxxviii) Republicans running for the House of Representatives in 2016?

xxxix) Democrats running for Governor in 2016?

xl) Republicans running for Governor in 2016?

xli) Democrats running in State or local legislative races in 2016?

xlii) Republicans running in State or local legislative races in 2016?

xliii) Democrats running in State or local legislative races in 2018?

xliv) Republicans running in State or local legislative races in 2018?

xlv) Democrats running for Senate in 2018?

xlvi) Republicans running for Senate in 2018?

xlvii) Democrats running for the House of Representatives in 2018?

xlviii) Republicans running for the House of Representatives in 2018?

xlix) Democrats running for Governor in 2018?

l) Republicans running for Governor in 2018?

li) Democrats running in State or local legislative races in 2018?

lii) Republicans running in State or local legislative races in 2018?

d) Yes or no: does Facebook consider partisan affiliation in deciding whether to sell advertisements to a political candidate, political action committee, or other organization purchasing political advertisements?

e) Yes or no: does Facebook consider partisan affiliation in deciding at what rates to sell advertisements to a political candidate, political action committee, or other organization purchasing political advertisements?

f) Yes or no: does Facebook consider the likelihood of a candidate's ultimate electoral success (via polls or otherwise) in deciding whether to sell advertisements to a political candidate?

g) Yes or no: does Facebook consider the likelihood of a candidate's ultimate electoral success (via polls or otherwise) in deciding at what rates to sell advertisements to a political candidate?

Facebook offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered.

See also Response to Question 54.

54) Please provide Facebook's advertising rates for each U.S. Senate and U.S. House election for which Facebook quoted or sold advertisements to one or more candidates for the years 2008, 2010, 2012, 2014, 2016, and 2018. For elections not falling in those years or special elections, please provide and group these rates with the next sequential election cycle. Where Facebook offered or sold advertising to multiple

candidates within the same race, please pair those quotes or prices together along with party affiliation.

People can run ads on Facebook, Instagram and Audience Network on any budget. The exact cost associated with an ad being shown to someone is determined in Facebook's ad auction.

55) Yes or no: has Facebook ever provided at no cost advertising to political candidates, campaign committees, political action committees or similar groups, or issue-advocacy groups or campaigns, whether through outright advertising or by altering search rankings, trending topics, content rankings, or the position of content within any suggested content mechanism?

a) If so, please provide each instance in which Facebook has done so and indicate whether Facebook offered similar support to any other candidate or issue in that race or election.

b) If so, please indicate whether Facebook coordinated with that campaign, candidate, or issue in doing so, or if Facebook acted unilaterally.

Political candidates, campaign committees, political action committees and similar groups, as well as issue advocacy groups and campaigns can set up Facebook Pages for free and post free content via those Pages, in the same way that any Page creator may. To run ads on Facebook, a form of payment must be provided. The algorithms that set content rankings are not designed to promote any candidate or party.

56) Please list and describe all mandatory trainings that Facebook employees are required to undergo and the topics involved in each, including any trainings on sexual harassment, unconscious bias, racial privilege, and inclusivity.

At Facebook, we treat any allegations of harassment, discrimination, or retaliation with the utmost seriousness, and we have invested significant time and resources into developing our policies and processes. We have made our policies and processes available publicly—not because we think we have all the answers, but because we believe that the more companies are open about their policies, the more we can all learn from one another. Our internal policies on sexual harassment and bullying are available on our Facebook People Practices website (http://peoplepractices.fb.com/), along with details of our investigation process and tips and resources we have found helpful in preparing our Respectful Workplace internal trainings. Our philosophy on harassment, discrimination, and bullying is to go above and beyond what is required by law. Our policies prohibit intimidating, offensive, and sexual conduct even when that conduct might not meet the legal standard of harassment. Even if it's legally acceptable, it's not the kind of behavior we want in our workplace. In developing our policies, we were guided by six basic principles:

- First, develop training that sets the standard for respectful behavior at work, so people understand what's expected of them right from the start. In addition to prescribing mandatory harassment training, we wrote our own unconscious bias training program at Facebook, which is also available publicly on our People Practices website. Our training includes Sustainable Equity, a three-day course in the US about racial privilege and injustice, and Design for Inclusion, a multi-day course in the UK to educate on systemic inequity.

- Second, treat all claims—and the people who voice them—with seriousness, urgency, and respect. At Facebook, we make sure to have HR business partners available to support everyone on the team, not just senior leaders.

- Third, create an investigation process that protects employees from stigma or retaliation. Facebook has an investigations team made up of experienced HR professionals and lawyers trained to handle sensitive cases of sexual harassment and assault.

- Fourth, follow a process that is consistently applied in every case and is viewed by employees as providing fair procedures for both victims and those accused.

- Fifth, take swift and decisive action when it is determined that wrongdoing has occurred. We have a zero-tolerance policy, and that means that when we are able to determine that harassment has occurred, those responsible are fired. Unfortunately, in some cases investigations are inconclusive and come down to one person's word against another's. When we don't feel we can make a termination decision, we take other actions designed to help everyone feel safe, including changing people's roles and reporting lines.

- Sixth, make it clear that all employees are responsible for keeping the workplace safe—and anyone who is silent or looks the other way is complicit. There's no question that it is complicated and challenging to get this right. We are by no means perfect, and there will always be bad actors. Unlike law enforcement agencies, companies don't have access to forensic evidence and instead have to rely on reported conversations, written evidence, and the best judgment of investigators and legal experts. What we can do is be as transparent as possible, share best practices, and learn from one another—recognizing that policies will evolve as we gain experience. We don't have everything worked out at Facebook on these issues, but we will never stop striving to make sure we have a safe and respectful working environment for all our people.

We are also working to reduce unconscious bias. Our publicly available Managing Unconscious Bias class encourages our people to challenge and correct bias as soon as they see it—in others, and in themselves. We've also doubled down by adding two additional internal programs: Managing Inclusion, which trains managers to understand the issues that affect marginalized communities, and Be The Ally, which gives everyone the common language, tools, and space to practice supporting others.

57) Please list and describe all optional recommended trainings that Facebook employees are required to undergo and the topics involved in each, including any trainings on sexual harassment, unconscious bias, racial privilege, and inclusivity.

See Response to Question 56.

58) Do any of the materials Facebook uses in any of these trainings identify different preferences, values, goals, ideas, world-views, or abilities among individuals on the basis of the following? If so, please list each and include those materials.

a) Race

b) Sex

c) Sexual orientation

d) Place of origin

Diversity is core to our business at Facebook and we're committed to building and maintaining a workforce as diverse and inclusive as the people and communities we serve. We have developed and implemented programs and groups to help build a more diverse and inclusive company, and to better engage and support employees from diverse backgrounds. We have a number of Facebook Resource Groups (FBRGs) that are run by our internal communities from different backgrounds, such as Asians and Pacific Islanders, African-Americans, People with Disabilities, those of faith, Latinos/Hispanics, LGBTQ, Veterans, and women. These FBRGs provide members with support, foster understanding between all people, and can coordinate programming to further support members. Examples of such programs include Women@ Leadership Day, Black@ Leadership Day, Latin@ Leadership Day, and Pride@ Leadership Day. Facebook also values and creates programming to support its Veterans and People with Disabilities through dedicated program managers and recruiters, mentoring programs and awareness campaigns to promote education and inclusion. These groups and programs are created to support and provide a more inclusive work experience for people from diverse backgrounds, with membership and participation open even to those who do not self-identify with these groups. For example, people who do not self-identify as Black are still members of Black@ and have attended Black@ Leadership Day, and there are male members of Women@ and men can attend Women@ Leadership Day. Facebook is also an Equal Opportunity Employer.

59) Facebook acknowledges that it is located in a very liberal part of the country, and has suggested that it understands that many of its employees as well as the surrounding community share a particular (very liberal) culture.

a) Does Facebook have any training specifically aimed at discouraging political, ideological, or partisan bias in decision-making by its employees?

b) Does Facebook have any training specifically aimed at discouraging political, ideological, or partisan bias in hiring, retention, promotion, and firing of its employees?

c) Does Facebook have any training specifically aimed at discouraging political, ideological, or partisan bias in the monitoring and supervision of content, users, or advertisements on each of its platforms?

Our Community Standards are global and all reviewers use the same guidelines when making decisions.

They undergo extensive training when they join and, thereafter, are regularly trained and tested with specific examples on how to uphold the Community Standards and take the correct action on a piece of content. This training includes when policies are clarified, or as they evolve.

We seek to write actionable policies that clearly distinguish between violating and non-violating content and we seek to make the decision making process for reviewers as objective as possible.

Our reviewers are not working in an empty room. There are quality control mechanisms as well as management on site to help or seek guidance from if needed. When a reviewer isn't clear on the action to take based on the Community Standards, they can pass the content decision to another team for review.

We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

When we're made aware of incorrect content removals, we review them with our Community Operations team so as to prevent similar mistakes in the future.

We recently introduced the right to appeal our decisions on individual posts so users can ask for a second opinion when they think we've made a mistake. As a first step, we are launching appeals for posts that were removed for nudity / sexual activity, hate speech or graphic violence. We are working to extend this process further, by supporting more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up. We believe giving people a voice in the process is another essential component of building a fair system.

60) Please list the names of any third-party organizations or vendors that Facebook uses to facilitate its trainings.

We have a comprehensive training program that includes many hours of live instructor-led training, as well as hands-on practice for all of our reviewers.

All training materials are created in partnership with our policy team and in-market specialists or native speakers from the region.

After starting, reviewers are regularly trained and tested with specific examples on how to uphold the Community Standards and take the correct action on a report. Additional training happens continuously and when policies are clarified, or as they evolve.

61) In the last five years, how many discrimination complaints has Facebook received from Christians? Please indicate how these complaints were resolved.

Decisions about content are made based on whether content violates our Community Standards. A user's personal characteristics do not influence the decisions we make, and Facebook does not track the religious beliefs or other personal characteristics of complainants.

62) Yes or no: Does Facebook offer any compensation, amenities, trainings, or similar services to its employees on account of their race, sex, sexual orientation, or religious affiliation? If so, please list each and whether all other races, sexes, etc. are provided the same compensation, amenity, etc.

See Response to Question 58.

63) In August 2017, Google fired James Damore for violating its code of conduct after Damore submitted an internal memo criticizing the company's hiring practices and arguing that the company's political bias created a negative work environment.

a) Yes or no: Does Facebook agree with Google's decision to fire James Damore?

b) Would an individual at Facebook have been fired for publishing a memorandum like Damore's? Assume no previous negative disciplinary history.

c) Does Facebook permit employees to believe that some portion of the career differences between men and women are the result of differing choices between the sexes?

i) Would a Facebook employee be disciplined for mentioning that opinion in a conversation to a willing participant?

ii) Would a Facebook employee be disciplined for mentioning that opinion on his or her Facebook account?

d) Does Facebook permit employees to criticize its "diversity" efforts as being racist against whites or sexist against men?

i) Would a Facebook employee be disciplined for mentioning that opinion in a conversation to a willing participant?

ii) Would a Facebook employee be disciplined for mentioning that opinion on his or her Facebook account?

We try to run our company in a way where people can express different opinions internally. We are not in a position to comment on the personnel decisions of another company or to engage in speculation about how we might respond in particular hypothetical circumstances.

64) In October 2017, Prager University filed suit against Google and Youtube, alleging that the two companies illegally discriminated against Prager University because of its conservative political perspective. As evidence, Prager University pointed to the dozens of educational videos that Youtube either put in "restricted mode" or demonetized.

a) Yes or no: Does Facebook agree with YouTube/Google's decision to restrict the following Prager University video, and if so, why?

i) The World's Most Persecuted Minority: Christians?

ii) Israel's Legal Founding?

iii) Are the Police Racist?

iv) Why Did America Fight the Korean War?

v) What Should We Do About Guns?

vi) Why America Must Lead?

vii) The Most Important Question About Abortion?

b) Yes or no: Does Facebook agree with YouTube/Google's decision to demonetize the following Prager University video, and if so, why?

i) Are The Police Racist?

ii) Israel's Legal Founding

iii) The Most Important Question About Abortion?

iv) Who's More Pro-Choice: Europe or America?

v) Why Do People Become Islamic Extremists?

vi) Is the Death Penalty Ever Moral?

vii) Why Isn't Communism as Hated as Nazism?

viii) Radical Islam: The Most Dangerous Ideology?

ix) Is Islam a Religion of Peace?

See Response to Question 27.

65) Recently, Jack Dorsey, Twitter's CEO, praised an article by two Democrats calling for a "new civil war" against the Republican Party, in which "the entire Republican Party, and the entire conservative movement that has controlled it for the past four decades" will be given a "final takedown that will cast them out" to the "political wilderness" "for a generation or two."

a) Does you agree with the premise of this article? It is located here: https://medium.com/s/state-of-the-future/the-great-lesson-of-california-in-americas-new-civil-war-e52e2861f30

b) Do you or Facebook believe it is appropriate for its platform or company to call for a "new civil war?"

c) Do you or Facebook believe it is appropriate for its platform or company to call for an end to one of the Nation's two major political parties?

d) Do you or Facebook believe it is appropriate for its platform or company to call for an end to the conservative movement?

e) Do you or Facebook condemn Twitter for calling for an end to the Republican Party?

f) Do you or Facebook condemn Twitter for calling for an end to the conservative movement?

g) Do you or Facebook condemn Twitter for calling for a new American civil war?

We are not in a position to comment on the decisions of another company or on another company's executive's statements about a news articles.

We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

66) Does Facebook collect information regarding its users':

a) Usage of non-Facebook apps?

b) Email?

c) Audio or ambient sound?

d) Telephone usage?

e) Text messaging?

f) iMessaging?

g) Physical location when the user is not using the Facebook app?

h) Spending?

As explained in our Data Policy, we collect three basic categories of data about people:

1) data about things people do and share (and who they connect with) on our services,

2) data about the devices people use to access our services, and

3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—i.e., their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

67) Does Facebook give its users the opportunity to opt out of Facebook collecting its users' data while still using the service?

The Ad Preferences tool on Facebook shows people the advertisers whose ads the user might be seeing because they visited the advertisers' sites or apps. The person can remove any of these advertisers to stop seeing their ads.

In addition, the person can opt out of these types of ads entirely—so he or she never sees those ads on Facebook based on information we have received from other websites and apps.

We've also announced plans to build Clear History, a feature that will enable people to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make user experience on Facebook better.

If a user clears his or her history or uses the new setting, we'll remove identifying information so a history of the websites and apps the user used won't be associated with the user's account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with the user's account, and as always, we don't tell advertisers who users are.

It will take a few months to build Clear History. We'll work with privacy advocates, academics, policymakers and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world, and heard specific demands for controls like these at a session we held at our headquarters. We're looking forward to doing more.

68) Yes or no: In preparation for the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of the U.S. Senators scheduled to take part in the hearing?

a) If so, please identify the Facebook pages visited and the information sought.

b) If so, please identify the individuals who sought such information and what information they obtained.

c) If so, please identify all individuals who possessed or reviewed that information.

While Facebook employees regularly look at the public pages of members of Congress to track the issues that are important to them, we are confident that no employees accessed any private data on personal profiles to prepare for the hearing or the questions for the record.

69) Yes or no: In preparation for the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of U.S. Senators' family members?

a) If so, please identify the Facebook pages visited and the information sought.

b) If so, please identify the individuals who sought such information and what information they obtained.

c) If so, please identify all individuals who possessed or reviewed that information.

See Response to Question 68.

70) Yes or no: In preparation for the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of any Senate employees?

a) If so, please identify the Facebook pages visited and the information sought.

b) If so, please identify the individuals who sought such information and what information they obtained.

c) If so, please identify all individuals who possessed or reviewed that information.

See Response to Question 68.

71) Yes or no: In responding to these or any other questions for the record arising from the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of the U.S. Senators scheduled to take part in the hearing?

a) If so, please identify the Facebook pages visited and the information sought.

b) If so, please identify the individuals who sought such information and what information they obtained.

c) If so, please identify all individuals who possessed or reviewed that information.

See Response to Question 68.

72) Yes or no: In responding to these or any other questions for the record arising from the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of U.S. Senators' family members?

a) If so, please identify the Facebook pages visited and the information sought.

b) If so, please identify the individuals who sought such information and what information they obtained.

c) If so, please identify all individuals who possessed or reviewed that information.

See Response to Question 68.

73) Yes or no: In responding to these or any other questions for the record arising from the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of U.S. Senate employees?

a) If so, please identify the Facebook pages visited and the information sought.

b) If so, please identify the individuals who sought such information and what information they obtained.

c) If so, please identify all individuals who possessed or reviewed that information.

See Response to Question 68.

74) Yes or no: Does Facebook collect data on individuals who are not registered Facebook users?

a) If so, does Facebook use this data as part of the advertising products it sells?

b) If so, does Facebook share or has Facebook ever shared this data with third parties?

Facebook does not create profiles for people who do not hold Facebook accounts.

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 Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. 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.

75) To the extent that Facebook collects and uses data from individuals who are not registered Facebook users, has Facebook gained consent from those individuals to collect and use their personal data?

Facebook does not create profiles about or track web or app browsing history for people who are not registered users of Facebook.

76) To the extent that Facebook collects and uses data from individuals who are registered Facebook users, has Facebook obtained those individuals' informed consent on an opt-in basis prior to the acquisition of that data?

a) If so, please provide the basis for concluding that data was acquired on an informed consent basis.

b) If so, please provide the basis for concluding that users opted-in to Facebook's collection and commercialization of their data.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information. After joining Facebook, people are presented with the opportunity to consent to additional data collection and uses, such as the use of location or the users' address book on their mobile device.

In response to your specific questions, depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

Things users and others do and provide.

- **Information and content users provide.** We collect the content, communications and other information users provide when they use our Products, including when they sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content they provide (like metadata), such as the location of a photo or the date a file was created. It can also include what they see through features we provide, such as our camera, so they can do things like suggest masks and filters that users might like, or give them tips on using camera formats. Our systems automatically process content and communications users and others provide to analyze context and what's in them for the purposes described below.
    - **Data with special protections.** Users can choose to provide information in their Facebook profile fields or Life Events about their religious views, political views, who they are "interested in," or their health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) could be subject to special protections under the laws of a user's country.

- **Networks and connections**. We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how users interact with them across our Products, such as people users communicate with the most or groups they are part of. We also collect contact information if users choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping users and others find people they may know and for the other purposes listed below.

- **Users' usage.** We collect information about how users use our Products, such as the types of content they view or engage with; the features they use; the actions they take; the people or accounts they interact with; and the time, frequency and duration of their activities. For example, we log when users are using and have last used our Products, and what posts, videos and other content users view on our Products. We also collect information about how users use features like our camera.

- **Information about transactions made on our Products.** If users use our Products for purchases or other financial transactions (such as when they make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as their credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.

- **Things others do and information they provide about users.** We also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about users, such as when others share or comment on a photo of them, send a message to them, or upload, sync or import their contact information.

Device Information

- As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices users use that integrate with our Products, and we combine this information across different devices users use. For example, we use information collected about users' use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone on a different device.

- Information we obtain from these devices includes:

    - **Device attributes:** information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.

- **Device operations:** information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).

- **Identifiers:** unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts users use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).

- **Device signals:** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.

- **Data from device settings:** information users allow us to receive through device settings they turn on, such as access to their GPS location, camera, or photos.

- **Network and connections:** information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help users stream a video from their phone to their TV.

- **Cookie data:** data from cookies stored on a user's device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy (https://www.facebook.com/policies/cookies/) and Instagram Cookies Policy (https://www.instagram.com/legal/cookies/)

Information from partners.

- Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about users' activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a user plays, or a business could tell us about a purchase a user made in its store. We also receive information about users' online and offline actions and purchases from third-party data providers who have the rights to provide us with users' information.

- Partners receive users' data when users visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share users' data before providing any data to us.

77) **Yes or no: Does Facebook give non-Facebook users a reasonable opportunity to learn what information has been collected about them by Facebook? If yes, please describe how.**

Yes. If a person doesn't have a Facebook account but believes Facebook may have information about them, they can contact us to request a copy of their information. A contact form is available at https://www.facebook.com/help/contact/180237885820953.

However, Facebook does not create profiles about or track web or app browser behavior of non-users.

78) During the April 10, 2018 joint committee hearing, you stated, "Every piece of content that you share on Facebook, you own and you have complete control over who sees it and—and how you share it, and you can remove it at any time." To corroborate that statement, you cited multiple mechanisms provided by Facebook that allow users to locate, edit, download, and delete information collected about them by Facebook.

a) Yes or no: Does Facebook offer non-Facebook users the same opportunities to control and edit any data collected about them by Facebook?

A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We believe everyone deserves good privacy controls. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so. However, non-Facebook users cannot post content on Facebook. Accordingly, there are not corresponding controls for non-Facebook users.

b) Facebook's "Privacy Basics" on deleting posts states "Hiding lets you keep your post but no one else will be able to see it when they view your Timeline. Note that it might still show up in search results and other places on Facebook."

i) How does an individual have "complete control" over their data if a post that has been hidden still shows up "in search results and other places on Facebook?"

A user can delete any post they have made. If they do so, it will not appear in search results and in other places on Facebook. The language you refer to appears in a feature that allows people to hide—not delete—content from their personal timeline. That is, a person can choose to delete a post that they have made from Facebook entirely, or they can choose to hide a post from their timeline even though it may be visible in other places on Facebook.

ii) Does Facebook give users an opportunity delete their content or information from these "other places" or search results?

Yes. See Response to Question 78(b)(i).

iii) Does Facebook give non-users an opportunity to delete content containing or relating to them from these "other places" or search results?

Since this passage refers to content created by Facebook users and whether it's visible on their timeline, this does not apply to non-users. See the responses to the sub-questions above and below.

c) If a Facebook user deletes a post will it show up in search results and other places on Facebook? If so, please describe the other places on Facebook in which a deleted post may appear.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

d) If a Facebook user deletes his account, will any of his data show up in search results and other places on Facebook?

See Response to Question 78(c).

i) Will Facebook retain any of his data for any purpose? If so, please describe what data and for what purposes.

See Response to Question 78(c).

79) Yes or no: does Facebook employ facial-recognition technology?

a) If so, does Facebook collect user data using facial-recognition technology?

b) If so, does Facebook collect data on individuals who are not registered Facebook users using facial-recognition technology?

c) If yes, does Facebook allow third-parties access to its facial-recognition technology or related information obtained as a result of the technology?

d) If yes, does Facebook allow government entities access to its facial recognition technology and/or the information obtained as a result of the technology?

e) To the extent that Facebook uses facial-recognition technology, what policies and procedures does Facebook have to safeguard information and data collected using that technology?

f) Does Facebook offer individuals, whether registered users or not, any opportunity to not be subject to facial-recognition technology or to have data collected using facial-recognition technology deleted?

g) Yes or no: Will Facebook commit to not using its facial-recognition technology to assemble data on individuals who have never consented to being part of Facebook?

Facebook uses facial recognition technology to provide people with products and features that enhance online experiences for Facebook users while giving them control over this technology. Facebook's facial recognition technology helps people tag their friends in photos; gives people an easier and faster way to privately share their photos with friends; helps people with visual impairments by generating descriptions of photos that people using screen readers can hear as they browse Facebook; lets people know when a photo or video of them has been uploaded to Facebook, even if they are not tagged; and helps prevent people from impersonating other Facebook users.

Facial recognition technology uses machine-learning algorithms to analyze the pixels in photos and videos in which a user is tagged, and the photo used by the person as his or her profile picture, and generates a unique number called a template. When a photo or video is uploaded to Facebook, Facebook uses the template to attempt to identify someone by determining whether there are any faces in that content, and analyzing the portion of the image in which the face appears to compare it against certain Facebook users depending on the purpose for which facial recognition is being performed.

Facebook has not shared and does not have plans to share or make available to any third party its facial recognition templates. Moreover, these templates do not provide meaningful information on their own; they can be used to identify a person only in conjunction with Facebook's software. They could not be reverse-engineered to recreate someone's face.

Facebook designed its facial-recognition technology and the applications that use it with privacy considerations in mind and incorporated various safeguards and controls that protect both (1) users' ability to control the collection, use, and disclosure of their personal information, and (2) the security of that personal information.

Facebook gives users control over whether Facebook uses facial recognition to recognize them in photos and videos. That control is exercised through users' privacy settings. If a user chooses to turn facial recognition off, Facebook does not create a template for that person or deletes any template it has previously created. Facebook will then be unable to recognize that person in any photos or videos that are uploaded to the service. Facebook also deletes templates of people who delete their Facebook accounts. Additionally, Facebook does not maintain templates for users who have no photos tagged of themselves and do not have a profile photo that is capable of being used to generate a face signature or template (e.g., where a user has no

profile photo, where a user's profile photo does not contain a human face, or where a user's profile photo contains multiple untagged faces).

We inform people about our use of facial-recognition technology through the Data Policy, Help Center, posts on Facebook, and direct user notifications. Facebook users are told that they can opt out of facial recognition at any time—in which case Facebook will delete their template and will no longer use facial recognition to identify them.

In creating facial recognition templates, Facebook uses only data that people have voluntarily provided to Facebook: the photos and videos that people have voluntarily uploaded to Facebook (including public profile pictures) and the tags people have applied to those photos and videos. Facebook does not use facial recognition to identify someone to a stranger.

80) Yes or no: does Facebook collect users' audio or visual information for any reason whatsoever, or otherwise activate, monitor, or capture data from a microphone or camera from a user's phone without the user's contemporaneous knowledge and express, contemporaneous consent? If so, please list each and every instance under which Facebook does so.

No, Facebook does not engage in these practices or capture data from a microphone or camera without consent. Of course, we do allow people to take videos on their devices and share those on our platform.

