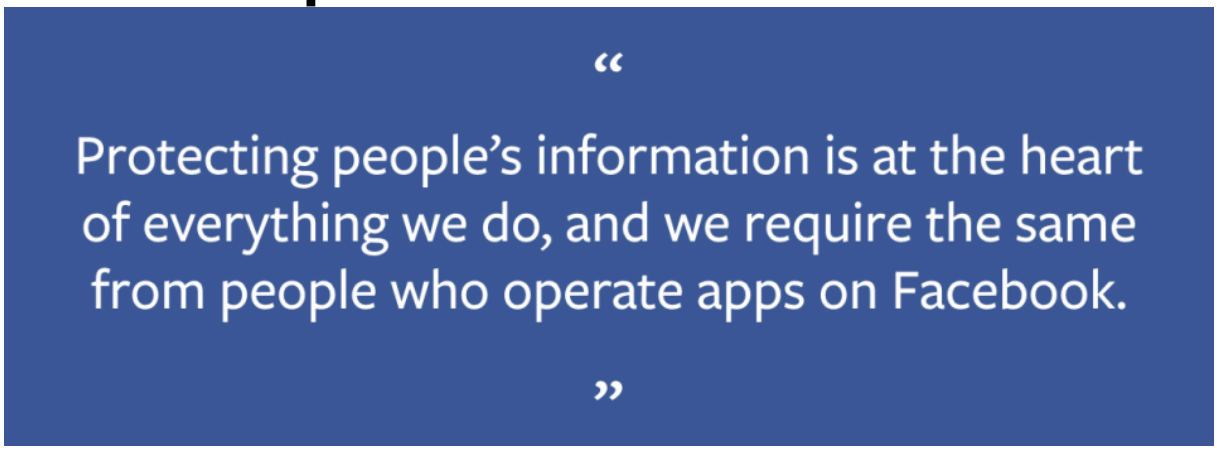
1. Annexes

1. Communiqués de presse 16 mars 2018

March 16, 2018

Suspending Cambridge Analytica and SCL Group From Facebook



By Paul Grewal, VP & Deputy General Counsel!

Update on March 17, 2018, 9:50 AM PT: The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked.

Originally published on March 16, 2018:
We are suspending Strategic Communication Laboratories (SCL), including their political data analytics firm, Cambridge Analytica, from Facebook. Given the public prominence of this organization, we want to take a moment to explain how we came to this decision and why.

We Maintain Strict Standards and Policies
Protecting people’s information is at the heart of everything we do, and we require the same from people who operate apps on Facebook. In 2015, we learned that a psychology professor at the University of Cambridge named Dr. Aleksandr Kogan lied to us and violated our Platform Policies by passing data from an app that was using Facebook Login to SCL/Cambridge Analytica, a firm that does political, government and military work around the globe. He also passed that data to Christopher Wylie of Eunoia Technologies, Inc.
Like all app developers, Kogan requested and gained access to information from people after they chose to download his app. His app, “thisisyourdigitallife,” offered a personality prediction, and billed itself on Facebook as “a research app used by psychologists.” Approximately 270,000 people downloaded the app. In so doing, they gave their consent for Kogan to access information such as the city they set on their

profile, or content they had liked, as well as more limited information about friends who had their privacy settings set to allow it.
Although Kogan gained access to this information in a legitimate way and through the proper channels that governed all developers on Facebook at that time, he did not subsequently abide by our rules. By passing information on to a third party, including SCL/Cambridge Analytica and Christopher Wylie of Eunoia Technologies, he 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.

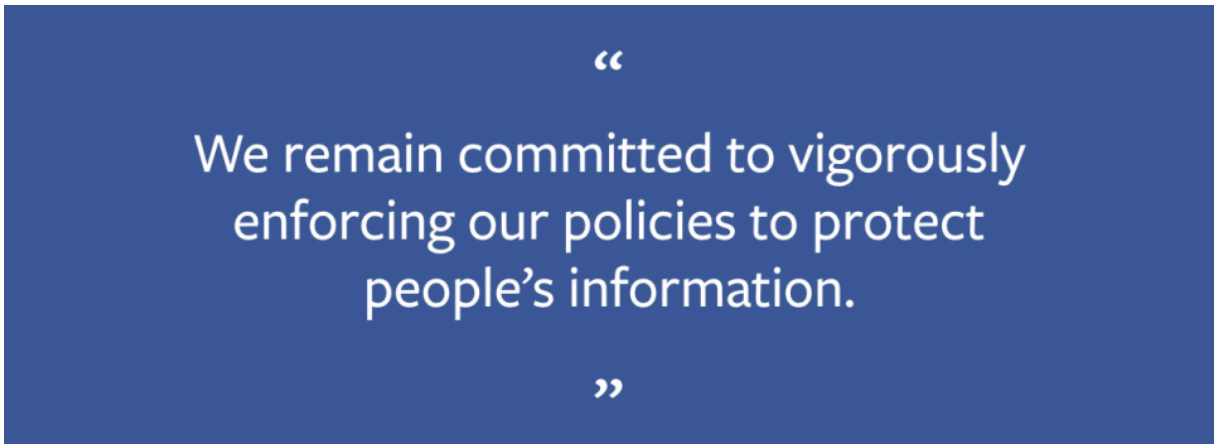
Breaking the Rules Leads to Suspension
Several days ago, we received reports that, contrary to the certifications we were given, not all data was deleted. We are moving aggressively to determine the accuracy of these claims. If true, this is another unacceptable violation of trust and the commitments they made. We are suspending SCL/Cambridge Analytica, Wylie and Kogan from Facebook, pending further information.
We are committed to vigorously enforcing our policies to protect people's information. We will take whatever steps are required to see that this happens. We will take legal action if necessary to hold them responsible and accountable for any unlawful behavior.

How Things Have Changed
We are constantly working to improve the safety and experience of everyone on Facebook. In the past five years, we have made significant improvements in our ability to detect and prevent violations by app developers. Now all apps requesting detailed user information go through our App Review process, which requires developers to justify the data they're looking to collect and how they're going to use it – before they're allowed to even ask people for it.
In 2014, after hearing feedback from the Facebook community, we made an update to ensure that each person decides what information they want to share about themselves, including their friend list. This is just one of the many ways we give people the tools to control their experience. Before you decide to use an app, you can review the permissions the developer is requesting and choose which information to share. You can manage or revoke those permissions at any time.
On an ongoing basis, we also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for users. These include steps such as random audits of existing apps along with the regular and proactive monitoring of the fastest growing apps.
We enforce our policies in a variety of ways — from working with developers to fix the problem, to suspending developers from our platform, to pursuing litigation.

2. **Communiqués de presse 19 mars 2018**

March 19, 2018

Pursuing Forensic Audits to Investigate Cambridge Analytica Claims



Update on March 19, 2018, 3:25 PM PT: Independent forensic auditors from Stroz Friedberg were on site at Cambridge Analytica’s London office this evening. At the request of the UK Information Commissioner’s Office, which has announced it is pursuing a warrant to conduct its own on-site investigation, the Stroz Friedberg auditors stood down.

Originally published March 19, 2018, 11:40 AM PT:
We have hired a digital forensics firm, Stroz Friedberg, to conduct a comprehensive audit of Cambridge Analytica. Cambridge Analytica has agreed to comply and afford the firm complete access to their servers and systems. We have approached the other parties involved — Christopher Wylie and Aleksandr Kogan — and asked them to submit to an audit as well. Mr. Kogan has given his verbal agreement to do so. Mr. Wylie thus far has declined.
This is part of a comprehensive internal and external review that we are conducting to determine the accuracy of the claims that the Facebook data in question still exists. This is data Cambridge Analytica, SCL, Mr. Wylie, and Mr. Kogan certified to Facebook had been destroyed. If this data still exists, it would be a grave violation of Facebook’s policies and an unacceptable violation of trust and the commitments these groups made.
We are moving aggressively to determine the accuracy of these claims. We remain committed to vigorously enforcing our policies to protect people’s information. We also want to be clear that today when developers create apps that ask for certain information from people, we conduct a robust review to identify potential policy violations and to assess whether the app has a legitimate use for the data. We actually reject a significant number of apps through this process. Kogan’s app would not be permitted access to detailed friends’ data today.