81) Will Facebook commit to not using its platform to gather such audio or visual information surreptitiously?

See Response to Question 80.

82) During the April 11, 2018 House Energy and Commerce Hearing, you stated, "there may be specific things about how you use Facebook, even if you're not logged in, that we keep track of, to make sure that people aren't abusing the systems." You further stated that "in general, we collect data on people who have not signed up for Facebook for security purposes."

a) What categories of data does Facebook collect about registered users' activity on websites and mobile applications other than Facebook?

b) What categories of data does Facebook collect about individuals who are not registered Facebook users and their activity on websites and mobile applications other than Facebook?

c) To the extent Facebook collects such data, does Facebook sell or provide this data to third parties?

d) To the extent Facebook collects such data, has Facebook gained consent from those individuals to collect and use their personal data?

e) To the extent Facebook gathers such data, what opportunity does Facebook provide to individuals not using Facebook to know, correct, or delete any information Facebook has gathered and retained about them?

See Response to Question 74.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

83) Most of your answers to the questions you received on April 10, 2018, and likely most of the answers to these questions for the record, will depend on information that Facebook alone possesses.

a) Why is/are Facebook's content-suggesting algorithm(s) secret?

b) Why are Facebook's editorial decisions secret?

See Response to Question 74.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

84) Numerous Americans receive all or a significant portion of their news from Facebook, which, in turn, suggests that news to them based on an algorithm that determines appropriate content based on criteria known only to Facebook.

a) To what extent will Facebook make public the criteria on which this algorithm relies?

b) To what extent will Facebook make public any changes that it makes to this or similar algorithms?

Facebook is a distribution platform that reflects the conversations already taking place in society. We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help.

As to the questions regarding ranking and algorithmic changes, see Response to Question 47.

85) Facebook conducts numerous social experiments on its users, examining everything from the effects of Facebook on voter turnout to the effects of Facebook on the mood of its users.

a) Will Facebook commit to not experimenting on its users without express, informed consent in advance?

b) Will Facebook commit to making the results of any such experiments known publicly?

c) Will Facebook commit to not experimenting on human subjects at all?

Facebook does research in a variety of fields, from systems infrastructure to user experience to artificial intelligence to social science. We do this work to understand what we should build and how we should build it, with the goal of improving the products and services we make available each day. We're committed to doing research to make Facebook better, but we want to do it in the most responsible way.

In October 2014, we announced a new framework that covers both internal work and research that might be published:

- Guidelines: we've given researchers clearer guidelines. If proposed work is focused on studying particular groups or populations (such as people of a certain age) or if it relates to content that may be considered deeply personal (such as emotions) it will go through an enhanced review process before research can begin. The guidelines also require further review if the work involves a collaboration with someone in the academic community.

- Review: we've created a panel including our most senior subject-area researchers, along with people from our engineering, research, legal, privacy and policy teams, that will review projects falling within these guidelines. This is in addition to our existing privacy cross-functional review for products and research.

- Training: we've incorporated education on our research practices into Facebook's six-week training program, called bootcamp, that new engineers go through, as well as training for others doing research. We'll also include a section on research in the annual privacy and security training that is required of everyone at Facebook.

- Research website: our published academic research is now available at a single location (https://research.facebook.com/) and will be updated regularly.

We believe in research because it helps us build a better Facebook. Like most companies today, our products are built based on extensive research, experimentation and testing.

It's important to engage with the academic community and publish in peer-reviewed journals, to share technology inventions and because online services such as Facebook can help us understand more about how the world works. We want to do this research in a way that

honors the trust users put in us by using Facebook every day. We will continue to learn and improve as we work toward this goal.

86) What, if any, procedures does Facebook employ to verify the identities of individuals who purchase or employ data from Facebook?

Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

Our Data Policy makes clear the circumstances in which we work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

87) Research and reporting by NYU Professor of Marketing Scott Galloway suggests that, combined, Facebook and Google (parent company now known as Alphabet) are together worth approximately $1.3 trillion. He concludes that this figure exceeds the world's top five advertising agencies (WPP, Omnicom, Publicis, IPG, and Dentsu) with five major media companies (Disney, Time Warner, 21st Century Fox, CBS, and Viacom) and still need to add five major communications companies (AT&T, Verizon, Comcast, Charter, and Dish) approach 90% of Facebook and Google's combined worth.

a) What business or product lines does Facebook consider itself to be in?

i) On what basis does Facebook make that determination?

ii) Who does Facebook consider its major competitors in each of these business or product lines?

b) Of those business or product lines, what market share does Facebook believe that it has?

c) What other entities provide *all* of the services that Facebook does in one place or platform, if any?

d) What other entities provide *any* of the services that Facebook does?

e) What is the relevant product market for Facebook (the platform)?

f) What are the relevant product markets for each of Facebook's products?

g) What is the relevant geographic market for Facebook (the platform)?

h) What is the relevant geographic market for each of Facebook's products?

i) Given these relevant geographic and product markets, what is Facebook's market share in each distinct market in which it operates?

j) What procedures, tools, programs, or calculations does Facebook use to ascertain its market position relevant to its five largest competitors overall (if five exist)?

k) What procedures, tools, programs, or calculations does Facebook use to ascertain its market position relevant to its five largest competitors in each product market (if five exist)?

In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if a user wants to share a photo or video, they can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if a user is looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services their mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon or Snapchat. Facebook represents a small part (in fact, just 6%) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

88) As you indicated in your testimony, Facebook's business model relies on advertising to individuals, typically through tailored advertisements. This means that Facebook has monetized access to the information that those individuals have published on Facebook.

a) To Facebook's best approximation, what is the total value of all user information that Facebook has acquired or to which Facebook has access?

Facebook generates substantially all of its revenue from selling advertising placements to third parties. Our total revenue and the percentage of which comes from third-party ads is below. This information is from our SEC filings.

2017: 40,653,000,000 (98% from third party ads)

2016: 27,638,000,000 (97% from third party ads)

2015: 17,928,000,000 (95% from third party ads)

2014: 12,466,000,000 (92% from third party ads)

2013: 7,872,000,000 (89% from third party ads)

2012: 5,089,000,000 (84% from third party ads)

2011: 3,711,000,000 (85% from third party ads)

2010: 1,974,000,000 (95% from third party ads)

2009: 777,000,000

2008: 272,000,000

b) How does Facebook categorize individual pieces of information for purposes of monetizing that information? (For example, Facebook acknowledges that if it is approached by a company selling ski equipment, it will target ads to individuals who have expressed an interest in skiing. We want to know in what ways Facebook organizes this information.)

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests.

We use data from each of the categories described above to obtain these interests and to personalize every aspect of our services, which is the core value we offer and the thing that makes Facebook services unique from other online experiences. This includes selecting and ranking relevant content, including ads, posts, Page recommendations, to cite but a few examples.

For example, we use the data people provide about their age and gender to help advertisers show ads based on those demographics but also to customize the pronouns on our site and deliver relevant experiences to those users.

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, so we can rank posts relating to those interests higher in NewsFeed, for example, or enable advertisers to reach audiences—i.e., groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them organic posts from friends who have been in that location or we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of email addresses of people they would like to reach on Facebook. 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).

Again, for people who are new to Facebook, we may have minimal data that we can use to personalize their experience, including their NewsFeed, their recommendations and the content (organic and sponsored) that they see. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls.

As noted above, in addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

c) What types of advertisements does Facebook categorically prohibit?

Section 4 of our Advertising Policies list the types of ads that we categorically prohibit. These include ads that violate Community Standards, ads for illegal products and services, ads with adult content, ads that are misleading or false, ads that include profanity, and many more.

d) What external controls restrict how Facebook monetizes, sells, rents, or otherwise commercializes an individual's information? Please include (separately) any laws that Facebook views as applicable, any injunctions presently binding Facebook, any regulations directing how Facebook may monetize information, and any publicly available, independent audits of how Facebook monetizes information.

Facebook complies with all applicable laws. In addition, we adhere to the commitments set forth in our Data Policy, which describes how we collect and use data.

e) What internal controls restrict how Facebook monetizes, sells, rents, or otherwise commercializes an individual's information? Please include (separately) any internal policies, statements of ethics or principles, directives, guidelines, or prohibitions that Facebook routinely applies in determining whether to use an individual's personal information for commercial gain.

See Response to previous question.

89) When an individual chooses to "lock down" or otherwise publicly conceal his Facebook profile, does Facebook:

a) Continue to use that individual's private information for commercial gain? (This includes aggregating data as well as targeting advertisements at that individual.)

b) Continue to retain that individual's private information for its own archives or records?

When people post on Facebook—whether in a status update or by adding information to their profiles—the ability to input the information is generally accompanied by an audience selector. This audience selector allows the person to choose who will see that piece of information on Facebook—whether they want to make the information public, share it with friends, or keep it for "Only Me." The tool remembers the audience a user shared with the last time they posted something and uses the same audience when the user shares again unless they change it. This tool appears in multiple places, such as privacy shortcuts and privacy settings. When a person makes a change to the audience selector tool in one place, the change updates the tool everywhere it appears. The audience selector also appears alongside things a user has already shared, so it's clear who can see each post. After a person shares a post, they have the option to change who it is shared with.

The audience with which someone chooses to share their information is independent of whether we use that information to personalize the ads and other content we show them. Specifically, our Data Policy explains that we may use any information that people share on Facebook "to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads)." However, people can use our Ad Preferences tool to see the list of interests that we use to personalize their advertising. This means that, for example, a person who is interested in cars can continue to share that interest with their friends but tell us not to assign them an interest in ads for ad targeting purposes.

Likewise, the audience of a post does not determine whether a post is retained. Someone can choose to share a post with "Only Me" (meaning that they don't want anyone to see it but want to retain it in their Facebook account). They may also choose to delete the information entirely. When people choose to delete something they have shared on Facebook, we remove it from the site. In most cases, this information is permanently deleted from our servers; however, some things can only be deleted when a user permanently deletes their account.

90) What are Facebook's total advertising revenues for each of the calendar years 2001 to 2018?

Our total revenue and the percentage of which comes from third-party ads is below. This information is from our SEC filings.

2017: 40,653,000,000 (98% from third party ads)

2016: 27,638,000,000 (97% from third party ads)

2015: 17,928,000,000 (95% from third party ads)

2014: 12,466,000,000 (92% from third party ads)

2013: 7,872,000,000 (89% from third party ads)

2012: 5,089,000,000 (84% from third party ads)

2011: 3,711,000,000 (85% from third party ads)

2010: 1,974,000,000 (95% from third party ads)

2009: 777,000,000

2008: 272,000,000

a) What are Facebook's online advertising revenues for each of the calendar years 2001 to 2018?

b) What are Facebook's five largest competitors for online advertising in each year from 2001 to 2018?

i) What were each of those competitors' advertising revenues through each of those years?

ii) How many of Facebook's executive staff previously worked at each of those entities?

We expect that our competitors make their numbers available in their SEC filings. And, like many industries across the private sector, many people may work in multiple technology companies throughout the course of their careers.

91) Regardless of place of incorporation, does Facebook consider itself an American company?

Yes, we're an American-based company where ninety percent of our community are outside the US.

92) When Facebook makes policy decisions, are American citizens the company's top priority? If not, what is the company's top priority when it comes to policy decisions?

We are proud to be a US-based company that serves billions of people around the world. While the majority of our employees are located here in the United States, more than 80% of the people who use Facebook are outside this country. We consider the needs of all of our users when making policy decisions. Of course, with headquarters in the US and Ireland, we have particularly strong relationships with policy makers in those regions. We regularly engage with policy makers around the world, however, and work to take account of regional policy concerns as we build our products and policies for a global user base.

93) Facebook, WhatsApp, and Instagram have all reportedly been blocked or partially blocked from the People's Republic of China (PRC) since 2009.

a) Please describe the extent to which these services may be accessed from within the territory of the PRC, including Hong Kong and Macau, and describing in detail any geographical limits or limits on the available content.

Facebook, WhatsApp, and Instagram are available in Hong Kong and Macau. Facebook and Instagram are blocked in Mainland China. However, these can be accessed by people in Mainland China who employ VPNs. WhatsApp is typically available in Mainland China although we notice availability is often restricted around important events.

b) On what basis does Facebook evaluate whether to honor a foreign government's request to block specific content?

When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs.

c) How does Facebook determine whether to honor a foreign government's request to block specific content or users?

See Response to previous question.

d) Listed by country, what percentage of requests to block specific content (or users) from foreign governments does Facebook honor in whole or part?

This information is available here: https://transparency.facebook.com/content-restrictions.

e) How does Facebook determine whether to honor the U.S. government's request to block specific content or users?

Our Transparency Report contains data on restrictions we place on content that does not violate community standards but that is alleged to violate local law. We do not have any such reports for the United States.

f) What percentage of requests to block specific content (or users) from the U.S. government does Facebook honor in whole or part?

See Response to previous question.

94) Yes or no: Has Facebook made any alterations, modifications, or changes to the encryption security of WhatsApp in response to or as a result of the PRC government or any of its agencies or in order to comply with PRC law?

No.

a) If so, what changes has Facebook made to the encryption security?

b) Does Facebook program in "back doors" or other mechanisms to decrypt or otherwise decode encrypted information at a government's request?

No.

i) If so, under what circumstances does Facebook decrypt such data?

ii) If so, on what platforms does Facebook have such protocols?

c) Does Facebook make WhatsApp or Facebook information available to the PRC government on a searchable basis?

No.

95) Since 2014, the PRC government has held a World Internet Conference. Charles Smith, the co-founder of the non-profit censorship monitoring website GreatFire, described foreign guests of the Conference as "complicit actors in the Chinese censorship regime [that] are lending legitimacy to Lu Wei, the Cyberspace Administration of China and their heavy-handed approach to Internet governance. They are, in effect, helping to put all Chinese who stand for their constitutional right to free speech behind bars."

a) How many Facebook employees have attended the PRC's World Internet Conference?

b) Have any Facebook employees ever participated on any panels or advisory committees that are held or have been established by the World Internet Conference?

There have been four World Internet Conferences. Several Facebook employees have attended one or more of these four conferences.

i) If so, please list the employees and the panels or high-level advisory committees they have participated on.

One Facebook representative, Vaughan Smith, has participated in World Internet Conference panels and keynotes alongside representatives of other leading US technology companies, for example Tim Cook and Sundar Pichai. No employees participated in advisory

committees. Mr. Smith has provided keynotes on AI, innovation and how Facebook is building the knowledge economy.

ii) Has Facebook assisted other countries in designing regimes to monitor or censor Facebook content? If so, which countries, and under what circumstances? Please describe each.

When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs. This information is available here: https://transparency.facebook.com/content-restrictions.

Government criticism does not violate our community standards, and we do not evaluate or categorize accounts based on whether they engage in government criticism.

See also Response to Question 93(c)

c) Has Facebook ever provided any financial support to the World Internet Conference? If yes, please provide and itemize all financial support that has been provided to the World Internet Conference.

Facebook has not paid to participate in the World Internet Conference. In 2016 we paid $10,000 to rent exhibit space at the event to showcase Oculus VR which is manufactured in China.

96) Has Facebook ever temporarily shut down or limited access to Facebook, WhatsApp, or Instagram within a country or a specific geographic area, at the request of a foreign government or agency, including but not limited to, the PRC, the Islamic Republic of Iran, Syria, the Russian Federation, and Turkey?

a) If so, please describe each instance Facebook has complied with a foreign government's request to censor content or users, the requesting government, the provided justification for the government request, and a description of the content requested to be removed.

b) Please describe what if any policies Facebook has in place governing Facebook's responses to government censorship requests.

We do not block access to Facebook products and services in areas where they are otherwise generally available on the basis of specific government requests. We may independently limit access to certain functionality—such as peer-to-peer payments or facial recognition—in some jurisdictions based on legal and regulatory requirements.

In some instances, we may receive requests from governments or other parties to remove content that does not violate our Community Standards but is alleged to contravene local law. When we receive such requests, we conduct a careful review to confirm whether the report is legally valid and is consistent with international norms, as well as assess the impact of our response on the availability of other speech. When we comply with a request, we restrict the content only within the relevant jurisdiction. We publish details of content restrictions made pursuant to local law, as well as details of our process for handling these requests, in our Transparency Report (https://transparency.facebook.com/content-restrictions).

Questions from Senator Durbin

For questions with subparts, please answer each subpart separately.

1. **Mr. Zuckerberg, at your hearing I asked whether it is fair for users of Facebook to expect to know what information Facebook is collecting on them, who Facebook is sending the information to, and whether Facebook asked the user in advance for permission to do that. You answered "yes" and said "I think everyone should have control over how their information is used."**

   a. **In order for users to know what information Facebook is collecting on them, will Facebook commit to proactively notifying each Facebook user via email on at least an annual basis that the user can securely view all information that Facebook has collected on that user during the previous year and providing the user with instructions for how to do so?**

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 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 announced expansions to Download Your Information, which, among other things, will make it easier for 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, delete 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.

   b. **Will Facebook commit to proactively notifying each Facebook user via email on at least an annual basis that the user can securely view a list of all entities to which Facebook has sent any of the user's information during the previous year and providing the user with instructions on how to do so?**

Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can

manage their app settings is available at https://www.facebook.com/help/218345114850283?helpref=about_content.

The categories of information that an app can access are clearly disclosed before the user consents to use an app on the Facebook Platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

2. At your hearing, I pointed out that information is collected on users by Facebook and "sometimes, people have made money off of sharing that information" without the users' knowledge or advance consent. You responded by saying you would provide information about Facebook's developer platform, and I asked if you could provide that information for the record because of limited time. Please provide this information for the record.

In 2007, there was industry-wide interest in enriching and expanding users' experiences on various platforms by allowing them to take their data (from a device or service) to third-party developers to receive new experiences. For example, around that time, Apple and Google respectively launched their iOS and Android platforms, which were quickly followed by platform technologies and APIs that allowed developers to develop applications for those two platforms and distribute them to users through a variety of channels. Similarly, in 2007, Facebook launched a set of platform technologies that allowed third parties to build applications that could run on and integrate with the Facebook service and that could be installed by Facebook users who chose to do so. In December 2009, Facebook launched new privacy controls that enabled users to control which of the types of information that they made available to their friends could be accessed by apps used by those friends.

As with all of these platforms, the permissions model that governed the information that third-party applications could access from the Platform evolved. For example, in April 2010, Facebook launched granular data permissions (GDP), which allowed users to examine a list of categories of information that an app sought permission to access before they authorized the app.

Throughout the relevant period and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data obtained from Facebook or from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

In November 2013, when Kogan launched the app, apps generally could be launched on the Platform without affirmative review or approval by Facebook. The app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed the app to request permission from its users to bring their Facebook data (their own data and data shared with them by their friends) to the app, to obtain new experiences.

At that time, the Graph API V1 allowed app developers to request consent to access information from the installing user such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each

friend's own privacy settings) the same or similar categories of information the user's friends had shared with the installing user. Permitting users to share data made available to them by their friends had the upside of making the experience of app users more personalized and social. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his or her friends were listening to and (2) give the app permission to access the user's friend list and thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such access by third-party apps. In other words, Kogan's app could have accessed a user's friends' information only for friends whose privacy settings permitted such sharing.

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. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, email address, and a list of friends of the user who had installed and authorized the same app;

- Generally preventing new apps on the new platform from accessing friends data without review; and

- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API v.1.0 before we made technical changes to our platform to change this access.

The App Review process introduced in 2014 required developers who create an app that asks for more than certain basic user information to justify the data they are looking to collect and how they are going to use it. Facebook then reviewed whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for a user's permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018, including Kogan's second app. 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.

3. **At your hearing I asked you about Messenger Kids and asked "what guarantees can you give us that no data from Messenger Kids is or will be collected or shared" in ways that might violate the Children's Online Privacy Protection Act. You said "in general, that data is not going to be shared with third parties." I noted that your use of the qualifier "in general" "seems to suggest that in some circumstances it will be shared with third parties" You responded "no, it will not."**

    a. **Please describe any information collected via Messenger Kids that is shared by Facebook with any third party.**

We have no plans to include advertising in Messenger Kids. Moreover, there are no in-app purchases, and we do not use the data in Messenger Kids to advertise to children or their parents. In developing the app we assembled a committee of advisors, including experts in child development, online safety, and media and children's health, and we continue to work with them on an ongoing basis. In addition, we conducted roundtables with parents from around the country to ensure we were addressing their concerns and built the controls they need and want in the app. We are committed to approaching all efforts related to children 12 and under thoughtfully, and with the guidance and input of experts and parents.

    b. **Please confirm for the record that no data collected from Messenger Kids is, or will be, shared with third parties in violation of COPPA.**

See Response to Question 3a.

4. **At your hearing, I asked "would you be open to the idea that someone having reached adult age having grown up with Messenger Kids be allowed to delete the data you have collected?" You said "Senator, yes….I think it is a good idea to consider making sure that all that information is deleted."**

    a. **Will you commit to allow children, when they reach adulthood, to request that any information gathered about them by Facebook while they were under age 13 be deleted and will you commit that Facebook will comply with such requests?**

    b. **Do you support giving American internet users the ability to request the deletion of any and all information collected as a result of a user's online activities prior to age 13, and to require companies to delete such information when an individual has requested it?**

    c. **Do you think children would benefit from the ability to wipe clean the information that has been gathered and collected on them through their online activities before age 13?**

    d. **Do children deserve the chance to grow up and learn how to responsibly use the internet prior to age 13 without having their childhood internet data preserved in perpetuity by for-profit companies?**

Under our Messenger Kids Privacy Policy, available at https://www.facebook.com/legal/messengerkids/privacypolicy, Parents can control their

children's accounts. Through the Parent Dashboard in their Facebook (or Messenger) account, a parent or guardian can review and edit their child's Messenger Kids profile information, and remove contacts to prevent further communication with their child on Messenger Kids. In addition, a parent or guardian who has authorized the Messenger Kids app can see their child's interactions on Messenger Kids by accessing their child's account. In order to stop further collection and use of their child's personal information on Messenger Kids, a parent or guardian can delete their child's Messenger Kids account. If a parent deletes their child's account, Facebook deletes their Messenger Kids registration information, information about their activity and contacts, and device information, as described above. However, the messages and content a child sent to and received from others before their account was deleted may remain visible to those users.

5. What do you think is the maximum amount of time per day that a child under age 13 should spend using internet social media?

We are committed to working with parents and families, as well as experts in child development, online safety and children's health and media, to ensure we are building better products for families—that means building tools that promote meaningful interactions and help people manage their time on our platform and it means giving parents the information, resources and tools they need to set parameters for their children's use of online technologies and help them develop healthy and safe online habits. It also means continued research in this area.

Indeed, Messenger Kids, the only product we offer to children under the age of 13, includes Sleep Mode, which gives parents the ability to set parameters on when the app can be used, and the app does not have ads or in app purchases. In building the app, we worked closely with leading child development experts, educators, and parents to inform our decisions and we continue to work with them on an ongoing basis. Our advisors included experts in the fields of child development, online safety and children's media currently and formerly from organizations such as the Yale Center for Emotional Intelligence (http://ei.yale.edu/who-we-are/mission/), Connect Safely (http://www.connectsafely.org/about-us/), Center on Media and Child Health (http://cmch.tv/), Sesame Workshop (http://www.huffingtonpost.com/author/dr-lewis-bernstein) and more.

We also have a Parents Portal (https://www.facebook.com/safety/parents) and Youth Portal (https://www.facebook.com/safety/youth), which are both focused on fostering conversations around online safety, security, and well-being and giving parents and young people access to the information and resources they need to make informed decisions about their use of online technologies.

6. Does Facebook agree that states have a strong interest in protecting the privacy of their residents?

We believe strongly in providing meaningful privacy protections to people. This is why we work hard to communicate with people about privacy and build controls that make it easier for people to control their information on Facebook. For example, Facebook has redesigned its settings menu to make things easier to find and introduced new Privacy Shortcuts. These shortcuts allow users to make their account more secure, control their personal information,

control which ads they see, and control who sees their posts and profile information. Facebook has also introduced additional tools to find, download, and delete user data.

We've worked with regulators, legislators, and privacy experts, at both the state and national levels to educate people and businesses about privacy. We believe an important component of any privacy regulation is clear and consistent oversight and enforcement. We intend to continue this collaborative work to promote privacy protections for our community.

7. Does Facebook think companies should have to get Americans' consent before scanning and storing their biometric data?

Facebook uses facial recognition technology to provide people with products and features that enhance online experiences for Facebook users while giving them control over this technology. Facebook's facial recognition technology helps people tag their friends in photos; gives people an easier and faster way to privately share their photos with friends; helps people with visual impairments by generating descriptions of photos that people using screen readers can hear as they browse Facebook; lets people know when a photo or video of them has been uploaded to Facebook, even if they are not tagged; and helps prevent people from impersonating other Facebook users.

Facial recognition technology uses machine-learning algorithms to analyze the pixels in photos and videos in which a user is tagged, and the photo used by the person as his or her profile picture, and generates a unique number called a template. When a photo or video is uploaded to Facebook, Facebook uses the template to attempt to identify someone by determining whether there are any faces in that content, and analyzing the portion of the image in which the face appears to compare it against certain Facebook users depending on the purpose for which facial recognition is being performed.

Facebook has not shared and does not have plans to share or make available to any third party its facial recognition templates. Moreover, these templates do not provide meaningful information on their own; they can be used to identify a person only in conjunction with Facebook's software. They could not be reverse-engineered to recreate someone's face.

Facebook designed its facial-recognition technology and the applications that use it with privacy considerations in mind and incorporated various safeguards and controls that protect both (1) users' ability to control the collection, use, and disclosure of their personal information, and (2) the security of that personal information.

Facebook gives users control over whether Facebook uses facial recognition to recognize them in photos and videos. That control is exercised through users' privacy settings. If a user chooses to turn facial recognition off, Facebook does not create a template for that person or deletes any template it has previously created. Facebook will then be unable to recognize that person in any photos or videos that are uploaded to the service. Facebook also deletes templates of people who delete their Facebook accounts. Additionally, Facebook does not maintain templates for users who have no photos tagged of themselves and do not have a profile photo that is capable of being used to generate a face signature or template (e.g., where a user has no

profile photo, where a user's profile photo does not contain a human face, or where a user's profile photo contains multiple untagged faces).

We inform people about our use of facial-recognition technology through the Data Policy, Help Center, posts on Facebook, and direct user notifications. Facebook users are told that they can opt out of facial recognition at any time—in which case Facebook will delete their template and will no longer use facial recognition to identify them.

In creating facial recognition templates, Facebook uses only data that people have voluntarily provided to Facebook: the photos and videos that people have voluntarily uploaded to Facebook (including public profile pictures) and the tags people have applied to those photos and videos. Facebook does not use facial recognition to identify someone to a stranger.

8. Has Facebook advocated for any changes to the Illinois Biometric Information Privacy Act, either on its own or as the member of a trade association or state chamber of commerce?

We are aware of several pending measures to amend the Illinois Biometric Information Privacy Act to foster the use of technology to enhance privacy and data security and combat threats like fraud, identity theft, and impersonation. Facebook has not supported these measures or requested any organization or chamber of commerce to do so.

In 2016, Senator Terry Link, the author of the Illinois Biometric Information Privacy Act, introduced a measure (HB 6074) clarifying that the original law (1) does not apply to information derived from physical or digital photographs and (2) uses the term "scan" to mean information that is obtained from an in-person process. These clarifying amendments were consistent with industry's longstanding interpretation of the law and Facebook publicly supported them.

9. Would advocating for changes to the Illinois Biometric Identification Privacy Act be consistent with Facebook's commitment to protecting privacy?

Facebook's advocacy is consistent with our commitment to protecting privacy. As the findings of the Illinois General Assembly confirm, when people raise privacy concerns about facial recognition, they are generally about specific uses of facial recognition. In enacting the Illinois Biometric Information Privacy Act, the General Assembly explained that its concern was "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."

Facebook's use of facial recognition in our products, on the other hand, is very different. Facebook uses facial-recognition technology with users to provide Facebook users—who choose to join Facebook for the purpose of connecting with and sharing information about themselves with others, and affirmatively agree to Facebook's Terms of Service and Data Policy—with products and features that protect their identities and enhance their online experiences while giving them control over the technology. For example, Facebook uses facial-recognition technology to protect users against impersonators by notifying users when someone else has uploaded a photo of them for use as a profile photo and to enable features on the service to people who are visually impaired. Facebook also uses facial-recognition technology to suggest

that people who upload photos or videos tag the people who appear in the photos or videos. When someone is tagged in a photo or video, Facebook automatically notifies that person that he or she has been tagged, which in turn enables that person to take action if he or she does not like the content—such as removing the tag or requesting that the content be removed entirely. Facebook users have always had the ability to change their settings to prevent Facebook from using facial recognition to recognize them.

Given the very different uses of facial-recognition technology that exist, we believe that a one-size-fits-all approach to regulation of facial-recognition technology is not in the public's best interest, and we believe that clarification that the Illinois Biometric Information Privacy Act was not intended to apply to all uses of facial recognition is consistent with Facebook's commitment to protecting privacy. Furthermore, our commitment to support meaningful, thoughtfully drafted privacy legislation means that we can and do oppose measures that create confusion, interfere with legitimate law enforcement action, create unnecessary risk of frivolous litigation, or place undue burdens on people's ability to do business online.

10. Does Facebook oppose legislative efforts to revise and carve exceptions out of the Illinois Biometric Identification Privacy Act?

See Responses to Questions 8 and 9.

11. Last October, Facebook's general counsel, Colin Stretch, testified before the Senate Judiciary Subcommittee on Crime and Terrorism. I asked him about a letter that 19 leading civil rights organizations—including Muslim Advocates, The Leadership Conference on Civil and Human Rights, the NAACP, the Arab American Institute, Human Rights Campaign, and the Southern Poverty Law Center—sent to Facebook, which explained their "deep concern regarding ads, pages, and hateful content on your platform used to divide our country, and in particular, to promote anti-Muslim, anti-Black, anti-immigrant, and anti-LGBTQ animus."

The organizations referenced a number of examples that had previously been reported by the media, including a Russian Facebook account that "not only promoted anti-immigrant messaging online, but also managed to organize an in-person anti-refugee rally in Twin Falls, Idaho in August 2016." The letter also alleges that "Facebook offered its expertise to a bigoted advocacy group by creating a case study testing different video formats, and advising on how to enhance the reach of the group's anti-refugee campaign in swing states during the final weeks of the 2016 election."

Mr. Stretch agreed that the content was vile and responded that Facebook was "tightening our content guidelines as they apply to ads with respect to violence."

I know that Facebook has met with the groups that have expressed these concerns, but can you elaborate on the specific, substantive steps that Facebook has taken so far, and plans to take in the future, to combat violent hate content on your platform?

Facebook has engaged Relman, Dane & Colfax, a respected civil rights law firm, to 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.

On hate speech specifically, our policies prohibit direct attacks on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, or calls for exclusion or segregation, and we separate attacks into three tiers of severity.

We recently updated our hate speech policies to remove violent speech directed at groups of people defined in part by protected characteristics. Under the previous hate speech policy, a direct attack targeting women exclusively on the basis of gender, for example, would have been removed from Facebook, but the same content directed at women drivers would have remained on the platform. We have come to see that this distinction is a mistake, and we no longer differentiate between the two forms of attack when it comes to only the most violent hate speech. We continue to explore how we can adopt a more granular approach to hate speech.

In the last nine months, we have also made significant changes to advertising on Facebook, committing to a more robust ad review process and the hiring of 10,000 more people to aid in our safety and security efforts, increasing ads transparency, and tightening restrictions on advertiser content and targeting.

- **Strengthening enforcement.** Before any ad can appear on Facebook or Instagram, it must go through our ad review process. We rely on both automated and manual review, and we're taking aggressive steps to strengthen both. The process includes automated checks of an ad's images, text, targeting, and positioning, in addition to the content on the ad's Facebook and landing pages. Our automated systems also flag content for human review. We are increasing the size of our security and safety teams from 10,000 to 20,000 over the course of this year, and are simultaneously working to hire more people from African American and Hispanic communities. This will help increase the diversity of our workforce and improve our understanding and awareness of ads that are meant to exploit culturally sensitive issues. In addition, we are investing more in machine learning to better understand when to flag and take down ads.

- **Making advertising more transparent.** We believe that when users see an ad, they should know who ran it and what other ads they're running—which is why we show the Page name for any ads that run in a user's News Feed. To provide even greater transparency for people and accountability for advertisers, we're now building new tools that will allow users to see the other ads a Page is running as well—including ads that aren't targeted to them directly. We hope that this will establish a new standard for our industry in ad transparency. We try to catch content that shouldn't be on Facebook before it's even posted—but because this is not always possible, we also take action when people report ads that violate our policies. We hope that more transparency will mean more people can report inappropriate ads.

- **Tightening restrictions on advertiser content.** We hold people on Facebook to our Community Standards, and we hold advertisers to even stricter guidelines. Our ads policies already prohibit shocking content, direct threats and the promotion of the sale or use of weapons. Going forward, we are expanding these policies to prevent ads that use even more subtle expressions of violence.

- **Changes to advertiser targeting.** Being able to direct ads at a particular audience is particularly valuable for businesses and for people, but it's important that this be done in a safe and civil way. That's why we've been closely reviewing the targeting options we offer. Even though targeting is an important tool to reach people, we have heard concerns about potential abuse, particularly about the feature that lets advertisers exclude people from their ads. Advertisers want to show ads to people most likely to be interested in their offerings, and exclusion targeting helps avoid showing ads to people who likely aren't interested. For example, if a local basketball team is trying to attract new fans, they can exclude people who are already interested in the team. In response to the feedback we've received, we've removed thousands of categories from exclusion targeting. We focused mainly on topics that relate to potentially sensitive personal attributes, such as race, ethnicity, sexual orientation, and religion. Our review is continuous; the process will be ongoing and we'll continue soliciting feedback. We take our responsibility to keep advertising safe and civil seriously, and we will keep exploring more ways to make targeting work for people and businesses.

12. We have also seen the impact of hate content on the international stage. In Myanmar, United Nations investigators have found that Facebook has played a "determining role" in violence against the Muslim Rohingya population.

Specifically, the chairman of the U.N. Independent International Fact-Finding Mission on Myanmar told reporters that social media "has… substantively contributed to the level of acrimony and dissension and conflict, if you will, within the public. Hate speech is certainly of course a part of that. As far as the Myanmar situation is concerned, social media is Facebook, and Facebook is social media." Another investigator said that Facebook was used by ultra-nationalists who were "inciting a lot of violence and a lot of hatred against the Rohingya or other ethnic minorities."

In a recent interview with *Vox*, you suggested that Facebook's systems had detected inflammatory, widely-shared chain letters about imminent attacks, and that Facebook stopped those messages. In reality, a group of Myanmar civil society organizations had flagged this content, and the messages were shared thousands of times for three days before Facebook took steps to prevent the spread of the messages. After your interview, these organizations sent you a letter noting "this case exemplifies the very opposite of effective moderation: it reveals an over-reliance on third parties, a lack of a proper mechanism for emergency escalation, a reticence to engage local stakeholders around systemic solutions and a lack of transparency." I understand that you have personally responded to these organizations and that they have sent you a follow-up letter asking for additional information on how Facebook is addressing these issues.

The situation in Myanmar is not unique. Violent anti-Muslim content is also widely shared in Sri Lanka and recently led the Sri Lankan government to temporarily ban access to Facebook. A recent *Buzzfeed* report stated:

> **Government officials, researchers, and local NGOs say they have pleaded with Facebook representatives from as far back as 2013 to better enforce the company's own rules against using the platform to call for violence or to target people for their ethnicity or religious affiliation. They repeatedly raised the issue with Facebook representatives in private meetings, by sharing in-depth research, and in public forums. The company, they say, did next to nothing in response.**
>
> **Ethnic tensions run deep in Sri Lanka, particularly between the majority Sinhala Buddhists and minority groups, and the country has seen a troubling rise in anti-Muslim hate groups and violence since the end of its decades-long civil war in 2009. Many of those hate groups spread their messages on Facebook. The problem came to a head in March when Buddhist mobs in central Sri Lanka burned down dozens of Muslim shops, homes, and places of worship.**

a. What is your response to these reports?

b. What steps is Facebook taking to address anti-Muslim hate content in countries like Sri Lanka and Myanmar?

We've been too slow to deal with the hate and violence in places like Myanmar and Sri Lanka. The challenges we face in a country that has fast come online are very different than those in other parts of the world, and we are investing in people, technology, and programs to help address them as effectively as possible.

We are increasing the number of Burmese and Sinhalese-language content reviewers as we continue to grow and invest in Myanmar and Sri Lanka. Our goal is always to have the right number of people with the right native language capabilities to ensure incoming reports are reviewed quickly and effectively. That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are supplementing our hiring with investments in technology and programs.

We are building new tools so that we can more quickly and effectively detect abusive, hateful, or false content. We have, for example, designated several hate figures and organizations for repeatedly violating our hate speech policies, which has led to the removal of accounts and content that support, praise, or represent these individuals or organizations. We are also investing in artificial intelligence that will help us improve our understanding of dangerous content.

We are further strengthening our civil society partner network so that we have a better understanding of local context and challenges. We are focusing on digital literacy education with local partners in Myanmar and Sri Lanka. For example, we launched a local language version of our Community Standards to educate new users on how to use Facebook responsibly in 2015 and we have been promoting these actively in Myanmar, reaching over 8 million people through promotional posts on our platform alone. We've also rolled out several education programs and workshops with local partners to update them on our policies and tools so that they can use this

information in outreach to communities around the country. One example of our education initiatives is our work with the team that developed the Panzagar initiative (https://www.facebook.com/supportflowerspeech) to develop the Panzagar counterspeech Facebook stickers to empower people in Myanmar to share positive messages online. We also recently released locally illustrated false news tips, which were promoted on Facebook and in consumer print publications. We have a dedicated Safety Page for Myanmar (https://www.facebook.com/safety/resources/myanmar) and have delivered hard copies of our local language Community Standards and safety and security tips to civil society groups in Myanmar who have distributed them around the country for trainings. Similarly, in Sri Lanka, we ran a promotion in English, Sinhalese, and Tamil at the top of News Feeds in April 2017 to educate people on our Community Standards, in particular hate speech. The content has been viewed almost 100M times by almost 4M people.

13. When I chaired the Senate Judiciary Subcommittee on Human Rights and the Law, I held a series of hearings on internet freedom. I invited Facebook to testify at our 2010 hearing. Unlike Google, Yahoo, and Microsoft, Facebook declined.

Beginning in 2009, I urged you and other technology companies to join the Global Network Initiative, a voluntary code of conduct that requires participating companies to take reasonable measures to protect human rights. Again, unlike Google, Yahoo, and Microsoft, you declined.

I reached out to you again in 2011 about serious concerns that repressive governments were using Facebook to monitor and suppress democracy activists.

I was glad when Facebook finally joined other major technology companies and became a member of the Global Network Initiative in 2013. But it's also clear that Facebook has lagged behind other technology leaders in this area and that you continue to face serious ongoing human rights challenges.

For example, human rights activists in Vietnam have expressed concerns that Facebook is working with the Vietnamese government to suppress dissent. A number of Vietnamese human rights activists and independent media groups sent a letter to you yesterday that noted "your company's aggressive practices… could silence human rights activists and citizen journalists in Vietnam."

The letter went on to say the following: "We appreciate Facebook's efforts in addressing safety and misinformation concerns online in Vietnam and around the world. Yet it would appear that after this high profile agreement to coordinate with a government that is known for suppressing expression online and jailing activists, the problem of account suspension and content takedown has only grown more acute."

a. Can you comment on Facebook's commitment to human rights?

b. What is your response to this letter?

c. How is Facebook addressing free expression and user privacy concerns in countries with repressive regimes?

Facebook is committed to respecting human rights. 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 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.

As a GNI member, Facebook is committed to privacy and free expression principles and implementation guidelines regarding government requests. The GNI standards have been shaped by international human rights laws and norms and developed through a robust multi-stakeholder and consultative process. The GNI principles and guidelines inform Facebook's approach to evaluating government requests for user data in all the markets where we operate.

Regarding the letter from Vietnamese human rights activists and citizen journalists specifically, we are committed to protecting the rights of people using Facebook in Vietnam, and to providing a place where people can express themselves freely and safely.

- Our Community Standards (https://www.facebook.com/communitystandards), which outline what is and isn't allowed on Facebook, seek to encourage expression and create a safe community on the platform. We will remove content that violates these standards when we're made aware of it.

- There are also times when we may have to remove or restrict access to content because it violates a law in a particular country, even though it doesn't violate our Community Standards. We have a well-established process for this, which is no different in Vietnam to the rest of the world. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague requests. We report the number of pieces of content we restrict for contravening local law in our Transparency Report.

- We did not take any action on the accounts of the signatories of the letter at the request of the Vietnamese government, nor did we see mass reporting on their accounts.

- We continue to work with partners in industry and civil society to voice concerns about efforts to restrict expression and limit the voice that people have online.

14. Open Secrets recently reported that multimillionaire donor Robert Mercer was behind a secretive dark money group called Secure America Now. According to Open Secrets, this organization "worked hand in hand with Facebook and Google to target their message at voters in swing states who were most likely to be receptive to them."

Specifically, Secure America Now created mock travel ads that invited visitors to the "Islamic State of France," the "Islamic State of Germany," and the "Islamic States of

America." Each ad began with an image of missiles shooting through the sky. The "French" ad included clips of blindfolded men with guns held to their head and children training with weapons. The "German" ad discussed "sell[ing] your daughter or sister to be married" with the image of a woman wearing a burka. The "American" ad had an image of Ground Zero in New York City as a place where citizens "celebrate Islamic victories."

The ads were clearly designed to stoke anti-Muslim sentiment in the days leading up to the 2016 election.

a. Under your new policies, how will ads like this be handled in the future?

b. Will Facebook continue to work with groups like Secure America Now to create targeted, bigoted content?

We did not work directly with Secure America Now; we worked through a third-party advertising agency. We did not create any content for Secure America Now. As is customary across managed advertising agencies, we provided a general best practices training to the agency staff, and we provided the measurement tools to determine the efficacy of the ads and differences between formats.

We require everyone on Facebook to comply with our Community Standards, which outline what is and isn't allowed on Facebook.

Explicit in our Community Standards is our prohibition on hate speech. We are opposed to hateful content in all its forms, and are committed to removing it from our platform any time we become aware of it. We're also committed to getting better at addressing these issues, including improving specific policies, our review process, and community reporting.

We have Community Standards that prohibit hate speech, bullying, intimidation and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect people from things like discriminatory ads—and we have recently tightened our ad policies even further to prohibit additional shocking and sensational content.

15. As you noted in your testimony, before the 2017 French election Facebook found and took down 30,000 fake accounts. Will you commit to inform Congress and the public on a real-time basis how many fake accounts Facebook takes down in the lead-up to the 2018 U.S. midterm elections?

We recently released enforcement statistics in our Community Standards Enforcement Report, including how many Facebook accounts we took action on because we determined they were fake. We will refine our approach over time, and we also hope to release additional metrics in future reports.

16. What percentage of current Facebook accounts do you understand or estimate to be fake?

We estimate that fake accounts represented approximately 3% to 4% of monthly active users (MAU) on Facebook during Q1 2018 and Q4 2017. We share this number in the Facebook quarterly financial results. This estimate may vary each quarter based on spikes or dips in automated fake account creation.

17. I assume there is an advertising revenue loss when Facebook deletes an account that is active but that is a fake or imposter account created to sow disinformation. But it is important for the public and Congress to know how many of these accounts there are and whether they are being removed.

a. Will Facebook be transparent with Congress and the public about how many active fake accounts Facebook is deleting?

b. How will Facebook enable Congress to track your progress in addressing and removing fake accounts?

We publish information and metrics about fake accounts at https://transparency.facebook.com/community-standards-enforcement#fake-accounts and in our SEC filings. We estimate that fake accounts represented approximately 3% to 4% of monthly active users (MAU) on Facebook during Q1 2018 and Q4 2017. We share this number in the Facebook quarterly financial results. This estimate may vary each quarter based on spikes or dips in automated fake account creation.

18. You say in your testimony that Facebook now has about 15,000 people working on security and content review. How many of those people are dedicated to identifying and removing fake accounts?

Estimating a number is difficult because stopping this type of abuse is a focus for many teams, some more directly and some in more of a supportive role. For example, we are expanding our threat intelligence team, and more broadly, we are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. Many of the people we are adding to these efforts will join our ad review team, and we also expect to add at least 3,000 people to Community Operations, which reviews content that our users and automated tools flag as inappropriate, dangerous, abusive, or otherwise violating our policies.

19. You stated during your testimony that Facebook has built A.I. tools for identifying terror and extremist-related content and that, for example, 99 percent of the ISIS and al-Qaeda content that Facebook takes down is flagged first via A.I.

a. How much content did Facebook take down that was linked to ISIS and al-Qaeda and what was the basis of your 99 percent statistic? Please quantify this in terms of accounts closed per year or some other quantifiable metric.

b. How much extremist content does Facebook take down that is not first identified by A.I.? Please quantify this in terms of accounts closed per year.

c. How much extremist content would you estimate is not removed by Facebook because it is not flagged by A.I. or by users?

d. We are facing a rising threat from white supremacist and other domestic extremist groups. An unclassified May 2017 FBI-DHS joint intelligence bulletin found that "white supremacist extremism poses [a] persistent threat of lethal violence," and that white supremacists "were responsible for 49 homicides in 26 attacks from 2000 to 2016 … more than any other domestic extremist movement." And *Politico* reported in August 2017 that "suspects accused of extreme right-wing violence have accounted for far more attacks in the U.S. than those linked to foreign Islamic groups like al Qaeda and ISIS, according to multiple independent studies." What specific steps is Facebook taking to address extremist content from white supremacists and other domestic terrorist threats?

While these metrics are in development, in Q1 2018, we took action on 1.9 million pieces of terrorist propaganda content related to ISIS, al-Qaeda, and their affiliates, up from 1.1 million in Q4 2017. This increase is due to improvements in our ability to find violating content using photo detection technology, which detects both old content and newly posted content.

While these metrics are in development, in Q1 2018, we found and flagged 99.5% of the terrorist propaganda content related to ISIS, al-Qaeda, and their affiliates we subsequently took action on, before users reported it. We acted on the other 0.5% because users reported it to us first. The amount of content we flagged increased from around 97% in Q4 2017 because we improved our photo detection technology and processes to find and flag more content before users reported it.

Terrorists, terrorist content, and hate speech in all forms—including white supremacy and domestic terrorist content—have no place on Facebook. We prohibit content that incites violence, and we remove terrorists and posts that support terrorism whenever we become aware of them. We are using a variety of tools in this fight.

Our policies against terrorist organizations and hate organizations fall within the broader category of dangerous organizations and individuals. We do not want Facebook to be a platform for hatred or violence, so our policies apply to all groups that have engaged in premeditated acts of violence or attacks on the basis of race, religious affiliation, nationality, ethnicity, gender, sex, sexual orientation, and serious disease or disability.

We define terrorism as "Any non-governmental organization that engages in premeditated acts of violence against persons or property to intimidate a civilian population, government, or international organization in order to achieve a political, religious, or ideological aim." Our definition is agnostic to the ideology or political goals of a group, which means it includes everything from religious extremists and violent separatists to white supremacists and militant environmental groups. It's about whether they use violence to pursue those goals.

We are equally committed to identifying and rooting out domestic hate organizations. We define hate organizations as "Any association of three or more people that is organized under a name, sign, or symbol and that has an ideology, statements, or physical actions that attack

individuals based on characteristics, including race, religious affiliation, nationality, ethnicity, gender, sex, sexual orientation, and serious disease or disability." In evaluating groups and individuals for designation as hateful, we have an extensive process that takes into account a number of different signals, and regularly engage with academics and organizations to refine this process.

20. If Facebook's users have their personal information misused without their knowledge and consent and then seek redress in the court system, it is possible that the companies that misused their information will try to force Facebook's users into mandatory arbitration proceedings. These arbitration proceedings are typically kept secret and rules are titled in favor of the repeat corporate player and against the victims.

a. Do you think it is fair for Facebook users to be forced into mandatory arbitration when they are trying to seek redress for companies' misuse of their personal information?

b. Does Facebook prohibit apps that use the Facebook platform from using mandatory arbitration clauses on Facebook users? If not, will you commit to doing so going forward?

Our Terms of Service, available at https://www.facebook.com/terms.php, addresses dispute resolution for users and our Platform Policy, available at https://developers.facebook.com/policy, lists the requirements for developers. Facebook's Terms do not contain an arbitration clause and, in fact, we recently updated our Terms to make it easier for users outside of the United States to access court systems in their home countries.

21. In December, the Federal Communications Commission (FCC) voted to dismantle net neutrality rules, paving the way for internet providers to block, throttle, or manipulate consumer access to the Internet. This action threatens the right of every consumer to access a free and open internet.

In the past, Facebook has expressed support for net neutrality protections.

a. As one of the most visited websites in the world, how important is net neutrality to Facebook's mission?

b. If left unchanged, what impact will the FCC's decision to undo net neutrality protections have on Facebook's millions of users?

Keeping the internet open for everyone is crucial. Not only does it promote innovation, but it lets people access information that can change their lives and gives voice to those who might not otherwise be heard. For these reasons, Facebook supports net neutrality and is open to working members of Congress and anyone else on a solution that will preserve strong net neutrality protections.

Questions from Senator Feinstein

Scraping of Public Profiles

1. **Nearly 2.2 billion people who use Facebook[1] have likely had their public profiles scraped by malicious actors, including by use of a search feature that allowed people to use telephone numbers and email addresses to obtain user information and through the company's account recovery feature.**

    a. **Why didn't Facebook take any action when it learned in 2013[2] that malicious actors could use its features to obtain personal information from users' profile pages?**

    b. **Facebook has now disabled the search feature, but are there plans to replace it? If so, what has Facebook done to ensure that personal information cannot be obtained using this new search feature?**

    c. **What changes is Facebook making to the account recovery feature to reduce the risk that personal information will be accessible to malicious actors?**

    d. **What steps is Facebook taking to protect its 2.2 billion users whose information may have been scraped by malicious actors?**

    e. **What information is being provided to users?**

In April, we found out that a feature that lets users look someone up by their phone number and email may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously.

Third Parties

2. **In 2014, Facebook updated its policies to reduce third party applications' access to user data. Facebook is now investigating applications that, as you described had access to "a large amount of information," before this change.**

    a. **How is Facebook defining "a large amount of information?"**

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API v.1.0 before we made technical changes to our platform to change this access.

[1] Throughout these Questions, references to Facebook refer to Facebook as well as all other Facebook-owned platforms, products, applications, and subsidiaries. For example, this includes Instagram and WhatsApp.
[2] *See, e.g.*, Matt Burgess, "Facebook fixed a massive data scraping issue it said wasn't a problem," Wired UK (Apr. 5, 2018).

b. How is Facebook determining what applications to include in this investigation?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, we are undertaking a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

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 suspensions include apps that 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.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

c. When do you estimate this investigation will be complete?

It's going to take many months to do this full process.

d. Will Facebook make public the results of this investigation? If not, why not and will you notify Congress and provide the results when you are done?