3. **Communiqué de presse du 21 mars 2018**

March 21, 2018

Cracking Down on Platform Abuse

Protecting people's information is the most important thing we do at Facebook. What happened with Cambridge Analytica was a breach of Facebook's trust. More importantly, it was a breach of the trust people place in Facebook to protect their data when they share it. As Mark Zuckerberg explained in his post, we are announcing some important steps for the future of our platform. These steps involve taking action on potential past abuse and putting stronger protections in place to prevent future abuse.

People use Facebook to connect with friends and others using all kinds of apps. Facebook's platform helped make apps social — so your calendar could show your friends' birthdays, for instance. To do this, we allowed people to log into apps and share who their friends were and some information about them.

As people used the Facebook platform in new ways, we strengthened the rules. We required that developers get people's permission before they access the data needed to run their apps – for instance, a photo sharing app has to get specific permission from you to access your photos. Over the years we've introduced more guardrails, including in 2014, when we began reviewing apps that request certain data before they could launch, and introducing more granular controls for people to decide what information to share with apps. These actions would prevent any app like Aleksandr Kogan's from being able to access so much data today.

Even with these changes, we've seen abuse of our platform and the misuse of people's data, and we know we need to do more. We have a responsibility to everyone who uses Facebook to make sure their privacy is protected. That's why we're making changes to prevent abuse. We're going to set a higher standard for how developers build on Facebook, what people should expect from them, and, most importantly, from us. We will:

Review our platform. 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. If we find developers that misused personally identifiable information, we will ban them from our platform.

Tell people about data misuse. We will tell people affected by apps that have misused their data. This includes building a way for people to know if their data might

have been accessed via “thisisyourdigitallife.” 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 hasn’t used an app within the last three months, we will turn off the app’s access to their information.

Restrict Facebook Login data. We are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, profile photo and email address. Requesting any other data will require our approval.

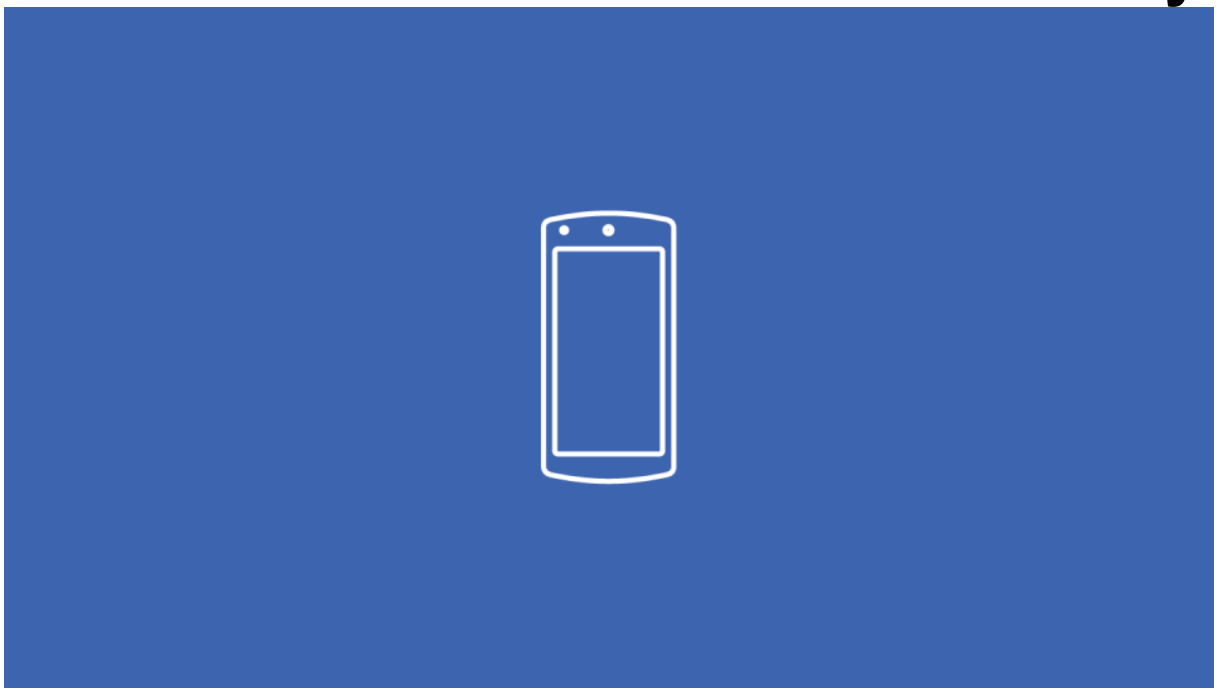
Encourage people to manage the apps they use. We already show people what apps their accounts are connected to and control what data they’ve permitted those apps to use. Going forward, we’re going to make these choices more prominent and easier to manage.

Reward people who find vulnerabilities. In the coming weeks we will expand Facebook’s bug bounty program so that people can also report to us if they find misuses of data by app developers.
There’s more work to do, and we’ll be sharing details in the coming weeks about additional steps we’re taking to put people more in control of their data. Some of these updates were already in the works, and some are related to new data protection laws coming into effect in the EU. This week’s events have accelerated our efforts, and these changes will be the first of many we plan to roll out to protect people’s information and make our platform safer.

4. **Communiqué de presse du 25 mars 2018**

March 25, 2018

Fact Check: Your Call and SMS History



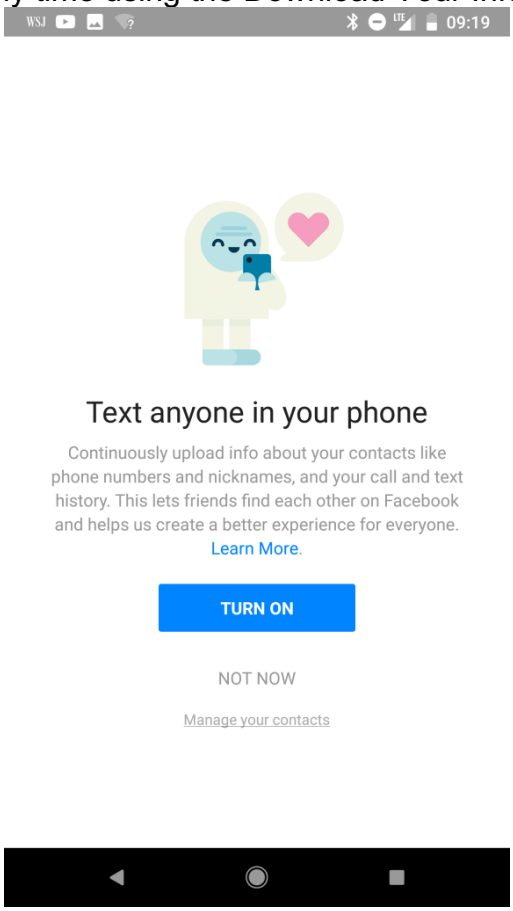
You may have seen some recent reports that Facebook has been logging people's call and SMS (text) history without their permission.
This is not the case.

Opt-in Features in Facebook Lite and Messenger

Call and text history logging is part of an opt-in feature for people using Messenger or Facebook Lite on Android. This helps you find and stay connected with the people you care about, and provides you with a better experience across Facebook. People have to expressly agree to use this feature. If, at any time, they no longer wish to use this feature they can turn it off in settings, or here for Facebook Lite users, and all previously shared call and text history shared via that app is deleted. While we receive certain permissions from Android, uploading this information has always been opt-in only.
We introduced this feature for Android users a couple of years ago. Contact importers are fairly common among social apps and services as a way to more easily find the people you want to connect with. This was first introduced in Messenger in 2015, and later offered as an option in Facebook Lite, a lightweight version of Facebook for Android.

How It Works

When you sign up for Messenger or Facebook Lite on Android, or log into Messenger on an Android device, you are given the option to continuously upload your contacts as well as your call and text history. For Messenger, you can either turn it on, choose 'learn more' or 'not now'. On Facebook Lite, the options are to turn it on or 'skip'. If you chose to turn this feature on, we will begin to continuously log this information, which can be downloaded at any time using the Download Your Information tool.