Where we find evidence that these or other apps did misuse data, we will ban them from the platform and tell people who used or may have had data shared with the app.

e. How will Facebook notify people whose data was improperly used?

See Response to Question (d).

f. What is Facebook doing to monitor and investigate whether developers or others are taking and selling personal information?

In general, on an ongoing basis, we proactively review all apps seeking access to more than basic information (and have rejected more than half of apps seeking such extended permissions). We also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for people. These include steps such as random checks of

existing apps along with the regular and proactive monitoring of apps. We also respond to external or internal reports and investigate for potential app violations. 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.

3. Individuals who use Facebook assume a certain level of privacy. There may be an understanding that if something posted is "public" that it's available broadly. However, the amount of data and personal information available through your platforms is enormous.

a. What data about individuals, if any, does Facebook make available to businesses?

Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

Our Data Policy makes clear the circumstances in which we work with third parties who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

When people choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what users post or share. For example, when users play a game with their Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about the users' activities in the game or receive a comment or link that users share from the website on Facebook. Also, when users download or use such third-party services, they can access users' public profile on Facebook, and any information that users share with them. Apps and websites that people use may receive their list of Facebook friends if they choose to share it with them. But apps and websites that people use will not be able to receive any other information about their Facebook friends from users, or information about any of the users' Instagram followers (although friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies.

Devices and operating systems providing native versions of Facebook and Instagram (i.e. where we have not developed our own first-party apps) will have access to all information people choose to share with them, including information that friends share with users, so they can provide our core functionality to our users.

b. Can businesses access users' emails, direct messages, buying history, or credit card information?

See Response to Question 3, part a.

c. Your privacy policies indicate Facebook collects the content of messages through your direct messenger applications and through private group postings. How is that information used? Is it shared with anyone?

We use the information we collect for purposes specified in our Data Policy. These purposes include:

- Providing, personalizing and improving our products;
- Providing measurement, analytics and other business services;
- Promoting safety, integrity and security;
- Communicating with our community;
- Conducting research and innovating for social good.

d. Does Facebook have the capacity to monitor how researchers or businesses use data they get from Facebook?

We have a variety of controls in place to help ensure researchers and businesses comply with our policies.

e. What does Facebook do, if anything, to ensure researchers and others comply with its use agreements?

If we discover a researcher or business has misused people's information, we take appropriate action to address the issue. Such action may include suspending the business from Facebook or even banning it altogether.

f. What limitations has Facebook placed on the personal information that application developers can request from Facebook users? How is this enforced?

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. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs.

We are further restricting the data that an app can access without review to a person's name, profile photo, and email address. We review 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.

g. What limits has Facebook placed on how personal information can be used by third parties? Has Facebook prohibited uses beyond what is necessary to run third party applications?

Developers can access Account Information in accordance with their privacy policies and other Facebook policies. All other data may not be transferred outside the Facebook app, except to service providers, who need that information to provide services to the Facebook app. With the exception of Account Information, developers may only maintain user data obtained from Facebook for as long as necessary for their business purpose. Developers may not use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan. Developers must protect the information they receive from Facebook against unauthorized access, use, or disclosure. For example, developers may not use data obtained from Facebook to provide tools that are used for surveillance.

Cambridge Analytica

4. Facebook learned in 2015 that Cambridge Analytica had obtained Facebook user information without notice or consent.

a. Why didn't Facebook notify users of this breach in 2015?

b. What is Facebook's current policy for notifying users of privacy breaches?

c. Why didn't Facebook suspend or ban Cambridge Analytica from its platforms until 2018?

d. Why didn't Facebook audit Cambridge Analytica?

e. What led Facebook to consider the matter "closed" without taking any of these steps?

f. Have there been any reforms to Facebook's internal investigative policies based on this experience? (If so, please describe these changes.)

g. Why didn't Facebook notify the Federal Trade Commission of this incident before press stories broke in March 2018?

h. What will Facebook do to protect the 87 million people whose personal information remains in the hands of third parties?[3]

When Facebook learned in December 2015 of allegations that Kogan may have violated Facebook's policies, we took immediate action. Facebook immediately banned Kogan's app

[3] *See, e.g.*, Matthew Rosenberg et al., "How Trump Consultants Exploited the Facebook Data of Millions," N.Y. Times (Mar. 17, 2018) (the New York Times viewed raw data from the profiles Cambridge Analytica obtained; copies of the data remain on Cambridge Analytica servers); Channel 4, "Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted," (Mar. 28, 2018) (Channel 4 News saw data on thousands of people in Colorado).

from our developer platform and retained an outside firm to investigate what happened and what further action we should take to enforce our Platform Policies and protect people. This culminated in certifications from Kogan, and from Cambridge Analytica and others whom he certified he had shared some data with, certifying that they had deleted all data and any derivatives of the data. Because Kogan's app could no longer obtain access to most user data (or any friends data) in December 2015 due to changes in Facebook's platform, the most responsible step to protect users at the time was to work with Kogan, Cambridge Analytica, and others to obtain deletion of the data.

Although our developer terms gave us the ability to audit Kogan's app, we did not have an agreement in place that would have allowed us to audit third parties that he may have shared data with. For this reason, we chose to require him to obtain certifications of deletion from each of these parties, leveraging our rights as to Kogan, who was the developer of the app.

In March 2018, Facebook received information from the media that possible questions existed around the validity of deletion certifications that Facebook received. In response, Facebook immediately banned Cambridge Analytica and other potentially related parties from distributing advertising on Facebook or from using other aspects of our service. At that time, we requested an on-site audit of Cambridge Analytica, which it agreed to. The forensic auditor's work is currently on hold at the request of UK regulatory authorities, who themselves are investigating Cambridge Analytica, which is located in the UK, and we are actively cooperating with the UK authorities to progress this analysis.

It is important to clarify that Kogan's improper disclosure of Facebook data that users shared with him does not involve a data breach on Facebook's platform. There was no unauthorized access to Facebook data by Kogan, and instead, his app could only access Facebook data that users specifically consented to share with him. Even though Kogan's improper disclosure of data was not a breach of our systems, these actions violate our Platform policy—and we took extensive measures to try to mitigate any potential misuse of that data by downstream parties by pushing aggressively for deletion. And we are implementing an approach that goes beyond legal requirements and informs people any time we learn than an app developer shared data with a third-party in violation of our policies. This is consistent with the responsibility we believe we have with our users, even if the law does not require this.

5. Cambridge Analytica whistleblower Christopher Wylie told the U.K.'s House of Commons that senior employees at another data analytics firm were also working on the Facebook data obtained through Aleksandr Kogan's application.

a. Did anyone besides Prof. Kogan and Cambridge Analytica have access to the data obtained by Prof. Kogan?

b. Does any company have that data today?

c. What steps are you taking to find out who had access to the data and how it was used?

d. Is this data still being used? How can its ongoing use be prevented?

On December 11, 2015, The Guardian published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. If this occurred, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed and provided to Facebook signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017, Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

6. Cambridge Analytica's managing director was recorded explaining that the company pushes propaganda "into the bloodstream of the internet, and then watch[es] it grow, give[s] it a little push every now and again… like a remote control."[4]

a. Has Facebook investigated what material Cambridge Analytica put on Facebook's platforms, how the material spread, and how Cambridge Analytica targeted people?

b. If yes, please provide your findings to the Committee.

c. If not, will Facebook conduct this investigation or allow researchers to do this, and to provide the findings to the Committee?

Our investigation of Cambridge Analytica's advertising activities is ongoing, and we have banned Cambridge Analytica from purchasing ads on our platform. Cambridge Analytica generally utilized custom audiences, some of which were created from contact lists and other identifiers that it generated and uploaded to our system to identify the people it wanted to deliver ads to on Facebook, and in some instances, refined those audiences with additional targeting attributes.

7. Cambridge Analytica and the Kremlin-backed Internet Research Agency both improperly targeted Facebook users to influence the 2016 election.

a. Has Facebook compared Cambridge Analytica's targeting of Facebook users in the United States during the 2016 presidential election cycle to targeting by the Internet Research Agency?

b. If yes, please describe how Cambridge Analytica's targeting was both similar to and different from the Internet Research Agency's targeting.

c. If not, will Facebook do this, and provide its findings to the Committee?

The targeting for the IRA ads that we have identified and provided to the Senate Committee on the Judiciary and the Senate Select Committee on Intelligence was relatively rudimentary, targeting very broad locations and interests, and for example, only used custom audiences in a very small percentage of its overall targeting and did not use Contact List Custom Audiences. In addition, all of the custom audiences used by the IRA were created based on user engagement with certain IRA pages. By contrast, Cambridge Analytica used hundreds of Contact List Custom Audiences during the 2016 election cycle created from contact lists that Cambridge Analytica uploaded to our system, and Cambridge Analytica used those and other custom audiences in the majority of its ads targeting in combination with demographic targeting tools.

Foreign Actors

[4] Sonam Sheth, "Cambridge Analytica began testing out pro-Trump slogans the same year Russia launched its influence operation targeting the 2016 election," Business Insider (Mar. 20, 2018).

8. A new study found that more than half of the sponsors of Facebook ads that featured divisive political messages during the 2016 election were from "suspicious" groups, and that one in six suspicious advertisers was linked to the Internet Research Agency.[5]

a. Will you work with these researchers to determine whether any of the "suspicious groups" they identified, other than those associated with the Internet Research Agency, are also linked to Russia or other foreign government actors?

b. If so, please also provide the findings to this Committee.

c. If not, will you perform your own analysis of who bought divisive issue ads leading up to the 2016 election, including how many were attributable to the Internet Research Agency or other Russian-backed accounts, and provide your findings to the Committee?

Facebook has conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by using Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite efforts by these accounts to mask the provenance of their activity. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again. That's why we have provided all of the ads and associated information to the committees with longstanding, bipartisan investigations into Russian interference, and we defer to the committees to share as appropriate. We believe that Congress and law enforcement are best positioned to assess the nature and intent of these activities.

9. What is Facebook doing to limit foreign actors' ability to obtain and use personal information about American users?

Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we have dedicated information security and related engineering teams.

Protecting the security of information on Facebook is at the core of how we operate. Security is built into every Facebook product, and we have dedicated teams focused on each aspect of data security. From encryption protocols for data privacy to machine learning for threat detection, Facebook's network is protected by a combination of advanced automated systems and teams with expertise across a wide range of security fields. Our security protections are regularly evaluated and tested by our own internal security experts and independent third parties. For the past seven years, we have also run an open bug bounty program that encourages

[5] Young Mie Kim et al., "The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook," Politcal Communication (forthcoming), *available a*t https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Kim.FB_.StealthMedia.Final_.PolCom.0411181.pdf.

researchers from around the world to find and responsibly submit security issues to us so that we can fix them quickly and better protect the people who use our service.

We anticipate continuing to grow these teams by hiring a range of experts, including people with specific types of threat intelligence expertise.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. 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 can already see all the ads that a Page is running on Facebook—and we're launching this globally in June.

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 are working hard to stop the spread of false news. We work with third party fact checking organizations to limit the spread of articles with rated false. 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. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page

Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

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.

10. Russian accounts continue to use social media to try to influence American opinion. For example, Fox News started a social media campaign to demand the declassification and release of the Nunes memo, which attacked the FBI's Russia investigation. Within hours, Russian bots were promoting the release of the memo.

a. When this began did Facebook investigate whether Russians were using its platforms to promote the "Release the Memo" campaign?

b. Has Facebook analyzed whether any of the accounts that users shared WikiLeaks' offer of $1 million for a copy of the Nunes memo (before it was declassified and released) had connections to Russian-backed accounts?

As of our February 7, 2018 letter to you on this issue, our internal Information Security team has not become aware of information or activity of a sort that would prompt further review. In addition to reaching out to law enforcement and our industry partners to understand whether they have any relevant information regarding this issue and Russian influence more generally, our Information Security team regularly conducts internal reviews to monitor for state-sponsored threats. While we do not publicly disclose the elements of these reviews for security reasons, factors include monitoring and assessing thousands of detailed account attributes, such as location information and connections to others on our platform. We are committed to keeping law enforcement apprised of our efforts and to working together to address this threat.

11. How many communications has Facebook had with individuals associated with any accounts that Facebook has identified as Internet Research Agency accounts?

Last fall, we concluded that sharing the ads we've discovered with Congress, in a manner that is consistent with our obligations to protect user information, will help government authorities complete the vitally important work of assessing what happened in the 2016 election. That is an assessment that can be made only by investigators with access to classified intelligence and information from all relevant companies and industries—and we want to do our part. Congress is best placed to use the information we and others provide to inform the public comprehensively and completely. Our practice is to provide messages in response to valid legal process. The ads (along with the targeting information) are publicly available at https://democrats-intelligence.house.gov/facebook-ads/social-media-advertisements.htm.

12. On October 27, 2017, I asked you to provide to the Committee all communications between Facebook and individuals or entities associated with Russia-connected users that posted ads or organic content targeted to any part of the United States for the time period from January 2, 2015 to the date of production. You have not yet provided a substantive response to this request. Please provide these communications.

See Response to Question 11.

13. Please provide all organic Instagram posts for Internet Research Agency accounts that targeted users in the United States.

Facebook provided all of these posts to the Senate Judiciary Committee last fall on October 30 and 31.

Global Privacy Protections

14. You have said that Facebook would apply the European Union's new privacy requirements globally in spirit.

a. Will the privacy requirements be incorporated into the terms of service that apply to users in the United States? If not, why not? If so, when will this change be made?

b. It was recently reported that Facebook users outside of the United States and Canada had previously been governed by terms of service agreed with Facebook in Ireland.[6] Facebook is apparently changing this so that non-European Union users will have their terms of service agreed with Facebook in the United States. This affects 1.5 billion users. Does this mean that the European Union's new privacy requirements will not apply to these 1.5 billion users? If Facebook intends to provide the same privacy protections and controls to users globally, why did it make this change?

The change referred to in this question involves the legal entity with which Facebook users contract when they use the service, which changed in some jurisdictions as a part of the most recent updates to our Terms of Service and Data Policy. This change did not impact people who live in the United States, who contract with Facebook, Inc. under both our new and old policies.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer (DPO) or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU.

In any case, the controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability, and others to people in the US and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

[6] Alex Hern, "Facebook moves 1.5bn users out of reach of new European privacy law," The Guardian (Apr. 19, 2018).

Questions from Senator Grassley

1. **Please provide a comprehensive list of all forms of content or data Facebook collects on Facebook users from the Facebook platform, whether it is content or data created by the user or not.**

   As explained in our Data Policy, we collect three basic categories of data about people:

   (1) data about things people do and share (and who they connect with) on our services,

   (2) data about the devices people use to access our services, and

   (3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—i.e., their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

We recently announced improvements to our Download Your Information tool, as well as a new feature that makes it easier for people to see the information that's in their account on Facebook. These recently-expanded tools for accessing information will allow people to see their data, delete it, and easily download and export it.

2. **Please provide a comprehensive list of all ways Facebook uses each form of content or data. Please provide as much detail as possible. For example, does Facebook ever use location information to tell a business that a consumer physically went to a store after seeing an ad?**

   See Response to Question 1.

3. **Does Facebook collect or purchase information about non-Facebook users? If so, what information is collected? How does Facebook acquire the information? What**

are all the ways Facebook uses the information? Please provide a comprehensive list of all forms of data Facebook collects on individuals, not collected from the Facebook website.

a. Can a person who does not have a Facebook account request deletion of any data? How?

b. If Facebook has utilized the information of a person who does not have an account in any way, such as building advertising profile, will deletion of the data ensure deletion from advertising profiles or any other products that the data was used to compile?

Facebook does not create profiles or track website visits for people without a Facebook account.

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 Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. 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.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

4. **When a user deletes information from Facebook, is that information still used to inform advertising?**

    a. **If it is, how does the user change this?**

    b. **When a user deletes their Facebook account, is underlying data still used in any way, including to inform advertising profile? Can the user prevent any further use?**

The audience with which someone chooses to share their information is independent of whether we use that information to personalize the ads and other content we show them. Specifically, our Data Policy explains that we may use any information that people share on Facebook "to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads)." However, people can use our Ad Preferences tool to see the list of interests that we use to personalize their advertising. This means that, for example, a person who is interested in cars can continue to share that interest with their friends but tell us not to assign them an interest in ads for ad targeting purposes.

Likewise, the audience of a post does not determine whether a post is retained. Someone can choose to share a post with "Only Me" (meaning that they don't want anyone to see it but want to retain it in their Facebook account). They may also choose to delete the information entirely. When people choose to delete something they have shared on Facebook, we remove it from the site. In most cases, this information is permanently deleted from our servers; however, some things can only be deleted when a user permanently deletes their account.

5. **How long does Facebook keep a user's data after they delete their account? Is there any data that is not deleted from Facebook's servers?**

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

6. **In your testimony you stated that the user has complete control over their Facebook page.**

    a. **Can a user make their profile invisible, so it cannot be found by searching Facebook or the web?**

b. Can a user choose to make their name or picture private?

c. Can a user opt out of specific uses of their data, such as academic research?

When someone creates a profile on Facebook, the purpose of the profile is to enable others on Facebook to see whatever information the person chooses to add to his or her profile. However, people are in control of what information they add—only a person's name and limited other data is required to create a Facebook profile. And, for nearly all information that people choose to add to their profiles, they can choose who is eligible to see this information. For example, a person might choose to share his or her hometown only with his or her friends.

A limited amount of information that people provide—including their name and, if they choose to add one, their profile photo—is always public on Facebook. Among other things, this helps us inform a user before they make or accept a friend request of the identity of the person with whom he or she is about to connect.

Through Facebook's Settings, people can make a range of choices about how their information will be used, including instructing that they do not want search engines to link to their profiles. We inform people that, even if they choose not to be linked to in search engines, anyone may see information that they share if they set the audience for that information to Public.

7. With regard to academic research, you recently updated your data policy as it was reported that Facebook was looking into partnering with healthcare providers to conduct medical research.

a. Why was it not disclosed earlier to users that their data could be used for research?

b. How does a user opt out of being a subject of medical or other academic research?

c. If they cannot, why not? Will you change this?

Facebook was exploring this type of data sharing because of the general health benefits to having a close-knit circle of family and friends and the need for more research on the impact of social connection on health. Deeper research into this link is needed to help medical professionals develop specific treatment and intervention plans that take social connection into account. With this in mind, last year Facebook began discussions with leading medical institutions, including the American College of Cardiology and the Stanford University School of Medicine, to explore whether scientific research using fully-anonymized Facebook data could help the medical community advance our understanding in this area. This work did not progress past the planning phase, and we have not received, shared, or analyzed anyone's data.

In March we decided that we should pause these discussions so we can focus on other important work, including doing a better job of protecting people's data and being clearer with them about how that data is used in our products and services.

Our Data Policy has explained that we have engaged in research collaborations for several years. As part of a general effort to be more transparent, we updated our Data Policy recently to provide additional detail on a range of practices, including academic research. We also explain this in other ways, including announcements in our Newsroom and in a dedicated website providing more information about research at Facebook.

8. **Does Facebook currently collect, or have any plans to collect, anonymized medical information of Americans?**

    a. **If so, what are the planned or potential uses of this information?**

    See Response to Question 7.

9. **In your testimony you stated that it would be too long a webpage if you provide a list of all the ways data is used. Is there a reason you could not have a short, easy to understand list, and a long comprehensive list for those who are interested to learn more?**

We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that 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 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.

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.

10. It has been reported that Facebook's download your information tool, contrary to your testimony, does not contain all the data Facebook has collected on that individual consumer. Can you explain that discrepancy? Will you be changing this?

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 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 announced expansions to Download Your Information, which, among other things, will make it easier for 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, delete 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.

11. Facebook has previously stated that private messages are not scanned for advertising, but are scanned for content such as child pornography and facilitating genocide. Is there any other way in which private messages are used by Facebook or any third party?

The way Facebook uses messages can be found in our Data Policy, located at: https://www.facebook.com/policy.php.

12. When a user logs in to Facebook, does Facebook continue to track, through cookies or other trading tools, the users pages visited (a) while the user is still logged onto the Facebook page, and (b) after the user logs out of the Facebook page?

See Response to Question 3.

13. Please provide a detailed explanation how Facebook tracks a user's internet browsing activity. Where is this disclosed on the Facebook website and could it be disclosed more fully?

We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users. Our goal is to show people content (including advertising) that is relevant to their interests. We use information people have provided on Facebook—such as things they've liked or posts they've engaged with—to help determine what people will be interested in. Like most online advertising companies, we also inform our judgments about what ads to show based on apps and websites that people use off of Facebook. People can completely turn off our use of web browser data and other data from third-party partners to show them ads through a control in Ads Preferences. They can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see. In addition, a person's browser or device may offer settings that allow users to choose whether browser cookies are set and to delete them

14. Can people opt-out of being tracked across the Web by Facebook via cookies and other tracking tools? How?

See Responses to Questions 10 and 13.

15. Has Facebook been collecting call history and SMS data from Android phones? If yes, how has it been collected and what is Facebook doing with this information?

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 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 services 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 anyone's call and text history, 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.

16. Does Facebook scan users' photos to generate biometric data on them? Does Facebook scan photos for any reason other than to match photos based on facial recognition and to search for inappropriate content?

Facebook uses facial recognition technology to provide people with products and features that enhance online experiences for Facebook users while giving them control over this technology. Facebook's facial recognition technology helps people tag their friends in photos; gives people an easier and faster way to privately share their photos with friends; helps people with visual impairments by generating descriptions of photos that people using screen readers can hear as they browse Facebook; lets people know when a photo or video of them has been uploaded to Facebook, even if they are not tagged; and helps prevent people from impersonating other Facebook users.

Facial recognition technology uses machine-learning algorithms to analyze the pixels in photos and videos in which a user is tagged, and the photo used by the person as his or her profile picture, and generates a unique number called a template. When a photo or video is uploaded to Facebook, Facebook uses the template to attempt to identify someone by determining whether there are any faces in that content, and analyzing the portion of the image in which the face appears to compare it against certain Facebook users depending on the purpose for which facial recognition is being performed.

Facebook has not shared and does not have plans to share or make available to any third party its facial recognition templates. Moreover, these templates do not provide meaningful information on their own; they can be used to identify a person only in conjunction with Facebook's software. They could not be reverse-engineered to recreate someone's face.

Facebook designed its facial-recognition technology and the applications that use it with privacy considerations in mind and incorporated various safeguards and controls that protect both (1) users' ability to control the collection, use, and disclosure of their personal information, and (2) the security of that personal information.

Facebook gives users control over whether Facebook uses facial recognition to recognize them in photos and videos. That control is exercised through users' privacy settings. If a user chooses to turn facial recognition off, Facebook does not create a template for that person or deletes any template it has previously created. Facebook will then be unable to recognize that person in any photos or videos that are uploaded to the service. Facebook also deletes templates of people who delete their Facebook accounts. Additionally, Facebook does not maintain templates for users who have no photos tagged of themselves and do not have a profile photo that is capable of being used to generate a face signature or template (e.g., where a user has no profile photo, where a user's profile photo does not contain a human face, or where a user's profile photo contains multiple untagged faces).

We inform people about our use of facial recognition technology through the Data Policy, Help Center, posts on Facebook, and direct user notifications. Facebook users are told that they can opt out of facial recognition at any time—in which case Facebook will delete their template and will no longer use facial recognition to identify them.

In creating facial recognition templates, Facebook uses only data that people have voluntarily provided to Facebook: the photos and videos that people have voluntarily uploaded to Facebook (including public profile pictures) and the tags people have applied to those photos and videos. Facebook does not use facial recognition to identify someone to a stranger.

17. Does Facebook collect user data through cross-device tracking? What types of data are collected? If a user accesses their Facebook account through a mobile device, for example, what information does Facebook collect about that mobile device? And what access, if any, does Facebook have to other data located on that user's mobile device? What are all the ways in which Facebook uses this data?

Facebook's services inherently operate on a cross-device basis: understanding when people use our services across multiple devices helps us provide the same personalized experience wherever people use Facebook—for example, to ensure that a person's News Feed or profile contains the same content whether they access our services on their mobile phone or in a desktop computer's web browser.

In support of those and other purposes, we collect information from and about the computers, phones, connected TVs and other web-connected devices our users use that integrate with our Products, and we combine this information across a user's different devices. For example, we use information collected about a person's use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone or on a different device.

Information we obtain from these devices includes:

- **Device attributes.** Information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.

- **Device operations.** Information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).

- **Identifiers.** Unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).

- **Device signals.** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.

- **Data from device settings.** Information a user allows us to receive through device settings they turn on, such as access to their GPS location, camera, or photos.

- **Network and connections.** Information such as the name of a user's mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help them stream a video from their phone to their TV.

- **Cookie data.** Data from cookies stored on a user's device, including cookie IDs and settings. More information is available at

https://www.facebook.com/policies/cookies/ and https://help.instagram.com/1896641480634370?ref=ig.

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about a person's activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a person plays, or a business could tell us about a purchase a person made in its store. We also receive information about a person's online and offline actions and purchases from third-party data providers who have the rights to provide us with that person's information.

We use the information we have to deliver our Products, including to personalize features and content (including a person's News Feed, Instagram Feed, Instagram Stories, and ads) and make suggestions for a user (such as groups or events they may be interested in or topics they may want to follow) on and off our Products. To create personalized Products that are unique and relevant to them, we use their connections, preferences, interests, and activities based on the data we collect and learn from them and others (including any data with special protections they choose to provide); how they use and interact with our Products; and the people, places, or things they're connected to and interested in on and off our Products.

For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant. We use location-related information—such as a person's current location, where they live, the places they like to go, and the businesses and people they're near—to provide, personalize and improve our Products, including ads, for them and others. Location-related information can be based on things like precise device location (if a user has allowed us to collect it), IP addresses, and information from their and others' use of Facebook Products (such as check-ins or events they attend). We store data until it is no longer necessary to provide our services and Facebook Products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies someone (information such as a person's name or email address that by itself can be used to contact them or identifies who they are) unless they give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led people to make a purchase or take an action with an advertiser.

18. There remains concern about timely fixes of security gaps in Facebook. In your written testimony you stated that a feature that allowed user look-up by phone number or email had been abused to scrape profiles and that the feature had

recently been shut down. However there are public reports that Facebook was made aware of the vulnerability as early as 2013.

a. Are these reports accurate?

b. If so, why was the feature not fixed earlier?

c. What steps is Facebook taking to ensure that any abuses of privacy are dealt with more expeditiously?

In April, we found out that a feature that lets users look someone up by their phone number and email may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously.

19. Does Facebook have a specific review protocol for a reported data breach or improper data transfer?

Yes, Facebook maintains a data incident response plan.

a. If not, why not? Will you be establishing one?

See response above.

b. If so, what is the protocol? Is there a timeline by which a review should be completed and the vulnerability addressed?

Facebook monitors its systems for potential breaches of personal data and logs any potential breach in a system that automatically triggers expedited review. Facebook reviews such potential incidents to determine: (i) whether there was in fact an incident, (ii) its root cause, including short- and long-term remediation (if applicable); and (iii) our legal and ethical obligations. Facebook moves quickly to review potential incidents. Because of the fluid nature of an incident, there are no set timelines for completion of reviews and addressing of a discovered vulnerability, but any potential breach is escalated for high priority processing.

c. What are the standards for when and how Facebook will notify users that their information may have been breached or improperly transferred?

Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at https://www.facebook.com/help/218345114850283?helpref=about_content.

The categories of information that an app can access is clearly disclosed before the user consents to use an app on the Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

In addition, Facebook notifies users in accordance with its obligations under applicable law and has also notified people in cases where there was no legal obligation to do so but we nevertheless determined it was the right thing to do under the circumstances.

20. Many of Facebook's vulnerabilities in security or privacy appear to be reported to Facebook and then addressed. Does Facebook have a specific proactive team or protocol for finding security leaks and privacy issues? In short, are there dedicated resources to seek out privacy issues on the platform? If not, why not? If so, when was the proactive approach implemented?

Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we have dedicated information security and related engineering teams.

Protecting the security of information on Facebook is at the core of how we operate. Security is built into every Facebook product, and we have dedicated teams focused on each aspect of data security. From encryption protocols for data privacy to machine learning for threat detection, Facebook's network is protected by a combination of advanced automated systems and teams with expertise across a wide range of security fields. Our security protections are regularly evaluated and tested by our own internal security experts and independent third parties. For the past seven years, we have also run an open bug bounty program that encourages researchers from around the world to find and responsibly submit security issues to us so that we can fix them quickly and better protect the people who use our service.

We anticipate continuing to grow these teams by hiring a range of experts, including people with specific types of threat intelligence expertise.

21. How many improper data transfers to third parties have there been?

a. Was Facebook only made aware of the improper data transfers by a third party?

b. Have you ever required an audit to ensure the deletion of improperly transferred data? If so, how many times?

c. Please provide a list of applications that Facebook has previously banned because data was transferred in violation of Facebook's terms.

d. Beyond an audit, what tools is Facebook using to proactively stop improper transfers of data?

e. How are you proactively ensuring that data is not improperly transferred by third parties in the future?

We launched an initial investigation after the December 11, 2015 publication of an article in *The Guardian* about Cambridge Analytica's potential misuse of Facebook data.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

22. In page 3 of your written testimony you state that "strict requirements" are going to be put on developers. What are those strict requirements?

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

- **Review our platform.** We are investigating 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.

- **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 in more detail how we use data and how data is shared with app developers.

23. Please list all the companies or persons to whom Aleksandr Kogan sold Facebook data.

Kogan represented that, in addition to providing data to his Prosociality and Well-Being Laboratory at the University of Cambridge for the purposes of research, GSR provided some Facebook data to SCL Elections Ltd., Eunoia Technologies, and the Toronto Laboratory for Social Neuroscience at the University of Toronto. However, the only party Kogan has claimed paid GSR was SCL. Our investigation is ongoing.

24. Please provide a detailed account of why Facebook did not detect that Mr. Kogan's user agreement included an agreement for resale, in violation of Facebook's polices?

Facebook has developed an automated system for checking that all apps had terms of service and data policies. In performing such checks, however, Facebook does not examine the content of the developers' terms and policies because app developers act as independent third parties with regard to the data they obtain; they determine the purposes for which, and the manner in which, that data is processed. Our understanding is that this is consistent with the practices of other major online and mobile platforms, which generally enable developers on their platforms to provide access to the developers' terms and policies in their app stores, but do not proactively review the substance of those policies.

Although developers act as independent third parties with regard to the data users share with them, all apps on the Facebook Platform must comply with our user data policies, Community Standards, Platform Policies, and Ad Guidelines. Our Platform policy also contains a number of enforcement provisions which apply after an app has been reviewed and approved. Facebook has several teams dedicated to detecting, escalating, investigating, and combating violations of its policies, including schemes to improperly access, collect, or exploit user data. The Developer Operations Policy Enforcement team looks for policy violations and either brings developers into compliance or removes them from the platform, and the Developer Operations Review team conducts an upfront review of apps to confirm proper use of advanced permissions.

25. What information exactly was received by Aleksandr Kogan? Private messages? Friends of friends' info?

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.

26. Does Facebook have any evidence or reason to believe Cambridge Analytica, GSR, or Kogan, retained Facebook data after they certified they had deleted it?

In March 2018, we learned from news reports that contrary to the certifications given, not all of the Kogan data may have been deleted by Cambridge Analytica. We have no direct evidence of this and no way to confirm this directly without accessing Cambridge Analytica's systems and conducting a forensic audit. We have held off on audits of Cambridge Analytica and other parties that are being investigated by the UK Information Commissioner's Office at its request. Our investigation is ongoing.

27. Are you currently engaged in any industry-wide conversations about setting best practices for disclosures of data collection and use, privacy policy settings, and/or proactively discovering privacy lapses? If not, why not? If so, will a public report be generated? If so, when?

We regularly consult with a range of experts in our effort to deliver and improve the strong privacy protections that people who use Facebook expect. This includes regular consultation with privacy experts, academics, other companies, and industry groups. While we recognize that there is no one-size-fits-all approach to strong privacy protections, we believe that these ongoing discussions better enable us to design our services in a way that responds to the feedback we're receiving, as well as new research and best practices around privacy.

28. Please provide a detailed breakdown of the principles that will guide the development of artificial intelligence (AI) practices, the details about what those practices are, and how they'll help users.

We are focused on both the technical and the ethical aspects of artificial intelligence. We believe these should go hand-in-hand together in order to fulfill our commitment to being fair, transparent, and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparenc,y and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

a. Many are skeptical AI will be a cure-all for content issues. Facebook has also announced it will hire more content reviewers. Does Facebook have any other plans to deal with content review?

We believe that over the long term, building AI tools is the scalable way to identify and root out most of this harmful content. We're investing a lot in building those tools. And we already use artificial intelligence to help us identify threats of real world harm from terrorists and others. For example, the use of AI and other automation to stop the spread of terrorist content is showing promise. Today, 99 percent of the ISIS and Al Qaeda related terror content we remove from Facebook is content we detect before anyone in our community has flagged it to us, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. We also use AI to help find child exploitation images, hate speech, discriminatory ads, and other prohibited content. Moreover, in the last year, we have basically doubled the number of people doing security and content review. We will have more than 20,000 people working on security and content review by the end of this year.

b. You have offered a "bounty" for information about improperly transferred user data. Are you concerned this bounty program may promote the hacking of third-party app developers? Could offering small bounties for finding hate speech, terrorism, etc. encourage more user reporting on the platform?

The Data Abuse Bounty Program is carefully designed to help us lawfully obtain data necessary to review apps that are operating from malicious intent of their developers. The program does not reward reports that were a direct or indirect result of hacking of third-party app developers. We made this explicitly clear in the terms of the program. Following an investigation, we will reward a submission only if the report is genuine, based on direct and personal knowledge, and the information was obtained lawfully. To prevent abuse, we require the submission to be submitted in narrative form without any data appended. We will request data only if we need it and we are absolutely confident that the reporter obtained it and can share it lawfully.

The Data Abuse Bounty will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence. We'll review all legitimate reports and respond as quickly as possible when we identify a credible threat to people's information. If we confirm data abuse, we will shut down the offending app and, if necessary, take legal action against the company selling or buying the data. We'll pay a bounty to the person who reported the issue, or allow them to donate their bounty to a charity, and we'll also alert those we believe to be affected. We also encourage our users to report to us content that they find concerning or that results in a bad experience, as well as other content that may violate our policies. We review these reports and take action on abuse, like removing content and disabling accounts.

29. Do you have a specific office that can respond to users' complaints and questions regarding privacy? If so, how is this office advertised? Could it be made more accessible to the public and or better equipped? If you have no such office, why not?

Yes. In addition to the range of online educational resources that we provide through our website and mobile apps, we have staff responsible for responding to questions from people about privacy. We distribute the contact information for this team in a number of ways, including in the section of our Data Policy that begins with the heading, "How to contact Facebook with questions."

30. What assistance do Facebook employees embedded with advertising and political clients provide?

Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. During the 2016 election cycle, for example, Facebook provided technical support and best practices guidance on optimizing their use of Facebook.

a. Is there any way these embedded persons could bypass a security or privacy feature?

b. Has Facebook investigated whether any Facebook personnel assisting the Obama campaign violated any Facebook policies?

c. What protocols are in place to make sure these embedded persons cannot take any steps to bypass privacy or security controls on Facebook?

Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. We continuously work to ensure that we comply with all applicable laws and policies.

31. You have received numerous questions about removing conservative content from Facebook. You have answered that these were enforcement errors.

a. Have you undertaken any study to determine whether any specific forms of content have been more or less likely to be removed? If not, why not? If so, what are the results? Have you found that conservative content is more likely to be removed?

b. What is the source of the enforcement errors? Are these individual people, AI algorithms, or something else?

c. How are you addressing the source of any errors? E.g., training for individuals, changes to the AI algorithm?

d. How do you notify persons whose content has been deleted of the deletion and the reasons for it?

e. Do you disconnect friends with deleted content?

f. Do you prevent information from reaching the feed of followers of persons who have previously had content deleted?

g. How quickly are complaints about improper censoring addressed?

h. How quickly are complaints about threats addressed?

Suppressing political content or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community.

We recently published a detailed set of Community Standards—which reflect our internal reviewer guidelines—to help people understand where we draw the line on complex and nuanced issues. Publishing these details will also make it easier for everyone to give us feedback so that we can improve the guidelines—and the decisions we make—over time. Our Community Standards, which are designed to encourage expression and create a safe environment on Facebook, outline what is and isn't allowed on the platform.

When someone violates our Community Standards, we send them a notification. We are also introducing the right to appeal our decisions on individual posts so people can ask for a second opinion when they think we've made a mistake.

32. How do you as a company deal with a person whose content was wrongly deleted? Do you simply restore the content? Do you offer an apology? Do you make any form of recompense, or otherwise make clear to the user their speech is welcome on the platform?

We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

When we're made aware of incorrect content removals, we review them with team members so as to prevent similar mistakes in the future. On April 24, 2018, we announced the launch of appeals for content that was removed for hate speech. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving where errors are being made.

We hope that our recent decision to publicize our detailed Community Standards, reflecting our internal reviewer guidelines, and the introduction of appeals will aid in this process. By providing more clarity on what is and isn't allowed on Facebook, we hope that people will better understand how our policies apply to them. For some violation types, where

people believe we have made a mistake, they can request review of our decisions, and we are working to extend this process further by supporting more violation types.

33. During the hearing, you testified that Facebook will soon, or does, employ 20,000 personnel to work exclusively on content moderation.

a. How many personnel currently work on content moderation? How many new personnel must you hire to reach 20,000?

b. Will all new personnel be directly employed by Facebook?

i. If the answer to question b is no, what percentage of new personnel will be employed directly by Facebook?

ii. What percentage will be employed by a third party?

c. For all new personnel, whether employed directly by Facebook or by a third party, how many will be American citizens?

i. How many new personnel will be foreign nationals?

ii. For all new personnel who are foreign nationals, what worker visa programs—including but not limited to the H-1B and TN visa programs—will Facebook or a third party use? Please provide a list of every specific worker visa program Facebook or a third party intends to use for employment purposes.

iii. What steps will Facebook take to ensure that both the spirt and the letter of the law governing any worker visa program is complied with, both by Facebook itself and any third party?

iv. What additional measures will Facebook or any contracted third party take to ensure that American workers are not displaced by foreign workers?

v. What additional measures will Facebook or any contracted third party take to ensure that foreign workers are not paid a lower wage than their American counterparts?

vi. Will you commit that no American workers will lose their job as a result of Facebook or a contracted third party employing a foreign worker?

Today, we have about 15,000 people working on security and content review across the company.

Of that 15,000, more than 7,500 people review content around the world.

- Our content review team is global and reviews reports in over 50 languages.

- Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours.

- Our goal is always to have the right number of skilled people with the right language capabilities to ensure incoming reports are reviewed quickly and efficiently.

- We hire people with native language and other specialist skills according to the needs we see from incoming reports.

- The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

To provide 24/7 coverage across dozens of languages and time zones and ensure that Facebook is a place where both expression and personal safety are protected and respected, our content review team includes a combination of employees, contractors, and vendor partners based in locations around the world.

Facebook endeavors to comply with all applicable immigration laws in the United States and the other countries where we operate.

34. What regulations would Facebook support?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Questions from Senator Harris

Follow-up Questions Never Answered

At the hearing, I raised a series of questions for which you did not have answers. Please respond to those questions, which include:

1. **Whether Facebook can track users' browsing activity even after the user has logged off of Facebook?**

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 Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. 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.

When the individual is a Facebook user, we are also able to use this information to personalize that individual's experiences on Facebook, whether or not the individual is logged out, but we will not target ads to users relying on this information unless they allow this in their privacy settings. We do not sell or share this information with third-parties.

2. **Whether Facebook can track your activity across devices even when you are not logged into Facebook?**

   See Response to Question 1.

3. **Who are Facebook's biggest competitors?**

In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover, and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if users want to share a photo or video, they can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if people are looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services their mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print, and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon, or Snapchat. Facebook represents a small part (in fact, just 6%) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

4. **Whether Facebook may store up to 96 categories of users' information?**

Your question likely references a *Washington Post* article that purported to identify "98 data points that Facebook uses to target ads to you." The article was based on the writer's use of the tool that allows advertisers to select the audience that they want to see their ads. Anyone on Facebook can see the tool and browse the different audiences that advertisers can select.

The "data points" to which the article refers are not categories of information that we collect from everyone on Facebook. Rather, they reflect audiences into which at least some people on Facebook fall, based on the information they have provided and their activity. For example, the article lists "field of study" and "employer" as two of the "data points" that can be used to show ads to people. People can choose to provide information about their field of study and their employer in profile fields, and those who do may be eligible to see ads based on that information—unless they have used the controls in Ad Preferences that enable people to opt out of seeing ads based on that information. The same is true of the other items in the list of 98.

Further, the specific number of categories that are used to decide what ads a person will see vary from person to person, depending on the interests and information that they have shared on Facebook, how frequently they interact with ads and other content on Facebook, and other factors. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for

them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about.

Please note, however, that (as the article explains) many of these refer to "Partner Categories"—audiences that are offered by third-party data providers. We announced in April that we would stop offering this kind of targeting later this year.

5. **Whether you knew Dr. Kogan's terms of service?**

Facebook has developed an automated system for checking that all apps had terms of service and data policies. In performing such checks, however, Facebook does not examine the content of the developers' terms and policies because app developers act as independent third parties with regard to the data they obtain; they determine the purposes for which, and the manner in which, that data is processed. Our understanding is that this is consistent with the practices of other online and mobile platforms, which generally enable developers on their platforms to provide access to the developers' terms and policies in their app stores, but do not proactively review the substance of those policies.

Although developers act as independent third parties with regard to the data users share with them, all apps on the Facebook Platform must comply with our user data policies, Community Standards, Platform Policies, and Ad Guidelines. Our Platform policy also contains a number of enforcement provisions which apply after an app has been reviewed and approved. Facebook has several teams dedicated to detecting, escalating, investigating, and combating violations of its policies, including schemes to improperly access, collect, or exploit user data. The Developer Operations Policy Enforcement team looks for policy violations and either brings developers into compliance or removes them from the platform, and the Developer Operations Review team conducts an upfront review of apps to confirm proper use of advanced permissions.

6. **Whether you knew that Dr. Kogan could sell or transfer data?**

Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibit selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker, or other advertising or monetization-related service.

Scope of Data Collection

The core of Facebook's business model is the commodification of personal user data. This data culling and packaging is a complex endeavor, but the crux of it is simple—Facebook collects user data, categorizes it into demographic buckets, and works with advertising companies to target ads.

There are two realms of data collection— user-generated data (*e.g.* data input by the user such as name, gender, etc.) and platform-generated data (*e.g.* IP addresses, searches, and likes).

1. **Please answer, for the record, the following with a simple yes or no response. Does Facebook collect and permanently store:**

    a. **Usernames?**

Yes, Facebook collects a user's Facebook URL (e.g., username or vanity for your account). Users can view the vanity URL in their Timeline URL. They can change their usernames via Settings.

    b. **Reported gender?**

Yes, Facebook collects information regarding the gender a user added to the About section of their Timeline.

    c. **Reported address?**

Yes, Facebook collects information regarding a user's current address or any past addresses they chose to include on their account.

    d. **Reported school affiliation?**

Yes, Facebook collects information regarding any information a user added to Education field in the About section of your Timeline. Users can download Education information, as well as other information associated with their Facebook accounts, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

    e. **Reported employment?**

Yes, Facebook collects any current information a user has added to Work in the About section of their Timeline. They can download Work information, as well as other information associated with their Facebook account, through our Download Your Information tool.
We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

    f. **Reported political affiliation?**

Yes, Facebook collects any information a user added to Political Views in the About section of Timeline. Users can download Political Views information, as well as other information associated with their Facebook accounts, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

We recently began to prompt people on Facebook who have added a political affiliation to their profiles to review this information and decide whether they want to keep it on their profiles. More information about these prompts is available at https://newsroom.fb.com/news/2018/05/pardon-the-interruption/.

g. Every friend in a user's network?

Yes, Facebook collects a list of a user's friends. Users can download a list of their friends, as well as other information associated with their Facebook accounts, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things you've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to remove a friend relationship. If they do so, we retain the fact that the friend relationship was removed in order to properly display privacy-protected content (for example, to avoid showing Friends-only information to people who previously had access) and for other purposes related to protecting the safety and privacy of people on Facebook.

h. Every friend ever deleted from a user's network?

Yes, Facebook collects information regarding people a user has removed as friends. Users can download deleted friend information, as well as other information associated with their Facebook account, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

i. Every ad ever clicked on?

Yes, Facebook collects information regarding dates, times, and titles of ads clicked, although the retention period is limited. Users can download information about ads clicked, as well as other information associated with their Facebook accounts, through our Download Your Information tool. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect

how, when, and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

j. Every IP address ever used when logging into Facebook?

Facebook automatically logs IP addresses where a user has logged into their Facebook account. Users can download a list of IP addresses where they've logged into their Facebook accounts, as well as other information associated with their Facebook accounts, through our Download Your Information tool, although this list won't include all historical IP addresses as they are deleted according to a retention schedule.

k. Every "like"?

Yes, Facebook collects posts, photos, or other content a user has liked; likes on their own posts, photos, or other content; and likes they've made on sites off of Facebook. Users can manage the content and information they share when they use Facebook, including "likes," through the Activity Log tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone chooses to Like content on Facebook, they can later choose to remove that like. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

l. Every status change?

Yes, Facebook collects status updates a user has posted. Users can download status updates, as well as other information associated with their Facebook accounts, through our Download Your Information tool, and they can also manage the content and information they share when they use Facebook, including status updates, through the Activity Log tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

m. Every search of another person on Facebook?

Yes, Facebook collects searches a user has made on Facebook. Users can manage the content and information they share when they use Facebook, including searches, through the Activity Log tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook.

When a user searches for something on Facebook, they can access and delete that query from within the search history in their Activity Log at any time, but the log of that search is deleted after 6 months.

2. **Assuming the above is not exhaustive, please list all types of data Facebook collects or otherwise acquires.**

   As explained in our Data Policy, we collect three basic categories of data about people:

   (1) data about things people do and share (and who they connect with) on our services;

   (2) data about the devices people use to access our services; and

   (3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—i.e., their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

We recently announced improvements to our Download Your Information tool, as well as a new feature that makes it easier for people to see the information that's in their account on Facebook. These recently-expanded tools for accessing your information will allow people to see their data, delete it, and easily download and export it.

3. **Please list all data that Facebook generates based on user inputs.**

Depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

- **Things you and others do and provide.** Information and content you provide. We collect the content, communications, and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera, so we can do things like suggest masks and filters that you might like, or give you tips on using camera formats. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described below. Learn more about how you can control who can see the things you share.
    - Data with special protections. You can choose to provide information in your Facebook profile fields or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs, or trade union membership) could be subject to special protections under the laws of your country.
- **Networks and connections**. We collect information about the people, Pages, accounts, hashtags, and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.
- **Your usage**. We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos, and other content you view on our Products. We also collect information about how you use features like our camera.
- **Information about transactions made on our Products.** If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
- **Things others do and information they provide about you.** We also receive and analyze content, communications, and information that other people provide when

they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.

- **Device Information.** As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.

  Information we obtain from these devices includes:

  - Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.

  - Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).

  - Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).

  - Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.

  - Data from device settings: information you allow us to receive through device settings you turn on, such as access to your GPS location, camera, or photos.

  - Network and connections: information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV.

  - Cookie data: data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy and Instagram Cookies Policy.

- **Information from partners.** Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—

including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information. Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us.

Application of European Data Protection Rules

Facebook is not the first company to experience a data breach or have its users' data misappropriated. Previously disclosed data breaches include Equifax, Uber, Yahoo, eBay, AOL, Target, and Home Depot. This suggests that there is a real need for a federal regulatory scheme.

The European Union recently adopted the General Data Protect Regulation (GDPR), which requires businesses to protect the personal data and privacy of EU citizens. These EU rules also protect the exportation of personal data outside the EU.

On April 4, 2018, Mr. Zuckerberg publicly committed to "make all the same controls and settings available everywhere, not just in Europe."

However, according to an April 2018 Reuters report, Facebook intends on altering its terms of service to ensure that non-EU users will have their data processed by Facebook USA. The result is change is that GDPR protections would no longer cover the more than 1.5 billion international Facebook users who are not EU citizens.

1. **Is Facebook still committed to making GDPR privacy settings available to "everywhere"?**

Yes. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability, and others to people in the US and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

   a. **For users in the United States, will Facebook commit to adopting a broad definition of "personal information" including information associated with an identifier number rather than a name is exempt from regulation?**

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important

part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

b. For users in the United States, will Facebook commit to requiring affirmative consent should they seek to use or disclose personal information?

We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within a companies' legitimate interests or the public interest. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue.

c. For users in the United States, will Facebook allow customers to access, correct, retrieve, and delete their personal information?

We enable people, including people in the United States, to learn more about the data we collect through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and through Access Your Information, a tool we've launched for people to more easily access and manage their data on Facebook. People can also control their information through their Settings and the Privacy Shortcuts tool that we're rolling out now.

d. For users in the United States, will Facebook commit to requiring individual notification in the event of a data breach?

Yes.

2. If not, please explain why Facebook no longer will apply GDPR protections to all Facebook users.

As explained in the previous question, the controls and settings that Facebook is enabling as part of GDPR are already available to other people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We also provide the same tools for access, rectification, erasure, data portability, and others to people in the US and rest of world that we

provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

3. **If Facebook does not intend to make GDPR protections available to users in the United States, please explain in detail how Facebook will ensure these users are covered by robust data protection policies?**

As explained in the previous response, Facebook will be making the same controls and settings available under GDPR to people in the US.

4. **Will Facebook change its default settings to minimize the collection and use of U.S. user data?**

We regularly review and update our settings to help people protect their privacy and give people choices about how their information is used and who can see it. That's why, for example, in 2014 we changed the default audience for posts from Public to Friends, and why we now ask people when they create a new account who they would like to see the things they post—their friends, the public, or a different audience.

Foreign Propaganda & Facebook Revenue

Last November, the Senate Intelligence Committee held a hearing on Social Media Influence in our 2016 elections where executives from Facebook, Twitter and Google testified. Following the hearing, I submitted 50 written questions to Facebook and the other companies.

The responses I received were evasive and some were nonresponsive. Please respond to the following question to the best of your ability. Where you have learned new information since submitting answers to previous QFRs, please supplement and amend your previous answers.

1. **How much revenue does Facebook earn from the user engagement that results from foreign propaganda?**

We believe that annual revenue that is attributable to inauthentic or false accounts is immaterial.

2. **How much revenue does Facebook earn from the user engagement that results from fake news?**

See Response to Question 1.

3. **How much revenue does Facebook earn from the user engagement that results from hyper-partisan content?**

We do not have a definition of hyper-partisan, as defining what is hyper-partisan is difficult and controversial.