If, at any point, you no longer wish to continuously upload this information, you can easily turn this feature off in your settings. You can also turn off continuous call and

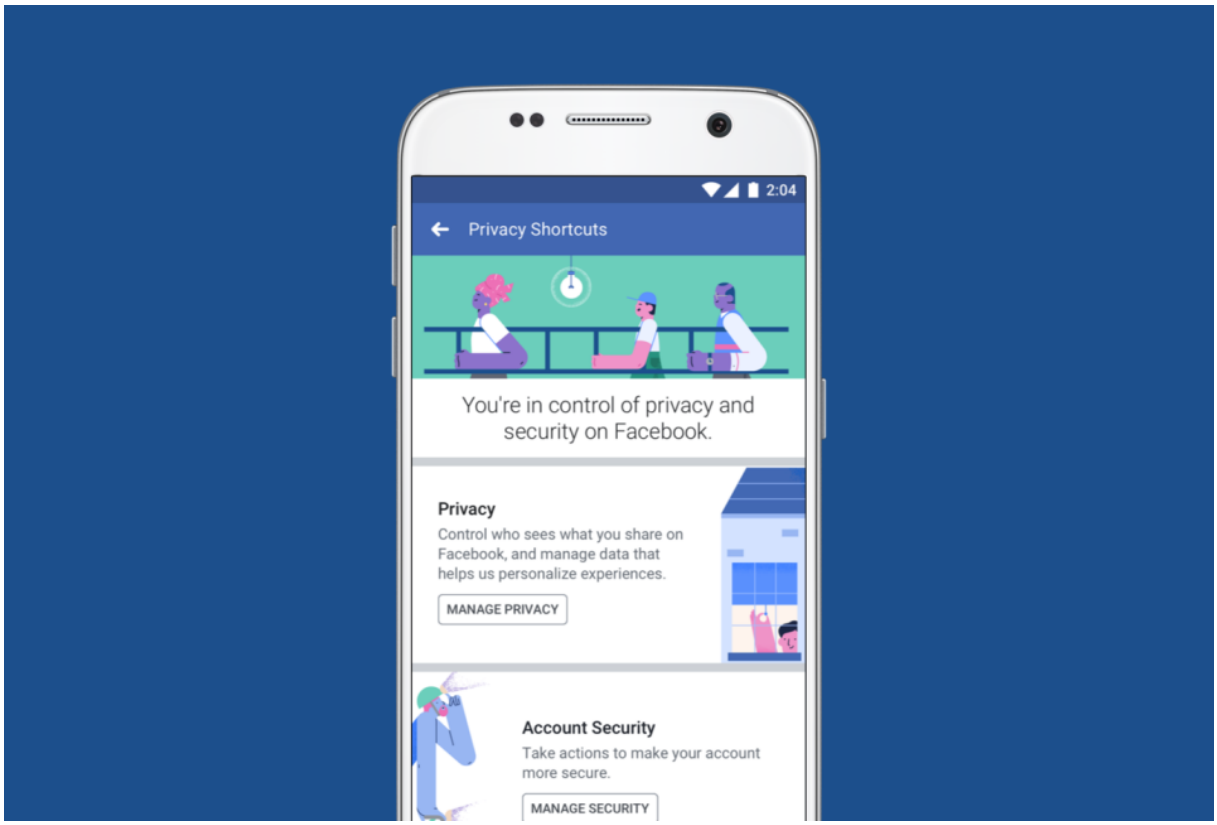
text history logging while keeping contact uploading enabled. You can also go to this page to see which contacts you have uploaded from Messenger, and you can delete all contact information you've uploaded from that app should you choose.

We never sell this data, and this feature does not collect the content of your text messages or calls
When this feature is enabled, uploading your contacts also allows us to use information like when a call or text was made or received. This feature does not collect the content of your calls or text messages. Your information is securely stored and we do not sell this information to third parties. You are always in control of the information you share with Facebook.

5. **Communiqué de presse du 28 mars 2018**

March 28, 2018

It's Time to Make Our Privacy Tools Easier to Find



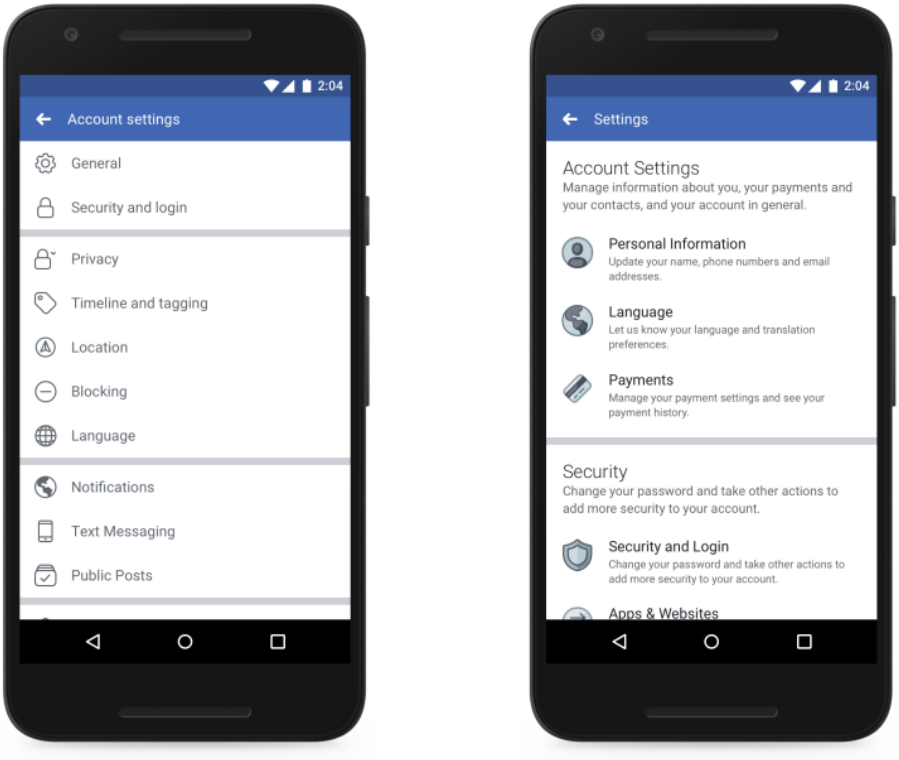
By Erin Egan, VP and Chief Privacy Officer, Policy and Ashlie Beringer, VP and Deputy General Counsel

Last week showed how much more work we need to do to enforce our policies and help people understand how Facebook works and the choices they have over their

data. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So in addition to Mark Zuckerberg's announcements last week – cracking down on abuse of the Facebook platform, strengthening our policies, and making it easier for people to revoke apps' ability to use your data – we're taking additional steps in the coming weeks to put people more in control of their privacy. Most of these updates have been in the works for some time, but the events of the past several days underscore their importance.

Making Data Settings and Tools Easier to Find

Controls that are easier to find and use. We've redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. Instead of having settings spread across nearly 20 different screens, they're now accessible from a single place. We've also cleaned up outdated settings so it's clear what information can and can't be shared with apps.



A comparison of the old settings menu (left) and new settings menu (right).

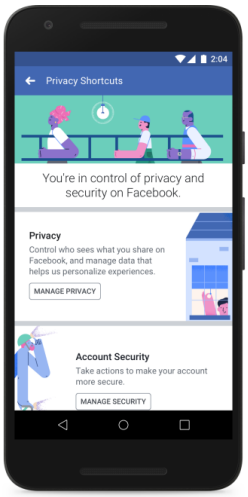
New Privacy Shortcuts menu. People have also told us that information about privacy, security, and ads should be much easier to find. The new Privacy Shortcuts is a menu where you can control your data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. From here you can:

Make your account more secure: You can add more layers of protection to your account, like two-factor authentication. If you turn this on and someone tries to log into your account from a device we don't recognize, you'll be asked to confirm whether it was you.