4. **What does Facebook do with money received from an entity that is found, either through internal audits or third-party notification, to be using the platform to distribute foreign propaganda, fake news, or hyper-partisan content?**

Fraudulent ads are not allowed on Facebook. They are in breach of our advertising policies and we will remove them when we find them. Where we discover ads that violate our policies or applicable laws, we do not generally return money to those attempting to deceive our users. Instead, we make investments in areas to improve security on Facebook and beyond. In addition, the investments that we are making to address security issues are so significant that we have informed investors that we expect that the amount that we will spend will impact our profitability.

5. **How many employees are dedicated to addressing foreign propaganda?**

We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. This type of abuse touches a number of different teams at Facebook. Thousands on our Business Integrity team will be working to better enforce our ad policies and to review more ads, and a significant number of engineers will build tools to identify ad and election abuse, and to enable us to follow through on our commitment to bring greater transparency to ads with political content.

Facebook Data Abuse Bounty

In April 2018, Facebook's announced a new "Data Abuse Bounty" program to "reward people who report any misuse of data by app developers."

According to your press release, "this program will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence."

Facebook also promised to shut down any offending apps if it confirms that an app has abused user data.

1. **Please list what abuses of data this program has identified and whether Facebook has investigated or is in the process of investigating these abuses.**

This is a pilot program. We assess all submissions for validity, and if valid, conduct an investigation. Since launching the program we have received and are reviewing hundreds of reports. Updates about the Bug Bounty Program and the Data Abuse Bounty Program will be posted at https://www.facebook.com/bugbounty and https://www.facebook.com/data-abuse.

2. **Please list how many offending apps have been identified and subsequently shut down.**

Since launching the program we have received and are reviewing hundreds of reports. Updates about the Bug Bounty Program and Data Abuse Bounty Program will be posted at https://www.facebook.com/bugbounty and https://www.facebook.com/data-abuse.

3. **Please explain how and when you intend to notify users impacted by newly-discovered data abuses.**

Where we find evidence that these or other apps did misuse data, we will ban them and notify people whose data was shared with these apps.

4. **Upon identifying a malicious app, has Facebook considered other punitive measures beyond denying apps access to the platform (such as fines, lawsuits, etc.)? If not, please explain why not.**

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica.

Embedding Employees in Campaigns

Facebook often embeds staff with advertising clients to help them target their campaigns.

Brad Parscale, the Trump Campaign's digital director, said of Facebook: "we had their staff embedded inside our offices," and "Facebook employees would show up for work every day in our offices." Mr. Parscale said that staff provided to the Trump Campaign by Facebook and other companies worked "side by side" with Cambridge Analytica.

Press reports indicate that Cambridge Analytica ultimately had 13 people working on the Trump campaign's digital operation, headquartered in San Antonio.

1. **What services did embedded Facebook staff provide?**

Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. During the 2016 election cycle, Facebook worked with campaigns to optimize their use of the platform, including helping them understand various ad formats and providing other best practices guidance on use of the platform. No one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign.

2. **Did these employees have a set of rules, standards or regulations under which they provide these services?**

We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

3. **Was there a mechanism through which they could alert Facebook if they had concerns about the campaign's activities?**

Facebook employees are encouraged to raise any concerns about improper activity to their managers.

4. **How many people did Facebook send to San Antonio to work with the Trump Campaign's digital operation? For how long?**

We offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered. The campaigns did not get to "hand pick" the people who worked with them from Facebook. And no one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign. Both campaigns approached things differently and used different amounts of support.

5. **Did Facebook employees embedded with the campaign work directly or indirectly with Cambridge Analytica?**

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.

6. **What, exactly, did the Facebook "embeds" work on with Cambridge Analytica in San Antonio?**

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. No one from Facebook was assigned full-time to the Trump campaign.

7. **Were Facebook employees aware of data sets that may have been scraped from Facebook users?**

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.

8. **Did Facebook work with Cambridge Analytica, directly or indirectly, on ad optimization or voter targeting?**

Facebook representatives provide general ad support to political advertisers on Facebook, as they do with other, non-political managed accounts. During the 2016 election cycle, for example, Facebook provided technical support and best practices guidance to advertisers, including Cambridge Analytica, on using Facebook's advertising tools.

9. **Did Cambridge Analytica or Parscale's digital operation purchase media on Facebook?**

Yes.

10. **Reports suggest that the Special Counsel has met with at least one Facebook employee who worked in San Antonio. Is Facebook cooperating fully with the investigation?**

We have stated publicly that we have cooperated with the Special Counsel.

11. **What role has Facebook played in supporting Cambridge Analytica/SCL work on elections in other countries (in Africa, the Caribbean, former Soviet Republics, etc.)?**

Facebook did not provide support to Cambridge Analytica/SCL in connection with elections in other countries. It also appears from the best information we have to date that Kogan only provided SCL with data on Facebook users from the United States. Kogan and SCL have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States, which is supported by a contract between Kogan's company and SCL, which was furnished by Christopher Wylie to the UK Parliament.

12. **Did Facebook, in the past 4 years, embed employees with Cambridge Analytica for foreign electoral campaigns/referenda, including Brexit or elections in Nigeria, Kenya, the Czech Republic, Lithuania, or Georgia?**

No.

13. **Has Facebook ever provided support to Secure America Now, a political action committee targeting swing state voters with anti-Muslim messaging?**

We did not work directly with Secure America Now; we worked through a third-party advertising agency. Neither did we create any content for Secure America Now. As is customary across managed advertising agencies, we provided a general best practices training to the agency staff. As is also customary, we provided the measurement tools to determine the efficacy of the ads and differences between formats.

14. Who at Facebook would have overseen work on this account?

We did not work directly with Secure America Now; we worked through a third-party advertising agency.

15. Did it raise any ethical concerns within Facebook? If not, please explain.

See Response to Question 13.

We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm. That said, we do not allow hate speech on our platform because it creates an environment of intimidation and exclusion and in some cases may promote real-world violence.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at https://www.facebook.com/communitystandards/objectionable_content/hate_speech.

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect you from things like discriminatory ads—and we have recently tightened our ad policies even further to prohibit additional shocking and sensational content.

Third-Party Data Aggregators & Third-Party Transfers

Prior to March 2017, Facebook worked with third-party data aggregators to enhance existing data sets. As a result, advertisers had access to data collected by Facebook and data collected by third parties such as Experian and Acxion.

In the aftermath of the Facebook-Cambridge Analytica debacle, Facebook announced that it would be shutting down Partner Categories and that third-party data providers would no longer be able to offer their targeting directly on Facebook.

This verbal commitment is laudable but must be implemented in order to ensure the public's data are safeguarded.

1. **Please detail any efforts Facebook has initiated and/or completed to identify other improper third-party data transfers.**

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. If we find suspicious activity, we will take immediate steps to investigate (including a full forensic audit) or take enforcement actions against the app. If we determine that there has been improper use of data, we will ban those developers and notify everyone affected. Facebook is launching the Data Abuse Bounty to reward people who report any misuse of data by app developers. The Data Abuse Bounty, inspired by the existing bug bounty program that we use to uncover and address security issues, will help us identify violations of our policies.

2. **What, if any, external audits has Facebook completed to ensure that all third parties are following Facebook privacy policies?**

See Response to Question 1.

Facebook's New Partnership with Independent Researchers

On April 9, 2018 the William and Flora Hewlett Foundation, announced it would fund a research initiative to examine Facebook's role in elections and democracy.

The fund will support an independent committee of scholars who will define research topics and vet research proposals that explore the intersection of elections, democracy, and social media.

In addition, according to media reports, Facebook has reportedly agreed to give research accesses to proprietary data.

1. **Facebook has limited this new initiative to prospective studies. Will Facebook commit to allowing studies of Russian interference in the 2016 election?**

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/.

2. **The new initiative also does not appear to cover studies on privacy and security, even though those are some of the most pressing issues related to your platform. Will you commit to expanding the initiative to cover privacy and security?**

We regularly work with privacy experts outside the company, including academics, to understand how to improve privacy protections for people on Facebook and to support efforts to improve privacy protections for people overall. For example, we recently hosted a workshop for privacy academics to discuss research around online privacy and worked with academics as a part of recent privacy consultations that we have conducted at our headquarters and around the world.

Also, we recently announced plans to collaborate with academics and other privacy experts as a part of our efforts to build Clear History, a new feature that will enable people to see the websites and apps that send us information when they use them, delete this information from their account, and turn off our ability to store it associated with their account going forward.

3. **Given that many of the issues with Facebook relate to income, ethnicity, gender, sexual orientation, and other diverse groups, will you commit to ensuring that this committee includes individuals who will adequately represent perspectives of these diverse groups?**

In consultation with the foundations funding the initiative, Facebook will invite respected academic experts to form a commission which will then develop a research agenda about the impact of social media on society—starting with elections. We are keen to have a broad range of experts—with different political outlooks, expertise and life experiences, gender, ethnicity, and from a broad range of countries.

Discriminatory Ad Practices

Facebook offers advertisers "targeting categories" that range from ethnic affinity, education level, political affiliation, and employment status. The categories may seem innocuous but invariably serve as proxies for demographic characteristics such as race, family status, class, and sexual orientation.

A recent *Pro Publica* report revealed that, in February 2017, companies could still buy rental-housing ads on Facebook and request that those ads not be shown to certain categories of users including African Americans, mothers of high school kids, people interested in wheelchair ramps, Jewish people, and Spanish speakers.

As of March 27, 2018 housing rights advocates are suing Facebook in Federal court for allowing real estate brokers and landlords to exclude select certain categories—family status, sex, and disability—when targeting advertisements.

1. **Does Facebook still allow advertisers to target based on the abovementioned categories?**

Discriminatory advertising has no place on Facebook's platform and Facebook removes such content as soon as it becomes aware of it. Facebook's policies prohibit advertisers from discriminating against people on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic conditions. Facebook educates advertisers on our anti-discrimination policy, and in some cases, requires the advertisers to certify compliance with Facebook's anti-discrimination policy and anti-discrimination laws.

Facebook also uses machine learning to help identify ads that offer housing, employment, or credit opportunities. When an advertiser attempts to show an ad that Facebook identifies as offering a housing, employment, or credit opportunity and includes Facebook's multicultural advertising segments, Facebook will disapprove the ad. Facebook also requires advertisers to certify that they are complying with Facebook's updated anti-discrimination policy and anti-discrimination laws when the advertiser attempts to show a housing, employment, or credit opportunity and uses any other audience segment on Facebook.

2. **Do you agree this categorization lends itself to discriminatory practices?**

See Response to Question 1.

3. **As Facebook works to reform company policies, how will Facebook protect the civil rights of all Facebook users?**

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running a housing ad—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

We look forward to finding additional ways to combat discrimination, while increasing opportunity for underserved communities, and to continuing our dialogue with policymakers and civil rights leaders about these important issues.

4. **Will you commit to modifying your existing policies and procedures to ensure that housing discrimination is prohibited on your platform?**

See Response to Question 3.

2015 Cambridge Analytical Leak & Decision not to Notify Users

On March 17, 2018, the *New York Times* reported that the data analytics firm, Cambridge Analytica, had secretly harvested the personal data of millions of Facebook users.

Reports have confirmed that Facebook knew of this data breach in December 2015, but declined to notify the affected users.

On April 10, 2018, Mr. Zuckerberg confirmed that such a decision had, in fact, been made. At a Joint hearing with the Senate Commerce and Judiciary Committees, when asked whether there was "decision made [by Facebook] not to inform the users [of the breach]," Mr. Zuckerberg replied "that is my understanding, yes."

1. **Please explain how, and when, Facebook first became aware of Cambridge Analytica's misappropriation of Facebook users' data?**

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. As part of its investigation, Facebook contacted Kogan and Cambridge Analytica to investigate the allegations reflected in the reporting. Thereafter, Facebook obtained written certifications or confirmations from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all such data they had obtained was accounted for and destroyed. In March 2018, Facebook received information from the media suggesting that the certification we received from SCL may not have been accurate and immediately banned SCL Group and Cambridge Analytica from purchasing advertising on our platform. Since then, Facebook has been actively investigating the issue, including pursuing a forensic audit of Cambridge Analytica, which is currently paused at the request of the UK Information Commissioner's Office (which is separately investigating Cambridge Analytica).

Mr. Zuckerberg did not become aware of allegations that Cambridge Analytica may not have deleted data about Facebook users obtained from Kogan's app until March of 2018, when these issues were raised in the media.

2. **What steps did Facebook take in deciding not to inform impacted Facebook users of Cambridge Analytica's misappropriation of their data? When did Facebook decide not to inform Facebook users who were impacted?**

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, it took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their newsfeed.

3. **Who at Facebook made the decision not to inform Facebook users?**

See Response to Question 2.

4. **What was the rationale for this decision?**

See Response to Question 2.

5. **When did Mr. Zuckerberg learn of this breach and the decision not to inform users?**

See Response to Question 2.

6. **Are there changes in place to improve the way Facebook responds to these breaches in the future?**

Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at https://www.facebook.com/help/218345114850283?helpref=about_content.

The categories of information that an app can access is clearly disclosed before the user consents to use an app on Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

7. **Please list other instances of abuse where Facebook user data was misappropriated and a decision was made not to inform users or where the company failed to inform users.**

See Response to Question 6.

Annual Transparency Report

On June 1, 2017 Facebook shareholders voted down a transparency proposal requesting that "Facebook issue a report reviewing the public policy issues associated with fake news enabled by Facebook. The report should review the impact of current fake news flows and management systems on the democratic process, free speech, and a cohesive society, as well as reputational and operational risks from potential public policy developments."

Facebook's board of directors urged a no vote on the proposal, calling the report "unnecessary" and "not beneficial to shareholders." The shareholder proposal failed.

Since then, Facebook has publicly acknowledged that Russian actors purchased ads to manipulate and interfere with the election. It took Facebook two years and a whistleblower before to disclose the data breach by Cambridge Analytica.

It appears that the ordinary practice and tendency of Facebook – like most other companies – is to advocate for less disclosure.

1. **Will Facebook commit to producing an annual public transparency report to your shareholders?**

Facebook publishes an annual transparency report, the most recent report was issued on May 15, 2018 and can be found here: https://transparency.facebook.com/.

Questions from Senator Hatch

1. **I understand that until just recently, Facebook split its privacy policy across 20 or more separate webpages, making it virtually impossible for a typical user to understand what information he or she was agreeing to allow Facebook to share. Why did you have in place such a convoluted privacy policy? Why not make the policy as clear, easy to understand, and accessible as possible?**

We've heard loud and clear that it's important to make privacy information and controls easy for people to find and use. We've made recent improvements to our privacy settings to centralize people's choices, and are providing access to people's key privacy choices through an updated Privacy Shortcuts feature.

With regard to our Data Policy specifically, it has been available in a single webpage for many years. We recently updated our Data Policy in response to feedback that, among other things, we should provide more detailed explanations and improve the design of the policy. Like its predecessor, this policy is framed around short, easy-to-understand topics and questions, like "What kinds of information do we collect" and "How can I manage or delete information about me."

In designing both our newly updated Data Policy and its predecessor, as well as our Privacy Basics educational center, we were mindful of guidance from the FTC and many other experts that recommend so-called "layered" privacy policies, which make it easy to find topics and high-level information but enable people to access more detailed information if they wish to do so.

2. **I've been a bit perplexed by the way Facebook has come in for such criticism when so many other online platforms use a similar business model. I don't necessarily want to name names here, but Facebook is far from the only website that makes money by offering advertisers the ability to target ads to specific user groups. How does your business model differ from, say, Google's, or from other social media sites?**

Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

3. **Is Facebook unique in the way it collects user information and offers targeted advertising? How do your data practices differ from those of other websites?**

No. Countless online and offline companies sell and display advertising to support the costs of their services, and most engage in a variety of practices (targeting, contextual placement, list management) to deliver the most relevant and cost-effective advertising to people and businesses. Ad-based business models have long been a common way to enable companies to offer free services, even before the advent of the Internet when media like radio, television, and newspapers were ad-supported. Online advertising is particularly important for smaller and more niche publishers, as well as services—like Facebook—whose mission is to provide access to everyone, regardless of their location or ability to pay for services.

While we provide similar services to other websites—and to the third-party providers of online advertising services on which many websites rely—we are unique in the level of control we offer over how we use information to deliver ads. For example, we launched an About Facebook Ads page (www.facebook.com/ads/about) that explains how we use information to deliver Facebook ads. Every ad on Facebook comes with a "Why am I seeing this?" tool that lets people learn why they are seeing that particular ad, and to control whether they would like to see similar ads in the future. And we have built a comprehensive Ad Preferences tool, which enables people to see interests that we use to decide what ads to show people, and the list of advertisers that are showing people ads on Facebook because of past interactions with the advertiser.

Although these features exceed the transparency and control offered by many other companies, we've heard that we need to continue to invest in improvements in this area. That's why, among other things, we've announced plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

4. **Does Facebook ever share user data with advertisers? If so, in what circumstances does Facebook share such data? Do advertisers ever learn the names of, or identifying information about, the individuals who receive their advertisements?**

We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies people (information such as name or that by itself can be used to contact or identifies a person) unless we have permission from people. For example, we provide statistical demographic information to advertisers (for example, that an ad was seen by 2,436 women between the ages of 25 and 34 in Maryland) to help them better understand their audience. We also confirm which Facebook ads led people to make purchases or take an action with an advertiser.

5. **How would limiting Facebook's ability to offer targeted advertising change your business model? How would it impact the services you offer to customers?**

To build a secure product with extensive infrastructure that connects people across continents and culture, we need to make sure everyone can afford it. To do this, we sell advertising, and we could not offer our service for free without selling advertising. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone.

Separately, our core service involves personalizing all content, features, and recommendations that people see on Facebook services. No two people have the same experience on Facebook or Instagram, and they come to our services because they expect everything they see to be relevant to them. If we were not able to personalize or select ads or other content based on relevance, this would fundamentally change the service we offer on Facebook—and it would no longer be Facebook.

6. **In your written testimony, you discuss new efforts to verify advertisers who want to run political or issue ads on Facebook. It strikes me that this effort should apply to more than just political ads. For example, shouldn't you also put in place checks for**

advertisers that use your platform to illegally peddle prescription drugs? Which advertisers will need to be verified under your new policies? And how can we be sure that Facebook won't use these new policies to engage in viewpoint discrimination?

Last October, we announced that we would require advertisers running electoral ads to verify their identities and locations. We also announced that we would require these ads to use a "paid for by" label and that we would include them in a searchable archive. In April, we announced that we would extend these transparency measures to "issue ads"—ads about national policy issues. We have worked with third parties like the Comparative Agendas Project to define an initial set of issues, and we will refine that list over time.

Questions from Senator Hirono

Collection of Personal Data of Non-Facebook Users

1. **We asked you many questions at our hearing about what rights Facebook users have or should have to know what personal data of theirs Facebook has, to know who their data is shared with, and to have effective control over the use of their personal data. At a hearing the next day in the House of Representatives, you testified that Facebook also collects "data of people who have not signed up for Facebook." These are people who are not on Facebook and have had no ability to opt in or out of sharing their personal data. In many if not most instances, they may not know that Facebook has collected this data.**

   In response to criticism of this revelation, Facebook told the press that it has no plans to build a tool that would disclose to non-users that their data had been collected. Facebook's statement stated that "[t]his kind of data collection is fundamental to how the internet works," and "standard to how the internet works" and suggested that people use "browser or device settings to delete cookies," which are one of the ways in which Facebook and others track people on the internet.

   I have serious concerns that this answer is incomplete and dismissive of the concerns. You said at the House hearing that this kind of 3rd-party data collection was done for "security purposes." But that answer also seems incomplete and not consistent with Facebook's later statement that this is "standard to how the internet works." Let me give you an opportunity to clarify.

   a. **Why do you collect this third party personal data from non-Facebook users?**

   b. **How do you collect this third party personal data from non-Facebook users? Please be specific, including whether and how you use "cookies" and other hidden trackers.**

   c. **How do you use the personal data you collect from non-Facebook users? What do you use it to measure or analyze?**

   d. **Do you use the personal data of non-Facebook users to target ads? If so, how is that consistent with your testimony at the hearing that such data is collected for "security purposes"?**

   e. **Does collecting cookies from any websites with Facebook "like" buttons or otherwise tracking the data of non-Facebook users serve any "security purposes"? If so, how? If not, why did you testify that the collection of such date was for "security purposes"?**

   f. **How do you store personal data you collect from non-Facebook users? Do you ever delete this data?**

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 Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. 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.

2. **According to the Princeton Web Transparency & Accountability Project (WebTAP), Facebook trackers are used on about 25% of the top million websites. Gabriel Weinberg, CEO and Founder of DuckDuckGo, an internet privacy company, wrote recently on FastCompany.com that Facebook uses these trackers to create "shadow profiles" even of non-Facebook users based on their browsing history. However, Facebook said in a press statement that it does not create databases on non-users by combining web-browsing history with uploaded contacts.**

    a. **Can you confirm that you do not create such databases of non-users or clarify in what ways you collect and use the personal data of non-users that you collect?**

b. Can you specify whether you use tracking of non-Facebook users' personal data to create "shadow profiles" of them and/or any other type of profile of them and, if so, how are these profiles used?

c. Do you believe that Americans who use the internet have a right to know they are being tracked and profiled by Facebook and other companies like Google? Do you believe American have the right to have access to the contents of those profiles?

d. Given that non-users of Facebook have not had the opportunity to consent at all to Facebook's collection of their data, let alone its use, do you believe they should be given the opportunity to "opt in" before their personal data is tracked and captured?

Facebook does not create profiles or track website visits for people without a Facebook account. See response to Question 1 for more detail.

Adopting the EU's Model for Personal Data Protection

3. On May 25, just a few weeks from now, the European Union will put into effect its new General Data Protection Regulation, or GDPR. Under that system, the concept of ownership over personal data is almost completely upside down from what we have in America. In Europe, where data protection is a fundamental right, consent to use that information can only be given if it is clear, affirmative and unambiguous. Owners of data may withdraw their consent at any time, and companies and organizations must notify the EU of serious data breaches as soon as possible, and not wait years, as happens here.

The week before our hearing, you told reporters that you intend to make the same controls and settings required under the GDPR everywhere. However, when you were asked about applying these new regulations in the U.S., you were much more vague, committing only that applying these European regulations here in the U.S. is "worth discussing." I want to start having that discussion now.

a. Will you commit to making the setting and controls required by GDPR available everywhere, including in America? If not, why not, and what privacy controls and settings will you make available here?

The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability, and others to people in the US and the rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

b. Will users in this country have the right to data portability, where they will be able to transfer their personal data from Facebook if they choose?

See Response to Question 3(a).

c. At the hearing many Senators discussed with you the need for Facebook users to be notified promptly when their data has been hacked. You told Senator Klobuchar you though 72 hours for notification "makes sense to [you]." Can you commit to a 72 hour timeline for notification?

One of the challenges with notification in the United States is that there is no federal breach notification law, which means that notification technically requires reaching out to 50 different state regulators under a patchwork of different frameworks. While we would support a short time period for notification in the United States, this would need to be part of a centrally managed federal scheme that would make this process efficient and manageable. In Europe, for example, we are required to notify our lead supervisory authority—the Irish Data Protection Commissioner—within 72 hours of a data breach that poses a risk to the rights and freedoms of data subjects, not every single Member State's data protection authority. Moreover, the GDPR only requires notification to people in cases where there is a high risk of harm to an individual resulting from the breach and where the data controller is unable to mitigate that harm through subsequent measures that prevent continued access to the data, etc. GDPR thus creates incentives for companies to work with a lead regulator and to mitigate harm to people, reserving notification to people for cases where there is no other means to avoid a high risk of harm to people. This reflects a responsible and thoughtful evaluation of the potential risks to people resulting from public notification, which would have the effect of publicizing a breach that could then be exploited by bad actors (who might not otherwise know about it). The regulatory notification requirement ensures there is appropriate oversight in a specific situation.

d. Will you treat what Article 9 of the GDPR calls "Special Categories" of personal data, such as data revealing, among other things, racial or ethnic origin, religious beliefs, and genetic data, according to the strict EU standards?

We are prompting people in Europe and in the United States to go through an engagement flow that educates them about data they have shared on their profiles that constitutes "special categories of personal data" under GDPR (such as information they choose to include in their profile like religious and political views). This experience gives people—including both people in Europe and people in the US—the ability to delete this information from their profile through in-line controls.

e. Will Facebook users who gave consent to share their data be able to withdraw that consent at any time?

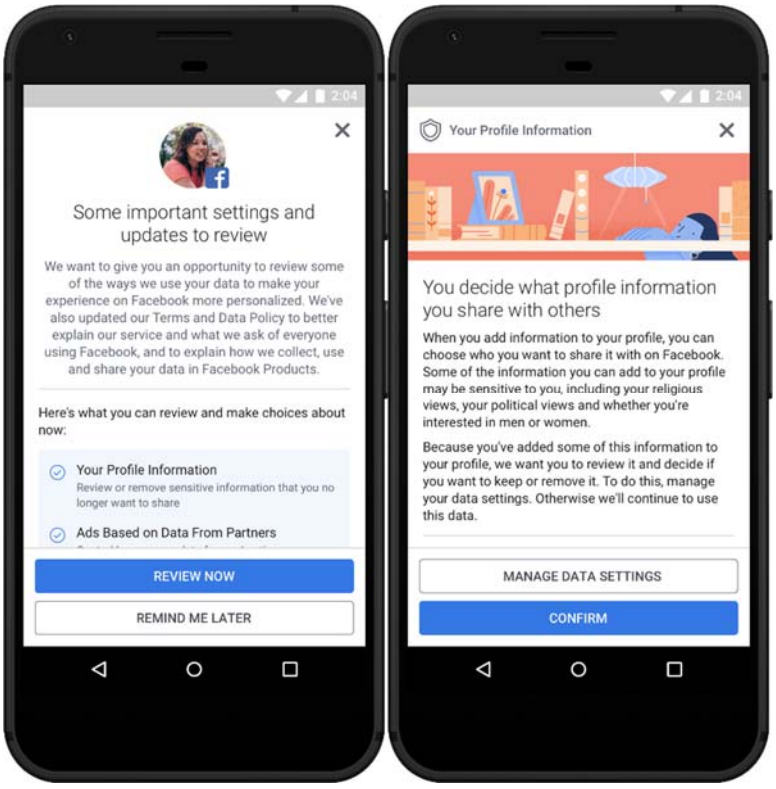
Yes, by visiting Facebook Settings. For sharing of specific pieces of information, such as a Facebook post or a field in a person's Facebook profile, people also have the ability to delete this information or change the audience who is eligible to see it.

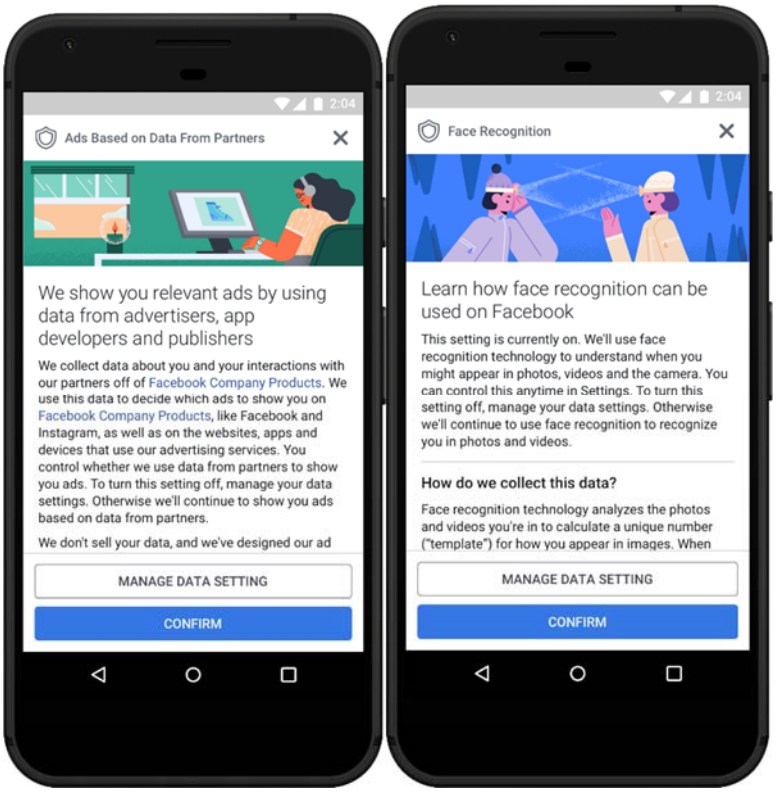
f. Would Facebook's collection of the personal data of non-users be permissible under these GDPR regulations, which require affirmative notice and consent?

GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within a company's legitimate interests or the public interest, etc. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue. The GDPR does not differentiate between users and non-users, and indeed, many online or digital services around the world do not require registration or distinguish between "users" and "non-users" before collecting or logging data, such as browser logs of people who visit their website.

g. Considering that these regulations go into effect in less than a month, can you produce to the Committee the language that European users of Facebook will be presented with on May 25?

Yes, here are screenshots of the consent flows being provided in Europe:





Discriminatory Targeting of Facebook Ads

4. **I asked you several questions about whether Facebook is following its own stated policy of forbidding Facebook ads that excluded audiences for the ads on the basis of race, gender, family status, sexual orientation, disability or veteran status. These are all categories prohibited by federal law in housing and employment law. Yet, in October 2016, journalists at Pro Publica revealed that it was possible to buy Facebook ads that excluded these audiences. Even though Facebook announced in In February 2017 that it would no longer allow such ads, a year later Pro Publica found they could still place them. They also found ads for employment that excluded age groups employers weren't interested in targeting, also a violation of federal law.**

   I appreciated your sincerity in telling me and other Senators that it is "against [Facebook] policies to have any ideas that are discriminatory." I also appreciate your candor, after describing the need for more active screening, in admitting that policing discriminatory targeting is "a work in progress." I want to ask you about the path forward in enforcing your policy, and your assessment of Facebook's capacity to handle these problems and the legal concerns they raise without outside enforcement.

   a. **At the hearing you cited your anti-discrimination policy. Yet, it has been well over a year since Facebook announced it would no longer allow ads that used discriminatory, and in some cases illegal, targeting and you admit that you still need to develop better tools. How do you measure and assess that you efforts to enforce your own anti-discrimination policies are working?**

b. The story from Pro Publica suggests little if any progress has been made, even though during the whole period of time your policy against discrimination was your policy, and you explicitly banned the purchase of ad engaging in discriminatory targeting over a year ago. Recognizing this is a "work in progress," what does improvement look like to you? What does complying with your policy look like to you?

c. What accountability is there for failure to comply with your policy against discriminatory targeting?

d. In addition to your existing screening of ads and flags raised by the community that you follow-up on with your team, you suggested that Facebook needs "to develop more AI tools that can more proactively identify those types of content and do that kind of filtering up front." What are your plans for developing and timeline for deploying these tools, and when do you expect to see a measurable progress the elimination of discriminatory targeting?

e. Is there a way for the public to verify that you have made progress or are we just expected to trust you?

Our Terms and Advertising Policies have long emphasized our prohibition on the use of Facebook's platform to engage in wrongful discrimination. Starting in late 2016, we began implementing additional protections for the people who use Facebook. Specifically, we set out to help better educate advertisers about our policies against discrimination and relevant federal and state laws, and to help prevent the abuse of our tools. First, we updated our Advertising Policies applicable to all advertisers and advertisements to strengthen our prohibition against discrimination, and we added a section to provide advertisers with anti-discrimination educational resources from government agencies and civil rights groups. Second, we implemented technical measures aimed at better protecting users from wrongful discrimination by advertisers that offer housing, employment and credit opportunities. We continue to work to improve these measures.

We are continuing to evaluate the targeting options we make available to advertisers. This work involves consultation with key stakeholders outside the company, including with policymakers, regulators, civil rights experts, and consumer advocates. The decision to remove targeting options is not something we take lightly: as many of these stakeholders have pointed out, targeting is a key mechanism for forging meaningful connections between people and organizations on Facebook.

One recent example illustrates the challenge of getting this work right. Earlier this year, we eliminated the ability to target people based on the "interested in" field that people can add to their Facebook profiles. People can indicate that they are interested in men, women, or both, and some consider the field to be a place where people can indicate their sexual orientation. After receiving feedback from a range of stakeholders, we eliminated the ability to target based on this field. Although some groups applauded the decision, others criticized it, noting that it would now be harder to reach certain groups.

We also are working to provide more in-product education about advertisers' obligations under our non-discrimination policy, and anticipate that this education will be more detailed and will be presented to a broader range of advertisers than our current education. Finally, we will soon launch View Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page. This level of transparency is unprecedented among advertising platforms, and we believe it will further our efforts to combat discrimination by giving people the opportunity to see ads regardless of whether they are in the target audience.

We have focused on measures that are designed to prevent advertisers from misusing our tools to place discriminatory housing, credit and employment ads, including: requiring such advertisers to certify their compliance with our Advertising Policies and with relevant anti-discrimination laws and prophylactically removing advertisers' ability to use certain categories of information to target their audience. Some of these measures are proactive, such as the classifiers we use to detect when an advertiser is attempting to run a housing, credit, or employment ad. Facebook rejects ads from advertisers who do not certify compliance. We also recently launched automated tools to proactively identify racist or offensive content and hate speech in ads.

In addition, Facebook conducts an automated review of ads to ensure that they do not assert or imply personal attributes in violation of our Advertising Policies. Ads that violate this policy are rejected. Advertisers can appeal these rejections. Understanding that we might not be able to prevent every misuse of our ad tools, we encourage users to report offensive ads to Facebook. Ads that violate our Advertising Policies are removed when we become aware of them. We also anticipate that the View Ads tool—which, as described above, will allow people to see all the ads an advertiser is currently running—will encourage people to report more ads to us, and will therefore enhance our efforts to curtail misuse of our tools.

Consumer Protection for Facebook Users

5. **American consumers rightfully expect that they can take part in the market for goods and services while being protected from certain kinds of harm. The government makes sure that our food and drugs aren't tainted. We have laws that make sure advertising in print or on TV and radio doesn't contain lies. We demand transparency and honesty from banks and stock brokers.**

   Yet, for Americans using Facebook, there is almost a total lack of these kinds of protections. And when Americans suffer harm, there is no accountability for Facebook. We are expected to hand over our most vital personal information with no control over how it is used or misused, and we are told this is the cost of "connection" and of being part of the Facebook "community". I know that since some of the worst breaches of trust were discovered you've been talking about the steps you are taking to do better.

   a. **Why should we leave it up to you to protect America's Facebook consumers?**

b. Do you think they are any less deserving of their government's protection than milk drinkers or detergent buyers or home buyers seeking a mortgage? What makes your business different?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on our platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

6. When users sign up for services on Facebook, they are asked for consent to use their personal data in certain ways. But it's typically in the form of pages of small print that pop up on the screen that few people bother to read. And as these terms of services change over time or as users sign up for new services, they are asked to click a box next to yet more pages of small print. The Pew Research Center tells us that about 52% of internet users believe that "when a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."

Do you believe this is a reasonable expectation of people who sign up to use Facebook? Should it be?

We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that 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 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.

Advertising Revenue Model and Facebook's Mission

7. **At the hearing and in recent interviews you have defended Facebook's approach to generating advertising revenue by targeting ads towards users. You proudly said that a model based on adverting is the only rational way to make Facebook accessible to all people. In response to Apple CEO Tim Cook saying he wouldn't have gotten himself into a situation like the one you and Facebook find yourselves in, you talked a lot about ways that Facebook shows it cares about its users. You defended your model as the best way to connect everyone.**

    a. **But is an advertising based model really the only way to make Facebook accessible to all people, or is it the only way to do so while making massive profits?**

Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together. To build a secure product with extensive infrastructure that connects people across continents and culture, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone.

Separately, our core service involves personalizing all content, features, and recommendations that people see on Facebook services. No two people have the same experience on Facebook or Instagram, and they come to our services because they expect everything they see to be relevant to them. If we were not able to personalize or select ads or other content based on relevance, this would fundamentally change the service we offer on Facebook—and it would no longer be Facebook.

We maintain our commitment to privacy by not telling advertisers who users are or selling people's information to anyone. That has always been true. We think relevant advertising and privacy are not in conflict, and we're committed to doing both well.

b. Isn't there a better way that balances the making of profits with stronger privacy protections, and shouldn't it be our role in Congress to make sure we are keeping that balance?

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control—to helping people understand how their data is collected and used, and to giving them meaningful controls.

8. Facebook's stated mission is "to give people the power to build community and bring the world closer together."

a. How is this mission consistent with your business model of finding ways to extract value from the personal data of users?

See Response to Question 7(a).

b. Doesn't the gross misuse of users' data without their consent to better target them with fake news undermine this mission by devaluing and dividing the community?

We believe targeted advertising creates value for people and advertisers who use Facebook. Being able to target ads to the people most likely to be interested in the products, service or causes being advertised enables businesses and other organizations to run effective campaigns at reasonable prices. This efficiency has particularly benefited small businesses, which make up the vast majority of the six million active advertisers on Facebook. That said, we are keenly aware of the concerns about the potential of our tools to be abused. That is why we are investing heavily in improving the security and integrity of our platform.

c. What happens the next time you have a business reason to again compromise the personal data of users, or at least look the other way?

We do not have a "business reason" to compromise the personal data of users; we have a business reason to protect that information. Our mission is to build community and bring the world closer together, but it is not enough to just connect people—we have to make sure those connections are positive. If people's experiences are not positive—if we fail to maintain their trust—they will not use our services.

Irish Elections

9. **On May 25, 2018, there will be a referendum conducted in Ireland to determine whether there will be changes in abortion laws. Is Facebook willing to implement full transparency of political ads that they have accepted have targeted Irish voters, together with any information they hold on the person or organizations who paid to promote the content?**

As of April 25, we added Ireland to our pilot program for the first phase of our transparency efforts—the View Ads tool. This has enabled Irish Facebook users to see all of the ads every page is running on Facebook targeting users in Ireland at the same time. We also announced on May 8 that we would begin rejecting ads related to the referendum if run by advertisers based outside of Ireland.

Questions from Senator Klobuchar

In the hearing, I asked if Facebook had determined whether the up to 87 million Facebook users whose data was shared with Cambridge Analytica were concentrated in certain states. You said that you could follow up with that information.

- **Can you provide a state-by-state breakdown of the Facebook users whose data was improperly obtained by Cambridge Analytica?**

See the state breakdown here: https://fbnewsroomus.files.wordpress.com/2018/05/state-by-state-breakdown.pdf.

As you know, I also asked whether any of the roughly 126 million people who may have been shown content from a Facebook page associated with the Internet Research Agency were the same Facebook users whose data was shared with Cambridge Analytica. You said that Facebook was investigating that question and that you believe it is "entirely possible that there will be a connection there."

- **Please provide an answer as to whether there was any overlap between the Facebook users who were shown content from a Facebook page associated with the Internet Research Agency and those whose data was shared with Cambridge Analytica.**

The targeting for the IRA ads that we have identified and provided to the Senate Committee on the Judiciary and the Senate Select Committee on Intelligence was relatively rudimentary, targeting very broad locations and interests, and for example, only used custom audiences in a very small percentage of its overall targeting and did not use Contact List Custom Audiences. In addition, all of the custom audiences used by the IRA were created based on user engagement with certain IRA Pages. By contrast, Cambridge Analytica used hundreds of Contact List Custom Audiences during the 2016 election cycle created from contact lists that Cambridge Analytica uploaded to our system, and Cambridge Analytica used those and other custom audiences in the majority of its ads targeting in combination with demographic targeting tools.

When I asked if you would support a rule that would require Facebook to notify users of a breach of their information within 72 hours, you responded that such a rule makes sense to you and that your team would follow up with my staff to discuss the details of such a proposal.

- **I am working to introduce bipartisan legislation requiring that online platforms notify users of a breach of their information within 72 hours. Will Facebook support this requirement?**

- **What process would Facebook implement to notify users of a breach of their information within 72 hours?**

Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

With more than two billion monthly active users, Facebook is by far the largest social networking platform on the internet. Some have called Facebook a monopoly and claimed that Facebook has no true competition.

- **If a Facebook user living in the United States wanted to switch to a different online social networking platform, what are the top ten alternative social networking platforms available? To the best of your knowledge, how many monthly active users does each attract?**

In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if you want to share a photo or video, you can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if you are looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services your mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon, or Snapchat. Facebook represents a small part (in fact, just 6%) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

Last week, legislation that I supported to combat online sex trafficking – the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) – was signed into law. Facebook also supported that legislation.

- **What has Facebook observed in terms of efforts to facilitate human trafficking on its platform, and what actions has Facebook taken in response?**

Sex trafficking has no place on Facebook. Our Community Standards make it very clear that human trafficking and smuggling are against our policies. This is true across the platform. We remove content that threatens or promotes sexual violence, assault, or exploitation, including

against minors, when we become aware of it. We have a team of professional investigators and work with agencies across the world that seek to identify and rescue victims and bring perpetrators to justice.

Facebook is committed to making our platform a safe place, especially for individuals who may be vulnerable. We have a long history of working successfully with governments to address a wide variety of threats to our platform, including child exploitation. When we learn of a situation involving physical abuse, child exploitation, or an imminent threat of harm to a person, we immediately report the situation to first responders or the National Center for Missing and Exploited Children (NCMEC).

Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have a global team that strives to respond within minutes to emergency requests from law enforcement.

Our relationship with NCMEC also extends to an effort that we launched in 2015 to send AMBER Alerts to the Facebook community to help find missing children. When police determine that a case qualifies for an AMBER Alert, the alert is issued by the NCMEC and distributed through the Facebook system with any available information, including a photograph of the missing child, a license plate number, and the names and descriptions of the child and suspected abductor. Law enforcement determines the range of the target area for each alert. We know the chances of finding a missing child increase when more people are on the lookout, especially in the critical first hours. Our goal is to help get these alerts out quickly to the people who are in the best position to help, and a number of missing children have been found through AMBER Alerts on Facebook.

Further, we work tirelessly to identify and report child exploitation images (CEI) to appropriate authorities. We identify CEI through a combination of automated and manual review. On the automated review side, we use image hashing to identify known CEI. On the manual review side, we provide in-depth training to content reviewers on how to identify possible CEI. Confirmed CEI is reported to the NCMEC, which then forwards this information to appropriate authorities. When we report content to the NCMEC, we preserve account information in accordance with applicable law, which can help further law enforcement investigations. We also reach out to law enforcement authorities in serious cases to ensure that our reports are received and acted upon.

Since 2015 we have proactively engaged with relevant NGOs working to safeguard girls and women from trafficking and violence to understand where we can do more. This included a number of roundtables on the topic of women's safety, including trafficking and prostitution. For example:

- **X-Industry Child Safety Hackathon:** In May 2016, we invited over 75 engineers from across industry, including Microsoft and Google, as well as from child safety NGOs, such as NCMEC, Thorn, and InHope, to the Facebook campus in San Francisco for the first-ever cross industry child safety hackathon to develop tools and

products that enhance child online safety (read more at https://www.wearethorn.org/blog/hackathon-creates-tech-solutions-child-safety/?utm_campaign=coschedule&utm_source=facebook_page&utm_medium=Thorn&utm_content=Hackathon%20Creates%20Tech%20Solutions%20for%20Child%20Safety). We again hosted the hackathon in 2017 and have now added the TechCoalition and Google as co-hosts to the event to expand its scope and reach. One of the prototypes that came out of the hackathon is a tool that enables people to match known photos of missing children against online trafficking ads.

- **Roundtable with leading organizations to share best practices and build network.** On October 24, 2017, we hosted our first anti-sex trafficking roundtable in Menlo Park. The roundtable was attended by representatives from law enforcement officials, government agencies and anti-trafficking non-governmental organizations. The focus of the roundtable was to allow participants to discuss and share expertise, experience, and research. The Sex Trafficking Cross-functional Team will continue to collaborate with both our internal and external partners on the objectives, projects, and deliverables discussed at the roundtable.

We have created shortcuts on Facebook and Instagram to provide education and additional resources (developed in conjunction with the National Human Trafficking Resource Center) to people who search for terms related to sex trafficking. These terms have been provided by internal and external experts and when someone searches for them on Facebook, we will have a pop-up that reminds them sex trafficking is illegal and violates our policies and shares resources for getting help.

Questions from Senator Leahy

1. **At the April 10, 2018 hearing, regarding Facebook's role in facilitating dangerous hate speech against Rohingya refugees from Myanmar, I asked: "How can you dedicate, and will you dedicate, resources to make sure such hate speech is taken down within 24 hours?"**

   You replied, "Yes. We're working on this."[7] I appreciate your commitment, in the context of Myanmar, to dedicate resources to take down hate speech within 24 hours. As you know, hours can save lives.

   a. **When will Facebook be able to fully implement your commitment to a 24-hour review time for Myanmar?**

      i. **Will Facebook commit to providing relevant data so that outside researchers can evaluate Facebook's performance metrics on this matter?**

   b. **Will you extend this same commitment to dedicating the resources necessary to achieve a 24-hour review time for hate speech in all other regions of the world in which Facebook is active?**

Reports are reviewed 24 hours a day, 7 days a week, and the vast majority of reports are reviewed within 24 hours. Where there are credible threats of violence we aim to respond much faster, and have significantly reduced our response time in Myanmar.

To support these efforts, we are investing in people, technology, and programs.

Over the last two years, we have added dozens more Burmese language reviewers to handle reports from users across our services, and we plan to more than double the number of content reviewers focused on user reports. We also have increased the number of people across the company working on Myanmar-related issues and we have a special product team working to better understand the local challenges and build the right tools to help keep people in the country safe. We will continue to hire more staff dedicated to Myanmar, including Burmese speakers and policy experts.

From a programmatic perspective, we will continue to work with experts to develop safety resources and counter-speech campaigns in these regions and conduct regular training for civil society and community groups on using our tools.

2. **At the hearing, I showed you an example of a Facebook post targeting a Muslim journalist in Myanmar. Although comments to the incendiary post called for the death of this journalist, upon an initial review the post was deemed not to breach Facebook's Community Standards.**

[7] Transcript of April 10, 2018 hearing, at https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate- hearing/?utm_term=.5789208de46b.

a. **Why was this post deemed not to breach Facebook's Community Standards?**

b. **Please describe what processes and systems you have in place to proactively identify content that breaches Facebook's Community Standards.**

c. **What emergency processes do you have in place for situations where there is content inciting people to violence, and that content has been reported by users and deemed not to breach your Community Standards?**

d. **Please describe any additional processes that you intend to put in place to address this problem in the future.**

We are unable to respond without further information on these Pages.

However, we can say that our Community Standards strictly prohibit credible threats of violence. We assess credibility based upon the information available to us and generally consider statements credible if the following are present:

- A target (person, group of people, or place) and:
    - Bounty/demand for payment, or
    - Mention or image of specific weapon, or
    - Sales offer or ask to purchase weapon, or
    - Spelled-out address or named building, or
- A target and two or more of the following details (can be two of the same detail):
    - Location
    - Timing
    - Method

In evaluating content, context is extremely important. A post itself may be benign, but the comments associated with the post may amount to credible threats of violence. That's why people can report posts, Pages, and Groups to us, as well as individual comments.

The other way we can identify and remove violating content from Facebook is by proactively finding it using technology. Advances in technology, including in artificial intelligence, machine learning, and computer vision, mean that we can now:

- **Remove bad content faster** because we don't always have to wait for it to be reported.

- **Get to more content** because we don't have to wait for someone else to find it.

- **Increase the capacity of our review team**, which includes more than 7,500 people around the world, to work on cases where human expertise is needed to understand the context or nuance of a particular situation.

3. **At the hearing, you stated that Facebook is hiring "dozens more" Burmese language content reviewers. There appear to be only three Burmese content reviewer vacancies currently listed on the Facebook careers page, all in Facebook's Dublin office.[8]**

    a. **How many Myanmar (Burmese) content reviewers does Facebook currently have, and how many does Facebook expect to have on staff by the end of 2018? Please use Full Time Equivalent (FTE) numbers.**

    b. **How does Facebook staff its Burmese language content reviewers to ensure the capacity to promptly review content outside of normal Dublin working hours, including during daytime and on weekends in the Myanmar time zone? How many Burmese language content reviewers do you have based in Southeast Asia?**

    c. **Facebook reportedly has approximately 1,200 German language content reviewers, in part to help ensure that hate speech is removed within 24 hours. How are "dozens" of Burmese content reviewers going to be sufficient to remove all Burmese language hate speech within 24 hours?**

To provide 24/7 coverage across dozens of languages and time zones and ensure that Facebook is a place where both expression and personal safety are protected and respected, our content review teams are made up of a combination of full-time employees, contractors, and vendor partners based in locations around the world.

Our content review team has included Burmese language reviewers since 2013, and we have increased this number over time as we continue to grow and invest in Myanmar. Our goal is always to have the right number of people with the native language capabilities to ensure incoming reports are reviewed quickly and effectively.

Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours. Where there are credible threats of violence we aim to respond much faster, and have significantly reduced our response time in Myanmar.

[8] *See* https://www.facebook.com/careers/.

That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are exploring the use of artificial intelligence to proactively identify this content so that we can find it and review it faster.

4. **Facebook has long stated its desire to re-enter the market in China.[9] As we have seen with other technology platforms, however, there is a cost to doing business in China, including potentially enabling the Chinese government's sophisticated censorship and surveillance regimes. I expressed these concerns to Apple in a letter with Senator Cruz last year.[10]**

    a. **In order to operate in China, internet companies must generally comply with Chinese laws and regulations on censorship.[11] This includes a requirement to remove content relating to a list of vaguely-defined prohibited topics such as "disrupting social order and stability" or "damaging state honor and interests."[12] Given the vagueness surrounding which precise words and terms are prohibited in China, how would Facebook decide what specific content to censor in China? And if a China-based user travels outside of China, will those censorship controls still apply to that user's account?**

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 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.

    b. **According to *The New York Times*, Facebook developed "software to suppress posts from appearing in people's news feeds in specific geographic areas," in order to "help Facebook get into China."[13] If true, then what procedures did such software assume would be used to identify specific content to censor, given the vagueness surrounding prohibited topics under Chinese law?**

---

[9] *See, e.g.,* Answers to Questions for the Record by Colin Stretch, submitted to the Subcommittee on Crime and Terrorism, Oct. 31, 2017, at https://www.judiciary.senate.gov/download/stretch-responses-to-questions-for-the-record.

[10] *See* https://www.cruz.senate.gov/files/documents/Letters/20171017_tim_cook_letter.pdf.

[11] "China Has Launched Another Crackdown on the Internet—but it's Different This Time", CNBC, Oct. 26, 2017, at https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html. *See also*, "Media Censorship in China," COUNCIL ON FOREIGN RELATIONS, at https://www.cfr.org/backgrounder/media-censorship-china.

[12] *See* https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/.

[13] "Facebook Said to Create Censorship Tool to Get Back Into China," THE NEW YORK TIMES, Nov. 22, 2016, at https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html.