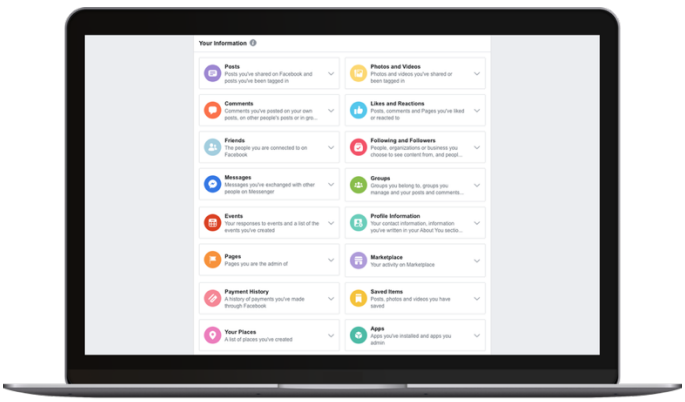
Control your personal information: You can review what you've shared and delete it if you want to. This includes posts you've shared or reacted to, friend requests you've sent, and things you've searched for on Facebook.

Control the ads you see: You can manage the information we use to show you ads. Ad preferences explains how ads work and the options you have.

Manage who sees your posts and profile information: You own what you share on Facebook, and you can manage things like who sees your posts and the information you choose to include on your profile.



Tools to find, download and delete your Facebook data.
It's one thing to have a policy explaining what data we collect and use, but it's even more useful when people see and manage their own information. Some people want to delete things they've shared in the past, while others are just curious about the information Facebook has. So we're introducing 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. You can go here to delete anything from your timeline or profile that you no longer want on Facebook.
We're also making it easier to download the data you've shared with Facebook – it's your data, after all. You can download a secure copy and even move it to another service. This includes photos you've uploaded, contacts you've added to your account, posts on your timeline, and more.



The Road Ahead

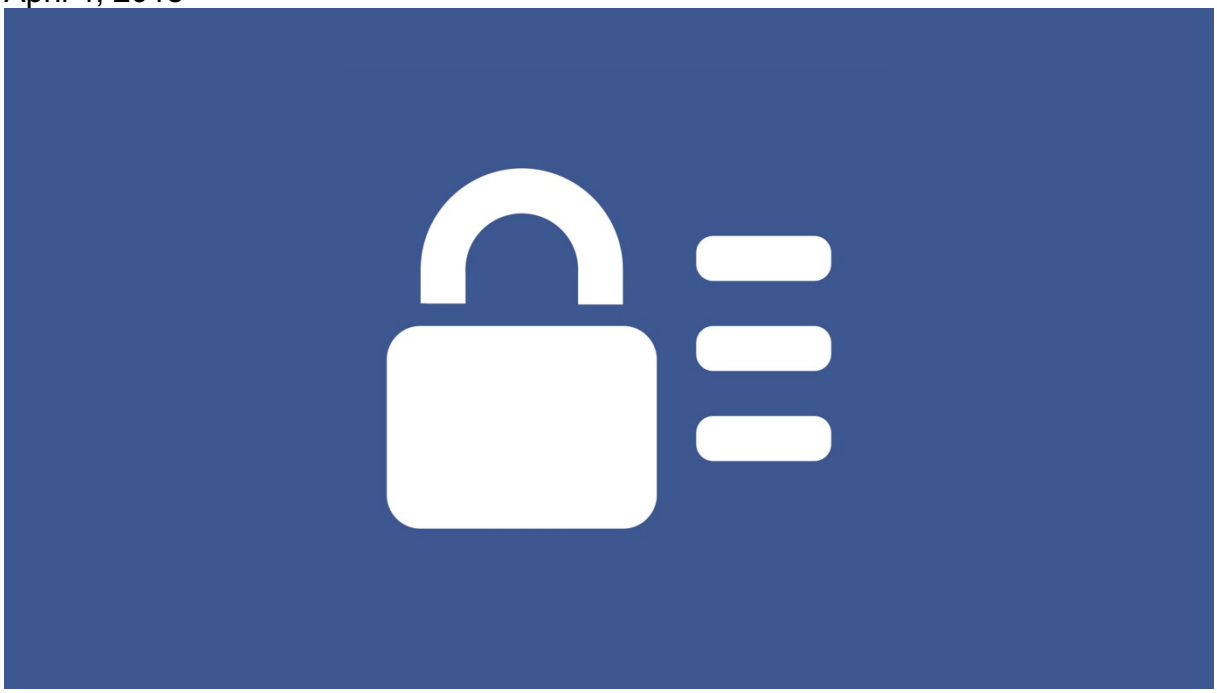
It’s also our responsibility to tell you how we collect and use your data in language that’s detailed, but also easy to understand. In the coming weeks, we’ll be proposing updates to Facebook’s terms of service that include our commitments to people. We’ll also update our data policy to better spell out what data we collect and how we use it. These updates are about transparency – not about gaining new rights to collect, use, or share data.
We’ve worked with regulators, legislators and privacy experts on these tools and updates. We’ll have more to share in the coming weeks, including updates on the measures Mark shared last week.

6. **Communiqués de presse du 04 avril 2018 (1,2 et 3)**

(1)

We’re Making Our Terms and Data Policy Clearer, Without New Rights to Use Your Data on Facebook

April 4, 2018



By Erin Egan, VP and Chief Privacy Officer, Policy and Ashlie Beringer, VP and Deputy General Counsel
It’s important to show people in black and white how our products work – it’s one of the ways people can make informed decisions about their privacy. So we’re proposing updates to our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that’s easier to read. We’re also updating our data policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger and other products.

These updates are about making things clearer.
We're not asking for new rights to collect, use or share your data on Facebook. We're also not changing any of the privacy choices you've made in the past.

Here are a few examples of what you'll find:

New features and tools:
We're providing information on recently introduced features. Since we last updated our terms or data policy three years ago, you can now buy and sell items on Marketplace, start a fundraiser for a cause you care about, share Live and 360 video, and add creative effects to your photos.

Personalized experience:
Everyone's experience on Facebook is unique, and we're providing more information on how this works. We explain how we use data and why it's needed to customize the posts and ads you see, as well as the Groups, friends and Pages we suggest.

What we share:
We will never sell your information to anyone. We have a responsibility to keep people's information safe and secure, and we impose strict restrictions on how our partners can use and disclose data. We explain all of the circumstances where we share information and make our commitments to people more clear.

Advertising:
You have control over the ads you see, and we don't share your information with advertisers. Our data policy explains more about how we decide which ads to show you.

One company:
Facebook is part of the same company as WhatsApp and Oculus, and we explain how we share services, infrastructure and information. We also make clear that Facebook is the corporate entity that provides the Messenger and Instagram services, which now all use the same data policy. Your experience isn't changing with any of these products.

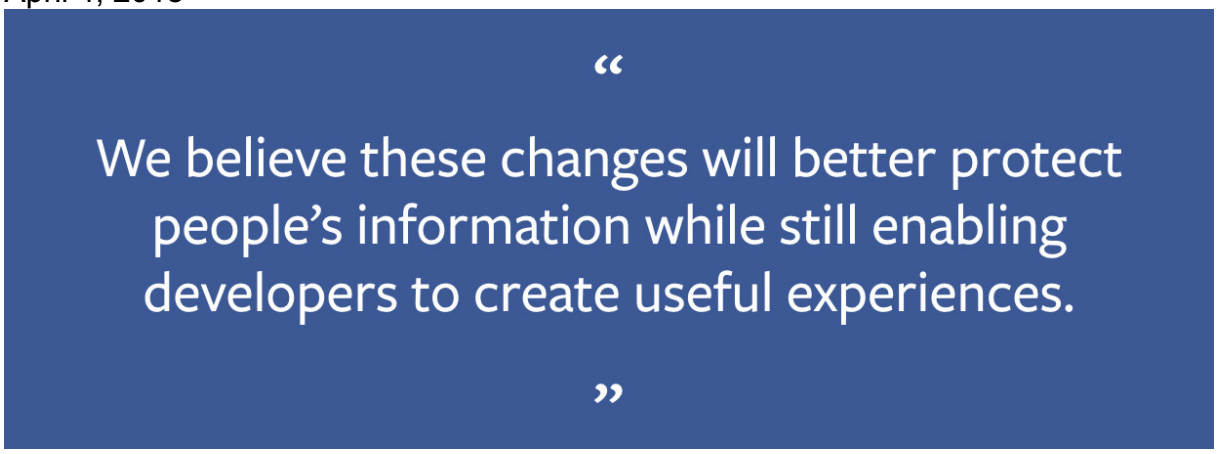
Device information:
People have asked to see all the information we collect from the devices they use and whether we respect the settings on your mobile device (the short answer: we do). We've also added more specific information about the information we collect when you sync your contacts from some of our products, including call and SMS history, which people have recently asked about.

Addressing harmful behavior:
We better explain how we combat abuse and investigate suspicious activity, including by analyzing the content people share.
For the next seven days, you'll be able to provide your feedback on the terms and data policy. Once finalized, we'll publish these documents and ask you to agree to them on Facebook, along with information about the choices you have over your privacy.

(2)

An Update on Our Plans to Restrict Data Access on Facebook

April 4, 2018



By Mike Schroepfer, Chief Technology Officer

Two weeks ago we promised to take a hard look at the information apps can use when you connect them to Facebook as well as other data practices. Today, we want to update you on the changes we’re making to better protect your Facebook information. We expect to make more changes over the coming months — and will keep you updated on our progress. Here are the details of the nine most important changes we are making.

Events API: Until today, people could grant an app permission to get information about events they host or attend, including private events. This made it easy to add Facebook Events to calendar, ticketing or other apps. But Facebook Events have information about other people’s attendance as well as posts on the event wall, so it’s important that we ensure apps use their access appropriately. Starting today, apps using the API will no longer be able to access the guest list or posts on the event wall. And in the future, only apps we approve that agree to strict requirements will be allowed to use the Events API.

Groups API: Currently apps need the permission of a group admin or member to access group content for closed groups, and the permission of an admin for secret groups. These apps help admins do things like easily post and respond to content in their groups. However, there is information about people and conversations in groups that we want to make sure is better protected. Going forward, all third-party apps using the Groups API will need approval from Facebook and an admin to ensure they benefit the group. Apps will no longer be able to access the member list of a group. And we’re also removing personal information, such as names and profile photos, attached to posts or comments that approved apps can access.

Pages API: Until today, any app could use the Pages API to read posts or comments from any Page. This let developers create tools for Page owners to help them do things

like schedule posts and reply to comments or messages. But it also let apps access more data than necessary. We want to make sure Page information is only available to apps providing useful services to our community. So starting today, all future access to the Pages API will need to be approved by Facebook.

Facebook Login: Two weeks ago we announced important changes to Facebook Login. Starting today, Facebook will need to approve all apps that request access to information such as check-ins, likes, photos, posts, videos, events and groups. We started approving these permissions in 2014, but now we're tightening our review process — requiring these apps to agree to strict requirements before they can access this data. We will also no longer allow apps to ask for access to personal information such as religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading activity, music listening activity, news reading, video watch activity, and games activity. In the next week, we will remove a developer's ability to request data people shared with them if it appears they have not used the app in the last 3 months.

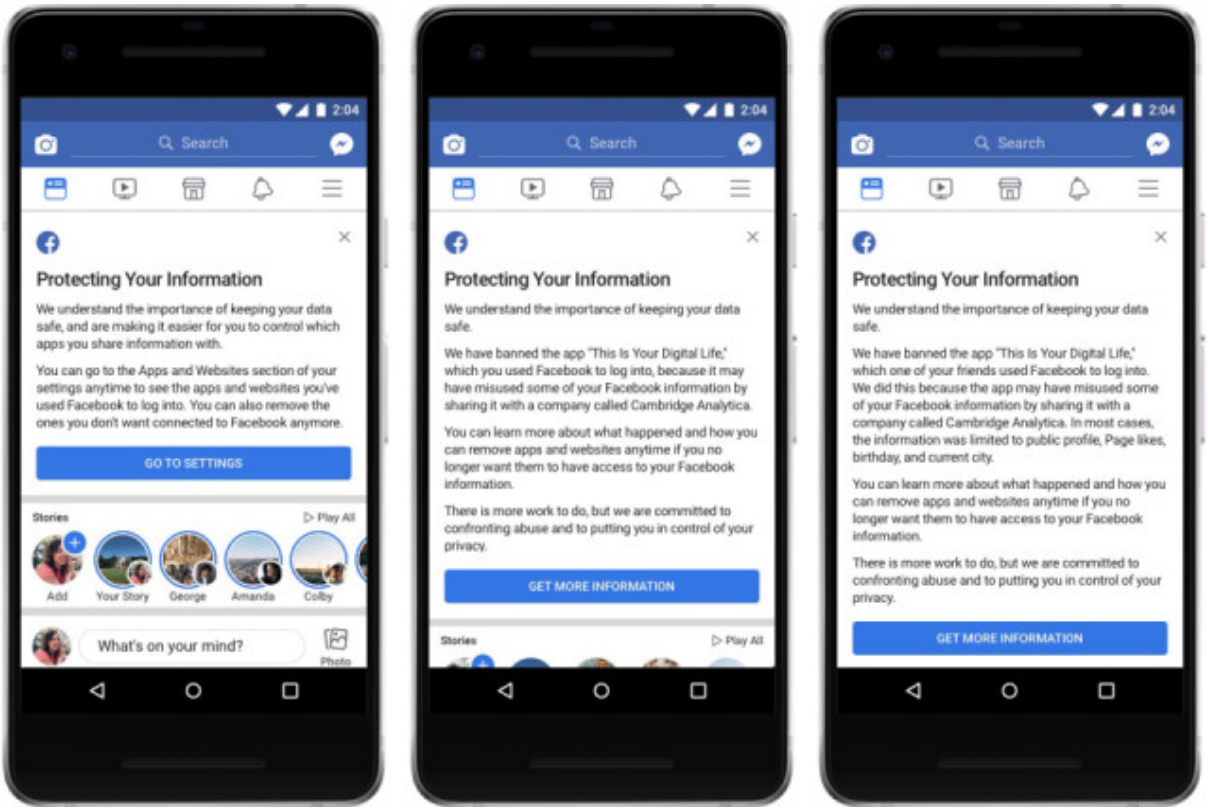
Instagram Platform API: We're making the recently announced deprecation of the Instagram Platform API effective today. You can find more information here.

Search and Account Recovery: Until today, people could enter another person's phone number or email address into Facebook search to help find them. This has been especially useful for finding your friends in languages which take more effort to type out a full name, or where many people have the same name. In Bangladesh, for example, this feature makes up 7% of all searches. However, malicious actors have also abused these features to scrape public profile information by submitting phone numbers or email addresses they already have through search and account recovery. Given the scale and sophistication of the activity we've seen, we believe most people on Facebook could have had their public profile scraped in this way. So we have now disabled this feature. We're also making changes to account recovery to reduce the risk of scraping as well.

Call and Text History: Call and text history is part of an opt-in feature for people using Messenger or Facebook Lite on Android. This means we can surface the people you most frequently connect with at the top of your contact list. We've reviewed this feature to confirm that Facebook does not collect the content of messages — and will delete all logs older than one year. In the future, the client will only upload to our servers the information needed to offer this feature — not broader data such as the time of calls.

Data Providers and Partner Categories: Last week we announced our plans to shut down Partner Categories, a product that lets third-party data providers offer their targeting directly on Facebook.

App Controls: Finally, starting on Monday, April 9, we'll show people a link at the top of their News Feed so they can see what apps they use — and the information they have shared with those apps. People will also be able to remove apps that they no longer want. As part of this process we will also tell people if their information may have been improperly shared with Cambridge Analytica.



Updated April 9, 2018: Three versions of the messages we're sending to people based on whether they've been affected by the app "This Is Your Digital Life." These messages link to facebook.com/help/yourinfo.
In total, we believe the Facebook information of up to 87 million people — mostly in the US — may have been improperly shared with Cambridge Analytica.

(***Update on May 1, 2018:*** Click here to see a state-by-state breakdown in the US of people whose Facebook information may have been improperly shared with Cambridge Analytica.)