See Response to Question 4a.

c. **Under domestic Chinese law, peaceful acts of free expression may be considered illegal. For example, the Chinese government has described the late Nobel Peace laureate Liu Xiaobo as "a criminal who has been sentenced by Chinese judicial departments for violating Chinese law."[14] The case of Tashi Wangchuk indicates that simply promoting the Tibetan language can be deemed illegally "inciting separatism."[15] If Facebook re-enters the Chinese market, what would it do if Chinese authorities serve it with a legal demand, properly issued under domestic Chinese law, asking Facebook to turn over the account information of a peaceful political or religious dissident in China?**

When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs. 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 were we permitted to offer our service to Chinese users. Wherever we operate our service, Facebook is committed to meeting human rights' standards and to providing transparency around any government requests for data. This information is available here: https://transparency.facebook.com/content-restrictions. Our Transparency Report contains data on restrictions we place on content that does not violate community standards but that is alleged to violate local law. We do not have any such reports for the United States.

5. **On April 9, 2018, a group of Vietnamese activists and journalists wrote to you to ask whether Facebook was "coordinating with a government known for cracking down on expression."[16]**

   a. **What safeguards does Facebook have in place to ensure that account suspension and content takedown are not abused by governments – including in conjunction with state-sponsored "trolls"—to silence legitimate criticism?**

As a GNI member, Facebook is committed to privacy and free expression principles and implementation guidelines regarding government requests. The GNI standards have been shaped by international human rights laws and norms and developed through a robust multi-stakeholder and consultative process.

---

[14] "Nobel Peace Prize Given to Jailed Chinese Dissident," THE NEW YORK TIMES, Oct. 8, 2010, at https://www.nytimes.com/2010/10/09/world/09nobel.html?pagewanted=all.

[15] "China to Try Tibetan Education Advocate Detained for 2 Years," THE NEW YORK TIMES, Dec. 30, 2017, at https://www.nytimes.com/2017/12/30/world/asia/tashi-wangchuck-trial-tibet.html.

[16] *See* http://viettan.org/en/open-letter-to-facebook/. See also, "Vietnam Activists Question Facebook on Suppressing Dissent," REUTERS, April 10, 2018, at https://www.reuters.com/article/us-facebook-privacy-vietnam/vietnam-activists-question-facebook-on-suppressing-dissent-idUSKBN1HH0DO.

b. **What <u>more</u> can and will Facebook do in this regard, including but not limited to providing more transparency and more accessible appeal mechanisms on takedown decisions?**

On April 24, 2018, we published the internal guidelines we use to enforce our Community Standards. We decided to publish these internal guidelines for two reasons. First, the guidelines will help people understand where we draw the line on nuanced issues. Second, providing these details makes it easier for everyone, including experts in different fields, to give us feedback so that we can improve the guidelines—and the decisions we make—over time.

We know we need to do more. That's why, over the coming year, we are going to build out the ability for people to appeal our decisions. As a first step, we are launching appeals for posts that were removed for nudity/sexual activity, hate speech or graphic violence.

Here's how it works:

- If a user's photo, video, or post has been removed because we found that it violates our Community Standards, they will be notified, and given the option to request additional review.

- This will lead to a review by our team (always by a person), typically within 24 hours.

- If we've made a mistake, we will notify the user and their post, photo or video will be restored.

We are working to extend this process further, by supporting review of more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up. We believe giving people a voice in the process is another essential component of building a fair system.

6. **Like so many other companies, Facebook has made promises before to do better on privacy, including in its consent decree with the FTC. But the American people want accountability, not promises. That is why I introduced my Consumer Privacy Protection Act, which would create standards and require prompt notification when a breach occurs. It is important to note that we only know about the Cambridge Analytica breach because of a whistleblower.**

    a. **Facebook did not notify the 87 million users when it learned of this breach in 2015, but you are doing so now. You have now said that Facebook's failure to notify 87 million users that their information had been compromised in the Cambridge Analytica breach was a "mistake." Would you support legislation requiring prompt notification of data**

breaches (with appropriate temporary exceptions for ongoing investigations, law enforcement, and national security)?

b. **Why did Facebook not verify that Cambridge Analytica actually deleted the data—especially in 2016 when it was known they were working for the Trump campaign?**

Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, it took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer obtain access to most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

7. **In a recent interview, Dr. Aleksandr Kogan described an extensive relationship with Facebook, stating that "I visited their campus many times. They had hired my students. I even did a consulting project with Facebook in November of 2015." According to *60 Minutes*, Facebook confirmed that Kogan had done research and consulting with the company in 2013 and 2015.[17] Please detail Facebook's relationship with Dr. Kogan, including any consulting and research he did for the company. Please describe what, if any, access to user data Dr. Kogan and his company was provided as part of this consulting agreement.**

Facebook was put in touch with Kogan (a researcher at the University of Cambridge) in late 2012, about a possible collaboration on research relating to the potential relationship between Facebook friendship ties and economic trade volumes between countries. Kogan collaborated with current and former Facebook employees on approximately ten academic papers. As part of these collaborations, Kogan could only access fully anonymized, aggregated data. Facebook frequently partners with leading academic researchers to address topics pertaining to wellbeing, innovation, and other topics of public importance, following strict protocols to ensure personal information is safeguarded.

[17] *See* https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/.

In October 2015, Facebook retained Kogan on a short-term contract to consult on a research project related to predicting survey outcomes.

8. **In 2010, media reports revealed that that an online tracking company, RapLeaf, was collecting and reselling data it had obtained from third-party Facebook apps. Facebook subsequently reportedly cut off RapLeaf's data access and took steps to limit apps' sharing of data with the company.[18]**

    a. **Please describe what steps, if any, Facebook took to require RapLeaf to delete the Facebook user data it had obtained, and the subsequent steps Facebook took to ensure that the information was in fact deleted. If Facebook did not act to ensure that RapLeaf deleted this data, please describe why.**

    b. **Please describe what steps, if any, Facebook took with respect to any third party apps that had sold or shared Facebook user data with RapLeaf.**

Facebook disabled all RapLeaf domains and instituted six-month moratoriums on access to Facebook distribution channels for the developers who shared data. RapLeaf agreed to delete all Facebook IDs in its possession, immediately terminate all agreements with Facebook developers, and no longer conduct any activity on the Facebook platform, whether directly or indirectly. Facebook updated its terms of service to explicitly prohibit developers from interacting with any data brokers.

9. **At the hearing, you stated "every single time they choose to share something, there [on Facebook]—they have a control right there about who they want to share it with."[19] If a user sets these privacy controls to limit their information to a specific audience (*e.g.* their "friends"), should that user expect that no other parties – including Facebook's advertising algorithms – will be able to view or use that information? Should this expectation extend to the trail of information that the user generates by interacting with the service (e.g. "likes" and other reactions, IP logins, geolocation, and operating system usage)?**

Our goal is to show people information on Facebook that's relevant and useful to them. To do this, we personalize people's news feeds and other information, including ads, that we show them based on the information that they've added to their Facebook accounts, like the things they like or comment on.

People can control how this works through their News Feed Settings and Ad Preferences, and they can also choose who can see the information that they choose to share on Facebook. With regard to advertisers specifically, though, we do not tell advertisers who

[18] *See, e.g.*, http://www.adweek.com/digital/facebook-shuts-down-apps-that-sold-user- data-bans-rapleaf/ and https://www.wsj.com/articles/SB10001424052702304772804575558484075236968.
[19] Transcript of April 10, 2018 hearing, at https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.5789208de46b.

people are or sell their information to anyone. We think relevant advertising and privacy aren't in conflict, and we're committed to doing both well.

10. **Beyond information provided directly in response to valid legal process in individual criminal matters, does Facebook provide any information about users to, or cooperate in any way with, Federal, State, or local agencies or authorities – or companies working on their behalf—in a way that would allow for user profiling and/or predictive analytics?**

Facebook is not familiar with government agencies' practices regarding profiling and/or predictive analytics and therefore cannot speculate what would "allow for" such agencies to use such techniques. Facebook discloses account records to Federal, State, or local agencies and authorities only in accordance with our terms of service and applicable law. Additionally, we prohibit developers from using data obtained from us to provide tools that are used for surveillance.

11. **One critique of social media in general is that the most sensational or provocative material often tends to spread the fastest, due to algorithms that prioritize "engagement." This can contribute to a deepening polarization of society. What is Facebook doing with regards to its algorithms, if anything, to address this problem? And what role to you see for outside auditing, verification, or checks of these solutions, given the impact on society?**

Facebook is a distribution platform that reflects the conversations, including polarized ones, already taking place in society. We are keenly aware of the concern that our platform is contributing to polarization, and we have been working to understand the role that we play in discourse and information diversity. The data on what causes polarization and "filter bubbles" is mixed. Some independent research has shown that social media platforms provide more information diversity than traditional media, and our own research indicates that most people on Facebook have at least some friends who claim an opposing political ideology—probably because Facebook helps people to maintain ties with people who are more distantly connected to them than their core community—and that the content in News Feed reflects that added diversity.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

12. **Some people have claimed that what Cambridge Analytica did was no different than the Obama campaign's data-driven campaign in 2012.**

    a. **Yes or no, did the Obama campaign in 2012 violate any of Facebook's policies, and thereby get banned from the platform?**

Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook.

b. **Yes or no, did Cambridge Analytica violate multiple policies—including misleading users and Facebook, and improperly exploiting user data – and thereby get banned from your platform?**

By passing information on to a third party, including SCL/Cambridge Analytica and Christopher Wylie of Eunoia Technologies, Kogan violated our platform policies. When we learned of this violation in 2015, we removed his app from Facebook and demanded certifications from Kogan and all parties he had given data to that the information had been destroyed. Cambridge Analytica, Kogan, and Wylie all certified to us that they destroyed the data. In March 2018, we received reports that, contrary to the certifications we were given, not all data was deleted. We are moving aggressively to determine the accuracy of these claims. If true, this is another unacceptable violation of trust and the commitments they made. We have suspended SCL/Cambridge Analytica, Wylie, and Kogan from Facebook, pending further information.

Questions from Senator Whitehouse

1. **Your written testimony referenced a number of policies Facebook has planned or implemented to prevent foreign nationals from using the platform to interfere in political and electoral processes.**

    a. **How will you ensure that the companies advertising on Facebook are who they purport and claim to be, rather than fronts for otherwise prohibited users?**

    b. **Do shell corporations impede your company's progress in preventing abuse of your platform by foreign agents? If so, how?**

    c. **Would incorporation transparency laws requiring the disclosure of beneficial ownership information at the time of incorporation enhance your ability to overcome those impediments?**

We announced that only authorized advertisers will be able to run electoral ads on Facebook or Instagram. And we're also extending that requirement to anyone that wants to show "issue ads"—like political topics that are being debated across the country. We are working with third parties to develop a list of key issues, which we will refine over time. To get authorized by Facebook, advertisers will need to confirm their identity and location. Advertisers will be prohibited from running political ads—electoral or issue-based—until they are authorized.

Further, we have processes designed to identify inauthentic and suspicious activity and we also maintain a sanctions compliance program to screen advertisers and paid app developers. Facebook's denied party screening protocol involves checking paid app developers and advertisers against applicable denied party listings. Those screened remain in an on-going monitoring portfolio and are screened against changes to applicable denied party listings. Moreover, our payments subsidiaries file Suspicious Activity Reports on developers of certain apps as appropriate.

However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer. In addition, the general challenge of attributing online activities to specific governments or organizations is widely recognized in the intelligence and law enforcement communities.

It is possible that such laws could help companies gain insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer.

2. **With respect to the exchange below, is there anything you would like to add to your statements about the process whereby Facebook required Cambridge Analytica to certify that it had deleted all improperly acquired data? Can you confirm that Facebook entered into a legally binding contract with Cambridge Analytica surrounding the deletion of unlawfully obtained user data? Would you**

be willing to share a copy of the contract in question with the Senate Committees before which you appeared, if so?

WHITEHOUSE:

And with respect to Cambridge Analytica, your testimony is that first you required them to formally certify that they had deleted all improperly acquired data. Where did that formal certification take place? That sounds kind of like a quasi-official thing, to formally certify. What did that entail?

ZUCKERBERG:

Senator, first they sent us an e-mail notice from their chief data officer telling us that they didn't have any of the data any more, that they deleted it and weren't using it. And then later we followed up with, I believe, a full legal contract where they certified that they had deleted the data.

WHITEHOUSE:

In a legal contract?

ZUCKERBERG:

Yes, I believe so.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. If this occurred, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker, or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed and provided to Facebook signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified

that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017. Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

3. Until 2014, Facebook allowed "friend permission," which meant that if one of your Facebook friends connected an authorized app to his Facebook account, the app could access not only that person's personal information, but also your personal information -- and all of his other friends' personal information -- regardless of his friends' privacy settings. Facebook rightly changed that permission in 2014.

a. **Do you have an estimate as to how many third party entities were authorized to collect friends' data while "friend permission" was in effect?**

b. Do you know what happened to that data and whether it was shared further?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

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 suspensions include apps that 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.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

c. How does Facebook audit third party applications to ensure that they are who they say they are?

In general, on an ongoing basis, we proactively review all apps seeking access to more than basic information (and have rejected more than half of apps seeking such extended permissions). We also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for people. These include steps such as random checks of existing apps along with the regular and proactive monitoring of apps. We also respond to external or internal reports and investigate for potential app violations. 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.

d. Do users have a way of tracking what data about them was shared with third parties, including when this data is shared by their friends? Should they?

With respect to our investigation into apps that had access to large amounts of information, if we find evidence that these or other apps did misuse data, we will ban them and notify people whose data was shared with these apps.

4. **Aleksander Kogan purported to be a researcher when he came to Facebook with the app Thisisyourdigitallife. He then funneled the information he collected about Facebook's users to Cambridge Analytica, which planned to use that information to influence Facebook users' political opinions. How was Dr. Kogan vetted? What policies and procedures does Facebook follow to ensure that researchers are who they say they are and that their research is legitimate?**

Facebook was put in touch with Kogan (a researcher at the University of Cambridge) in late 2012, about a possible collaboration on research relating to the potential relationship between Facebook friendship ties and economic trade volumes between countries. Kogan collaborated with current and former Facebook employees on approximately ten academic papers. As part of these collaborations, Kogan could only access fully anonymized, aggregated data from Facebook. Facebook frequently partners with leading academic researchers to address

topics pertaining to wellbeing, innovation, and other topics of public importance, following strict protocols to ensure personal information is safeguarded.

5. **The General Data Protection Regulation (GDPR) goes into effect in Europe in May. It will require that users be afforded meaningful opportunities for informed consent and the ability to opt-out of direct marketing. It will also require data portability and give users the right to access their personal data. Finally, it will mandate privacy by design and require that users be informed within 72 hours of a data breach. What is Facebook doing in Europe to get ready to comply with GDPR?**

The GDPR requires companies to obtain explicit consent to process certain kinds of data ("special categories of data" like biometric data). We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

We are also upgrading our tools for access, rectification, erasure, data portability, and others to people in the US and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

Many of the requirements under GDPR previously applied to Facebook Ireland under the Data Protection Directive, and we have therefore been following these principles for many years. The GDPR is founded on core principles of transparency and control, which are also central values we employ in designing our products.

6. **You've made headlines recently by saying that Facebook will not apply all of GDPR in the United States. Which GDPR requirements is Facebook choosing not to apply in the U.S.? Why? What parts of GDPR do you think the US should import?**

The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability and others to people in the US and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

7. **Facebook has announced that it will begin placing ads into a searchable database, which will include details about how much the ads cost and what kinds of people the advertisers were targeting. Ads will stay in the database for four years. Will the database include information on the audience that advertisers were *trying* to target or just the demographic information about which users were ultimately reached?**

The database will include demographic information (e.g., age, general location, gender) about the audience that the ads reached.

8. **As Chair of the Cybersecurity Task Force and a Co-Chair of the International Creativity and Theft-Prevention Caucus, I have focused time and attention on the issue of platform security and responsibility—including as it relates to intellectual property theft. What steps is Facebook taking to ensure that it provides a safe and secure platform in this respect? Will you devote the resources necessary to ensure that your platform and its features/tools, including Facebook Live, are used in a responsible and legal fashion?**

We take intellectual property rights seriously at Facebook and work closely with the motion picture industries and other rights holders worldwide to help them protect their copyrights and other IP. Our measures target potential piracy across our products, including Facebook Live, and continue to be enhanced and expanded. These include a global notice-and-takedown program, a comprehensive repeat infringer policy, integration with the content recognition service Audible Magic, and our proprietary video- and audio-matching technology called Rights Manager. More information about these measures can be found in our Intellectual Property Help Center, Transparency Report, and Rights Manager website.

9. **Your Q3 earnings disclosure in 2017 indicated that over 270 million Facebook accounts are fake or duplicate accounts. Fake and imposter accounts have been identified as central to the disinformation campaigns threatening democracies, and you have responded by banning tens of thousands of these accounts to protect elections in France, Germany, and Alabama. Do you intend to enforce your user policy and track and delete as many fake and imposter accounts on your site as possible and, if so, on what timeline? Are there circumstances under which Facebook would track, but opt not to delete, inauthentic accounts that may be involved in disinformation campaigns? What would such circumstances be?**

We are committed to finding and removing fake accounts. We continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection. When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

10. (a) How does Facebook define fake news?

(b) How does the company distinguish real news stories from fake ones, if at all?

(c) What mechanisms, if any, does Facebook use to prevent news stories identified as fake from appearing on users' news feeds?

(d) Does Facebook keep track of users who exhibit a pattern of sharing fake news stories? Does it suspend users who exhibit such a pattern? If not, would Facebook consider implementing a policy that disciplines users who spread fake news? What else could Facebook do to stop the spread of fake news?

At Facebook, we define false news as "[n]ews articles that purport to be factual, but which contain intentional misstatements of fact with the intention to arouse passions, attract viewership, or deceive."

We believe that tech companies, media companies, newsrooms, and educators all need to work together to address this societal problem. We are engaged with partners across these industries to help create a more informed community.

We are working to build a more informed community by promoting trustworthy, informative, and local news and by focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching

the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives**. When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products**. We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding. Among the products we've launched is:

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

11. It is my understanding that Facebook currently restricts notifications related to fake news to users who seek to share the content in question. In other words, before sharing a story flagged as fake on the site, a user will receive a warning that the story's accuracy has been "disputed." Does Facebook intend to expand the existing policy and begin notifying individual users each time they view (not just share) fake content? If not, why not?

As we announced in December 2017, we will no longer use Disputed Flags to identify false news. Instead, we will use Related Articles to help give people more context about the story. Academic research on correcting misinformation has shown that putting a strong image, like a red flag, next to an article may actually entrench deeply held beliefs—the opposite effect

to what we intended. Related Articles, by contrast, are simply designed to give more context, which our research has shown is a more effective way to help people get to the facts. Indeed, we have found that when we show Related Articles next to a false news story, it leads to fewer shares than when the Disputed Flag is shown.

We are giving people more context about the information they see on Facebook with Article Context. Since we launched this test, some of the articles you see in News Feed will feature an "i" icon that allows you to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

We continue to look for opportunities to improve this experience and help give people more context so that they can decide what to read, trust, and share on Facebook.

Senate Committee on the Judiciary

Hearing Follow-up Questions

Senator Durbin

They certainly know within the Facebook pages who their friends are, but they may not know, as has happened, and you've conceded this point in the past, that sometimes that information is going way beyond their friends and sometimes people have made money off of sharing that information, correct?

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 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 announced expansions to Download Your Information, which, among other things, will make it easier for 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, delete 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.

Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at https://www.facebook.com/help/218345114850283?helpref=about_content.

The categories of information that an app can access are clearly disclosed before the user consents to use an app on the Facebook Platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

Illinois has a biometric information privacy act, our state does, which is to regulate the commercial use of facial, voice, finger and iris scans and the like. We're now in a fulsome

debate on that and Facebook has come down on a position trying to carve out exceptions and I hope you'll fill me in on how that is consistent with protecting privacy.

We are aware of several pending measures to amend the Illinois Biometric Information Privacy Act to foster the use of technology to enhance privacy and data security and combat threats like fraud, identity theft, and impersonation. Facebook has not supported these measures or requested any organization or chamber of commerce to do so.

In 2016, Senator Terry Link, the author of the Illinois Biometric Information Privacy Act, introduced a measure (HB 6074) clarifying that the original law (1) does not apply to information derived from physical or digital photographs and (2) uses the term "scan" to mean information that is obtained from an in-person process. These clarifying amendments were consistent with industry's longstanding interpretation of the law and Facebook publicly supported them.

Facebook's advocacy is consistent with our commitment to protecting privacy. As the findings of the Illinois General Assembly confirm, when people raise privacy concerns about facial recognition, they are generally about specific uses of facial recognition. In enacting the Illinois Biometric Information Privacy Act, the General Assembly explained that its concern was "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5.

Facebook's use of facial recognition in our products, on the other hand, is very different. Facebook uses facial-recognition technology with users to provide Facebook users—who choose to join Facebook for the purpose of connecting with and sharing information about themselves with others, and affirmatively agree to Facebook's Terms of Service and Data Policy—with products and features that protect their identities and enhance their online experiences while giving them control over the technology. For example, Facebook uses facial-recognition technology to protect users against impersonators by notifying users when someone else has uploaded a photo of them for use as a profile photo and to enable features on the service to people who are visually impaired. Facebook also uses facial-recognition technology to suggest that people who upload photos or videos tag the people who appear in the photos or videos. When someone is tagged in a photo or video, Facebook automatically notifies that person that he or she has been tagged, which in turn enables that person to take action if he or she does not like the content—such as removing the tag or requesting that the content be removed entirely. Facebook users have always had the ability to change their settings to prevent Facebook from using facial recognition to recognize them.

Given the very different uses of facial-recognition technology that exist, we believe that a one-size-fits-all approach to regulation of facial-recognition technology is not in the public's best interest, and we believe that clarification that the Illinois Biometric Information Privacy Act was not intended to apply to all uses of facial recognition is consistent with Facebook's commitment to protecting privacy. Furthermore, our commitment to support meaningful, thoughtfully drafted privacy legislation means that we can and do oppose measures that create confusion, interfere with legitimate law enforcement action, create unnecessary risk of frivolous litigation, or place undue burdens on people's ability to do business online.

Senator Grassley

Do you know of any instances where user data was improperly transferred to a third party in breach of Facebook's terms? If so, how many times has that happened, and was Facebook only made aware of that transfer by some third party?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker, or other advertising or monetization-related service. We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity.

Have you ever required an audit to ensure the deletion of improperly transferred data? And if so, how many times?

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

Senator Klobuchar

Can you provide a breakdown of users affected by Cambridge Analytica by state?

See the state breakdown here: https://fbnewsroomus.files.wordpress.com/2018/05/state-by-state-breakdown.pdf.

Do you support a rule that would require you to notify your users of a breach within 72 hours?

Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Senator Whitehouse

Does Kogan still have an account?

Kogan's personal accounts have been suspended, as have the personal accounts of some Cambridge Analytica officers.

Senator Cruz

The predicate for Section 230 immunity under the CDA is that you're a neutral public forum. Do you consider yourself a neutral public forum or are you engaged in political speech, which is your right under the First Amendment?

We are, first and foremost, a technology company. Facebook does not create or edit the content that our users published on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

Section 230 of the Communications Decency Act provides that "[N]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Outside of certain specific exceptions, this means that online platforms that host content posted by others are generally not liable for the speech of their users, and, indeed, Section 230 explicitly provides that a platform that chooses to moderate content on its service *based on its own standards* does not incur liability on the basis of that decision. Specifically, 47 U.S.C. § 230(c)(2) provides, in relevant part, that "[N]o provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

Senator Leahy

Six months ago, your general counsel promised us you were taking steps to prevent Facebook from serving what I call unwitting conspiracy Russian interference. But these unverified, divisive pages are on Facebook today. They look a lot like Russian agents used to spread propaganda during the 2016 election. Are you able to confirm whether they are Russian groups, yes or no?

In general, we take aggressive investigative steps to identify and disable groups that conduct coordinated inauthentic activities on the platform, but it is extremely challenging to definitively attribute online activity to particular threat actors. We often rely on information from others, like information from the government, to identify actors behind abuse that we observe and to better understand these issues. We would need more information in order to review the specific Pages referenced at the hearing.

I want to know what you'll do about Chinese censorship when they come to you.

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 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.

When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs.

More information is available here: https://transparency.facebook.com/content-restrictions.

Senator Booker

Would you open the Company to audit companies dealing in credit and housing?

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.

And then for the record, my time has expired, but there's a lawsuit against Facebook about discrimination. You move for it to be dismissed because no harm was shown. Could you please submit to the record, you believe that people of color were not recruited for various economic opportunities or being harmed. Can you please clarify why you move to dismiss that lawsuit for the record?

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running housing ads—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

Senator Feinstein

How many accounts of this type [Russian IRA/fake accounts] have you taken down?

After the 2016 election, we learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that about 470 fake accounts associated with the IRA spent approximately $100,000 on around 3,500 Facebook and Instagram ads between June 2015 and August 2017. Our analysis also showed that these accounts used these ads to promote the roughly 120 Facebook Pages they had set up, which in turn posted more than 80,000 pieces of content between January 2015 and August 2017. More recently, we took down more than 270 Pages and accounts controlled by the IRA that primarily targeted either people living in Russia or Russian speakers around the world, including from countries neighboring Russia.

We are committed to finding and removing fake accounts. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts. We block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection. When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

Senator Blumenthal

I have a number of other specific requests that you agree to support as part of legislation. I think legislation is necessary. The rules of the road have to be the result of congressional action. We have—Facebook has participated recently in the fight against the scourge of sex trafficking and the bill that we've just passed. It will be signed into law tomorrow. The Stop Exploiting Sex Trafficking Act was as a result of our cooperation and I hope we can cooperate on this kind of measure as well.

Facebook supports SESTA, and we were very pleased to be able to work successfully with a bipartisan group of Senators on a bill that protects women and children from the harms of sex trafficking.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Senator Graham

Would you submit to us some proposed regulations?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.