Overall, we believe these changes will better protect people's information while still enabling developers to create useful experiences. We know we have more work to do — and we'll keep you updated as we make more changes. You can find more details on the platform changes in our Facebook Developer Blog.
Downloads
Cambridge Analytica Graph
App Controls Screenshots

(3)

Q&A With Mark Zuckerberg on Protecting People's Information

April 4, 2018
Hard Questions is a series from Facebook that addresses the impact of our products on society.
Today, Mark Zuckerberg spoke with members of the press about Facebook's efforts to better protect people's information. The following is a transcript of his remarks and the Q&A that followed.

Opening Remarks

Hey everyone. Thanks for joining today. Before we get started today, I just want to take a moment to talk about what happened at YouTube yesterday.
Silicon Valley is a tight-knit community, and we all have a lot of friends over there at Google and YouTube.
We're thinking of everyone there and everyone who was affected by the shooting.
Now I know we face a lot of important questions. So I just want to take a few minutes to talk about that upfront, and then we'll take about 45 minutes of your questions.
Two of the most basic questions that I think people are asking about Facebook are: first, can we get our systems under control and can we keep people safe, and second, can we make sure that our systems aren't used to undermine democracy?
And I'll talk about both of those for a moment and the actions that we're taking to make sure the answers are yes. But I want to back up for a moment first.
We're an idealistic and optimistic company. For the first decade, we really focused on all the good that connecting people brings. And as we rolled Facebook out across the world, people everywhere got a powerful new tool for staying connected, for sharing their opinions, for building businesses. Families have been reconnected, people have gotten married because of these tools. Social movements and marches have been organized, including just in the last couple of weeks. And tens of millions of small business now have better tools to grow that previously only big companies would have had access to.
But it's clear now that we didn't do enough. We didn't focus enough on preventing abuse and thinking through how people could use these tools to do harm as well. That goes for fake news, foreign interference in elections, hate speech, in addition to developers and data privacy. We didn't take a broad enough view of what our responsibility is, and that was a huge mistake. It was my mistake.

So now we have to go through every part of our relationship with people and make sure that we're taking a broad enough view of our responsibility. It's not enough to just connect people, we have to make sure that those connections are positive and that they're bringing people closer together. It's not enough to just give people a voice, we have to make sure that people are not using that voice to hurt people or spread disinformation. And it's not enough to give people tools to sign into apps, we have to ensure that all of those developers protect people's information too. It's not enough to have rules requiring they protect information, it's not enough to believe them when they tell us they're protecting information — we actually have to ensure that everyone in our ecosystem protects people's information.

So across every part of our relationship with people, we're broadening our view of our responsibility, from just giving people tools to recognizing that it's on us to make sure those tools are used well.

Now let me get into more specifics for a moment.

With respect to getting our systems under control, a couple of weeks ago I announced that we were going to do a full investigation of every app that had a large amount of people's data before we locked down the platform, and that we'd make further changes to restrict the data access that developers could get.

[VP, Product Partnerships] Ime Archibong and [Chief Technology Officer] Mike Schroepfer followed up with a number of changes we're making, including requiring apps you haven't used in a while to get your authorization again before querying for more of your data. And today we're following up further and restricting more APIs like Groups and Events. The basic idea here is that you should be able to sign into apps and share your public information easily, but anything that might also share other people's information — like other posts in groups you're in or other people going to events that you're going to — those should be more restricted. I'm going to be happy to take questions about everything we're doing there in a minute.

I also want to take a moment to talk about elections specifically.

Yesterday we took a big action by taking down Russian IRA pages targeting their home country.

Since we became aware of this activity, their activity after the 2016 US elections, we've been working to root out the IRA and protect the integrity of elections around the world. And since then there have been a number of important elections that we've focused on. A few months after the 2016 elections there was the French presidential election, and leading up to that we deployed some new AI tools that took down more than 30,000 fake accounts. After that there was the German election, where we developed a new playbook for working with the local election commission to share information on the threats we were each seeing. And in the US Senate Alabama special election last year, we successfully deployed some new AI tools that removed Macedonian trolls who were trying to spread misinformation during the election.

So all in, we now have about 15,000 people working on security and content review, and we'll have more than 20,000 by the end of this year.

This is going to be a big year of elections ahead, with the US midterms and presidential elections in India, Brazil, Mexico, Pakistan, Hungary and others — so this is going to be a major focus for us.

But while we've been doing this, we've also been tracing back and identifying this network of fake accounts the IRA has been using so we can work to remove them from Facebook entirely. This was the first action we've taken against the IRA in Russia itself, and it included identifying and taking down Russian news organization that we

determined were controlled and operated by the IRA. So we have more work to do here, and we're going to continue working very hard to defend against them.
All right. So that's my update for now. We expect to make more changes over the coming months, and we'll keep you updated, and now let's take some questions.
Q&A

David McCabe, Axios: Given that Colin testified just last year, and more has come out since then, and given that the numbers around the time of the IRA operation changed so drastically, why should lawmakers—why should users and Congress trust that you are giving them a full and accurate picture now?

Mark: Of the IRA — I think there is going to be more content that we are going to find over time. As long as there are people employed in Russia who have the job of trying to find ways to exploit these systems, this is going to be a never-ending battle. You never fully solve security — it's an arms race. In retrospect we were behind, and we didn't invest enough in it up front. We had thousands of people working on security, but nowhere near the 20,000 that we're going to have by the end of this year. So I am confident we are making progress against these adversaries. But they were very sophisticated, and it would be a mistake to assume that you can ever fully solve a problem like this, or think that they are going to give up and stop doing what they are doing.

Rory Cellan Jones, BBC: You, back in November 2016 when you could say this crisis began, dismissed as crazy the idea that fake news could influence the election, and more recently here in the UK you've turned down an invitation to speak to our Parliamentarians in the House of Commons, just as we learn tonight that 1 million UK users were affected by the Cambridge Analytica data leak. Are you taking this seriously enough, and can you convince British users that you care enough about the situation?

Mark: Yes. So we announced today that I'm going to be testifying in front of Congress. I imagine that is going to cover a lot of ground. I am going to be sending one of our top folks. I believe it's going to be [Mike Schroepfer], the CTO, or Chris Cox, the product officer. These are the top folks who I run the company with—to answer additional questions from countries and other places.
Oh sorry, I should also probably address — you asked about my comments after the 2016 election. I've said this already —but I think at this point that I clearly made a mistake by just dismissing fake news as "crazy"— as having an impact. People will analyze the actual impact of this for a long time to come, but what I think was clear at

this point is that it was too flippant. I should have never referred to it as crazy. This is clearly a problem that requires careful work, and since then we've done a lot to fight the spread of disinformation on Facebook from working with fact checkers to making it so that we're trying to promote and work with broadly trusted news sources. But this is an important area of work for us.

Ian Sherr, CNET: So you just announced 87 million people affected by the Cambridge Analytica stuff today. How long did you know this number was affected? Because the 50 million number was out there for quite a while. I know you guys weren't specifically saying that, but it feels like the data keeps changing on us. And we're not getting a full forthright view of what's going on here.

Mark: We only just finalized our understanding of the situation in the last I think couple of days on this. And as you said, we didn't put out the 50 million number. That came from other parties. We wanted to wait until we had the full understanding. Just to give you the complete picture on this: we don't have logs going back from when exactly [Aleksandr] Kogan's app queried for everyone's friends. What we did was basically constructed the maximum possible number of friends lists that everyone could have had over the time, and assumed that Kogan queried each person at the time when they had the maximum number of connections that would've been available to them. That's where we came up with this 87 million number. We wanted to take a broad view that is a conservative estimate. I am quite confident that given our analysis that it is not more than 87 million. It very well could be less, but we wanted to put out the maximum we felt that it could be as that analysis says.

David Ingram, Reuters: Hi Mark. I'm wondering if you can you address the audits that you're doing for third-party app developers. Specifically, I hear what you're saying about taking a broader view now about the company's responsibility, but why weren't there audits of the use of social graph API done years ago back in the 2010-2015 period?

Mark: Well, in retrospect, I think we clearly should have been doing more all along. But just to speak to how we were thinking about it at the time, as just a matter of explanation, I'm not trying to defend this now: I think our view in a number of aspects of our relationship with people is that our job is to give them tools, and that it was largely people's responsibility how they chose to use them — whether that's tools on how to share your voice, tools on how to log in to apps and bring your information to them. I think it was wrong in retrospect to have that limited of a view, but the reason why we acted the way that we did was because we viewed that when someone chose to share data with the platform it acted the way it was designed. With this personality quiz app, our view is that yes, Kogan broke the policies and that he broke peoples' expectations. But also that people chose to share that data with him. I think today, given what we know, not just about developers, but across all of our tools, and across what our place in society is, it's such a big service that's so central in peoples' lives. I think we need to take a broader view of our responsibility. We're not just building tools, but we need to take full responsibility for the outcome and how people use those tools as well. That's at least why we didn't do it at the time, but knowing what I know today, clearly we should have done more. And we will going forward.

Cecilia Kang, New York Times: Hi. Thanks for taking my question. Mark, you have indicated that you could be comfortable with some sort of regulation, and I think you alluded to potentially political ads. I'd like to ask you about privacy regulations that are about to take form, or take effect in Europe–GDPR. Would you be comfortable with those types of data protection regulations in the United States and deeper for global users?

Mark: Overall, I think regulations like the GDPR are very positive. I was somewhat surprised by yesterday's Reuters story that ran on this because the reporter asked if we are planning on running the controls for GDPR across the world and my answer was yes. We intend to make all the same controls and settings available everywhere, not just in Europe. Is it going to be exactly the same format? Probably not. We need to figure out what makes sense in different markets with the different laws and different places. But—let me repeat this—we'll make all controls and settings the same everywhere, not just in Europe.

Tony Romm, Washington Post: In a blog post, you acknowledged that profile information had been scraped by malicious actors? Who are these actors? Are they political organizations like Cambridge or others? And given that, do you believe this was all in violation of your 2011 settlement with the FTC? Thanks.

Mark: To take a step back on this, all of the changes we announced today were about ways that we built tools that were useful to a lot of people on sharing information or connecting with people but that we basically felt like the amount of information that potential bad actors could get—or specific folks who we've observed—could potentially misuse this. Whether that's the changes are in groups or events, it's not unreasonable to have an API where someone can bring the activity in a group to an app and be able to interactive with that in a group in an external app. We still wanted to shut that down because we felt like there was too many apps and too many folks who would have had access to people's content, and that would have been problematic. It's a similar situation with search. What we found here is we built this feature, and its very useful. There a lot of people who were using it until we shut it down today to look up the people who they want to add as friends but they don't have as friends yet. Especially in places where there are languages that makes it easier to type in a phone number or a number than for someone's name, or where a lot of people have the same name, it's helpful to have a unique identifier to disambiguate. But I think what was also clear is that the methods of rate limiting this weren't able to prevent malicious actors who cycled through hundreds of thousands of different IP address and did a relatively small number of queries for each one. Given that and what we know today, it just makes sense to shut that down.
You asked about the FTC consent order. We've worked hard to make sure that we comply with it. I think the reality here is that we need to take a broader view of our responsibility, rather than just the legal responsibility. We're focused on doing the right thing and making sure people's information is protected, and we're doing investigations. We're locking down the platform, et cetera. I think that our responsibilities to the people that use Facebook are greater than just what's written in that order, and that's the standard I want to hold us to.
Hannah Kuchler, Financial Times: Hi Mark. Thanks for taking my question. Investors have raised a lot of concerns about whether this is the result of

corporate governance issues at Facebook. Has the board discussed whether you should step down as chairman?

Mark: Not that I'm aware of.

Alexis Madrigal, The Atlantic: Every company, big and small, balances the service they provide with the needs of the business. In light of [Andrew Bosworth] Boz's post and your rethinking of Facebook's responsibility, have you ever made a decision that benefited Facebook's business but hurt the community?

Mark: I'll answer your question, but first because you brought up Boz's post. Let me take a moment to make sure that everyone understands that I disagreed with that at the time and I disagree with that now. I don't think that it stands for what most people inside the company believe. If you looked at the comments on that thread, when he initially wrote it, it was massively negative. So, I feel like that's an important point to set aside.
In terms of the questions you asked, balancing stakeholders, the thing that I think makes our product challenging to manage and operate are not the trade-offs between the people and the business — I actually think that those are quite easy because over the long term the business will be better if you serve people. I just think that it would be near-sighted to focus on short-term revenue over what value to people is, and I don't think we are that short-sighted. All of the hard decisions that we have to make are actually trade-offs between people. One of the big differences between the type of product that we are building is — which is why I refer to it as a community and what I think some of the specific governance challenges we have are — the different people that use Facebook have different interests. Some people want to share political speech that they think is valid, and other people feel like it's hate speech. And then, people ask us, "Are you just leaving that up because you want people to be able to share more?" These are real values and questions and trade-offs. Free expression on the one hand, making sure it's a safe community on the other hand. We have to make sure we get to the right place, and we're doing that in an environment that's not static. The social norms are changing continually, and they're different in every country around the world. Getting those trade-offs right is hard, and we certainly don't always get them right. To me, that's the hard part about running the company—not the trade-off between the people and the business.

Alyssa Newcomb, NBC News: Hi Mark, you said you've clearly made some mistakes in past, and I'm wondering do you still feel like you're the best person to run Facebook moving forward?

Mark: Yes. I think life is about learning from the mistakes and figuring out what you need to do to move forward. A lot of times people ask, "What are the mistakes you made early on, starting the company, or what would you try to do differently?" The reality of a lot of this is that when you are building something like Facebook that is unprecedented in the world, there are going to be things that you mess up. And if we had gotten this right, we would have messed something else up. I don't think anyone is going to be perfect, but I think what people should hold us accountable for is learning from the mistakes and continually doing better and continuing to evolve what our view of our responsibility is — and, at the end of the day, whether we're building things that

people like and that make their lives better. I think it's important to not lose sight of that through all of this. I'm the first to admit that we didn't take a broad enough view of what our responsibilities were. But, I also think it's important to keep in mind that there are billions of people who love the services that we're building because they're getting real value and being able to connect and build connections and relationships on day-to-day basis. And that's something I'm really proud of our company for doing, and I know that we will keep on doing that.

Josh Constine, TechCrunch: Thank you. During today's disclosure and announcement, Facebook explained that the account recovery and search tools using email and phone number could have been used to scrape information about of all of Facebook's users. When did Facebook find out about this scraping operation, and, if that was before a month ago, why didn't Facebook inform the public about it immediately?

Mark: We looked into this and understood it more over the last few days as part of the audit of our overall system. Everyone has a setting on Facebook, that controls — it's right in your privacy settings — whether people can look you up by your contact information. Most people have that turned on, and that's the default, but a lot of people have also turned it off. So it's not quite everyone, but certainly the potential here would be that over the period of time that this feature has been around, people have been able to scrape public information. The information—that if you have someone's phone number, you can put that in, and get a link to their profile which pulls their public information. So, I certainly think that it is reasonable to expect that if you had that setting turned on, that at some point during the last several years, someone has probably accessed your public information in this way.

Will Oremus, Slate: Thanks very much for doing this. You run a company that relies on people being willing to share data, that is then used to target them with ads. We also now know that it can be used in more manipulative ways or ways they don't expect. We also know you're protective of your own privacy. You acknowledged that you put tape over your webcam at one point, think you bought one of the lots surrounding your home just to get more privacy. I'm curious — what other steps do you take personally to protect your privacy online? Do you use an ad blocker? As a Facebook user, would you sign up for an apps like the personality quiz that folks signed up for? Thanks very much for having us.

Mark: I certainly use a lot of apps. I don't know if I use that one specifically, but I am a power user of the internet here. In order to protect privacy, I would just advise that people follow best practices around security: turn on two-factor authentication, change passwords regularly, don't have your password recovery responses be information that you made publicly available somewhere. All the basic practices, and then just look out and understand that most attacks are going to be social engineering, and not necessarily people trying to break into security systems. For Facebook specifically, one of the things we need to do and that I hope that more people look at are just the privacy controls that you have. I think, especially leading up to the GDPR event, a lot of people are asking us, "Okay, are you going to implement all those things?" And my answer is that we've had almost all of what's in there implemented for years, around the world, not just in Europe. So, to me, the fact that a lot of people might not be aware

of that is an issue, and I think we could do a better job of putting these tools in front of people and not just offering them, and I would encourage people to use them and make sure that they're comfortable with how their information is used on our services and others.

Sarah Frier, Bloomberg: Hi Mark. There's broad concern that these audits for developers won't actually work, that the data that users gave to third-parties years ago could be anywhere by now. What results do you hope to achieve from the audit and what won't you be able to find?

Mark: It's a good question. No measure that you take on security is going to be perfect, but a lot of the strategy has to involve changing the economics of potential bad actors to make it not worth doing what they might do otherwise. So I think you're right that we're not going to be able to go out and necessarily find every single bad use of data. What we can do is make it a lot harder for folks to do that going forward: change the calculus on anyone who is considering doing something sketchy going forward. And I actually do think that we'll be able to uncover a large amount of bad activity, of what exists, and we will be able to go in and do audits and ensure people go get rid of bad data.

Steve Kovach, Business Insider: Hi. Has anyone been fired related to the Cambridge Analytica issue or any other data privacy issue?

Mark: I have not… due to the Cambridge Analytica situation. We are still working through this. At the end of the day, this is my responsibility. So there have been a bunch of questions about that. I started this place. I run it. And I am responsible for what happens here. To the question before, I still think that I'm going to do the best job to help run it going forward. I'm not looking to throw anyone else under the bus for mistakes that we've made here.

Nancy Cortez, CBS News: Hi there. Thank you so much for taking the question. Your critics say, look, Facebook's model, Facebook's business model, depends on harvesting personal data. How can you ever personally reassure users that their data won't be used in ways they don't expect?

Mark: I think we can certainly do better job of explaining what we actually do. There are many misconceptions around what we do that I think we haven't succeeded in clearing up for years. So, first, the vast majority of data that Facebook knows about you is because you chose to share it. Right? It's not tracking. There are other internet companies or data brokers or folks that might try to track and sell data, but we don't buy and sell. In terms of the ad activity, I means that's a relatively smaller part of what we're doing. The majority of the activity is people actually sharing information on Facebook, which is why people understand how much content is there, because people put all the photos and information there themselves. The second point, which I touched on briefly there: for some reason we haven't been able to kick this notion for years that people think we will sell data to advertisers. We don't. That's not been a thing that we do. Actually it just goes counter to our own incentives. Even if we wanted to do that, it just wouldn't make sense to do that. So, I think we can certainly do a better job of explaining this and making it understandable, but the reality is the way we run the service is: people share information, we use that to help people connect and to

make the services better, and we run ads to make it a free service that everyone in world can afford.

Mathew Braga, CBC News: Hey Mark, I just want to go back to something that was brought up earlier around the scraping of profile information. I know Mike Schroepfer in his post said something about the scale and sophistication of the activity. And I'm just wondering can you put a little more context on that? Like what sort of scale are we talking about? Do you have exact numbers? Can you give us any harder sense than, sort of, what's in that post?

Mark: In terms of sophistication, this is stuff that I've already said on some of the other answers, so I'll try to keep this short. We had basic protections in place to prevent rate-limiting, making sure that accounts couldn't do a whole lot of searches. But we did see a number of folks who cycled through many thousands of IPs, hundreds of thousands of IP addresses to abade the rate-limiting system, and that wasn't a problem we really had a solution to. So now, that's partially why the answer we came to is to shut this down even though a lot of people are getting a lot of use out of it. That's not something we necessarily want to have going on. In terms of the scale, I think the thing people should assume, given this is a feature that's been available for a while and a lot of people use it in the right way, but we've also seen some scraping, I would assume if you had that setting turned on, that someone at some point has accessed your public information in this way.

Rebecca Jarvis, ABC News: Hi Mark. Thanks for doing this. Cambridge Analytica has tweeted now since this conversation began, "When Facebook contacted us to let us know the data had been improperly obtained, we immediately deleted the raw data from our file server, and began the process of searching for and removing any of its derivatives in our system." And I want to understand from you, now that you have this finalized understanding, do you agree with Cambridge's interpretation and the tweet they just shared? And will you be pursuing legal action against Cambridge Analytica?
Mark: I don't know that what we announced today really is connected to what they just said at all. What we announced with the 87 million is the maximum number of people we could calculate could have been accessed. We don't actually know how many people's information Kogan actually got. We don't know what he sold to Cambridge Analytica, and we don't know today what they have in their system. What we have said and what they've agreed to do, is a full forensic audit of their system, so we can get those answers. But, at the same time the UK government, and the ICO, are doing a government investigation and that takes precedence. So, we've stood down temporarily, to let the ICO do their investigation and their audit, and once that's done, we'll resume ours, so we can get answers to the questions that you're asking and ultimately to make sure that none of the data persists or is being used improperly. And at that point if it makes sense, we will take legal action if we need to do that to protect people's information.

Alex Kantrowitz, BuzzFeed: Hey Mark, thanks so much for doing this. We should do this every month, this is great. So, my question is that Facebook is really good at making money. But I wonder if your problems could be somewhat mitigated if the company didn't try to make so much. So, you can still run Facebook as a free service and collect significantly less data and offer

significantly less ad targeting criteria. So, I wonder if you think that would put you and society at less risk and if you think it's something you'd consider doing?

Mark: People tell us that if they're going to see ads, they want the ads to be good. And the way to make the ads good, is by making it so that when someone tells us they have an interest, they like technology or they like skiing or whatever it is they like, that the ads are actually tailored to what they care about. So, like most of the hard decisions that we make, this is one where there is a trade-off between values that people really care about. On the one hand people want relevant experiences, and on the other hand I do think that there is some discomfort for how data is used in systems like ads. But I think the feedback is overwhelming on the side of wanting a better experience. You know, maybe its 95-5 or something like that in terms of the preferences that people state to us and in their use of the product. So, that informs us of decisions that we make here to offer the best service to people, but these are hard values trade-offs and I think we are doing the right thing to serve people better.

Nancy Scola, POLITICO: When you became aware in 2015 that Cambridge Analytica inappropriately accessed this Facebook data, did you know that firm's role in American politics and in Republican politics in particular?

Mark: I certainly didn't. One of the things and in retrospect looking back at it, people ask, why didn't you ban them back then? We banned Kogan's app from our platform, but we didn't ban Cambridge Analytica in 2015, why did we do that? It actually turns out in our understanding of the situation, they weren't using any of Facebook's services back then. They weren't an advertiser, although they went on to become one in the 2016 elections. And I don't think they were administering tools and they didn't build an app directly. So, they were not really a player that we had been paying attention to. So, that's the history there.

Carlos Hernandez, Expansion: Hi Mark. You mentioned one of the main important things about Facebook is people… and users' understanding of the platform. Do you have any plans to let users know how their data is being used? Not just on Facebook but also on Instagram and other platforms that you are responsible for?

Mark: I think we need to do a better job of explaining principles that the service operates under, but the main principles are, you have control over everything you put on the service, and most of the content Facebook knows about you it because you chose to share that content with your friends and put it on your profile. And we're going to use data to make those services better, whether that's ranking News Feed, or ads, or search, or helping you connect with people through people you may know, but we're never going to sell your information. And I think if we can get to a place where we can communicate that in a way that people can understand it, then I think we have a shot of distilling this down to something, to a simpler thing, but that's certainly not something

we have succeeded at doing historically.

Kurt Wagner, Recode: Hey Mark. There’s been the whole #deletefacebook thing that went around a few weeks ago, there’s been advertisers that have that they are either going to pull advertising money or pull their pages down altogether. I’m wondering if on the back end, have you seen any actual change in usage from users or change in ad buys from advertisers over the past couple of weeks as result of all this?

Mark: I don’t think there has been any meaningful impact we’ve observed. But, look, it’s not good. I don’t want anyone to be unhappy with our services or what we do as a company. So, even if we can’t really measure a change and the usage of a product, or the business or anything like that, it still speaks to people feeling like this is a massive breach of trust and that we have a lot of work to do to repair that.

Fernando Santillanes, Grupo Milenio: Hi Mark. Thank you very much for doing this. There’s a lot of concern in Mexico about the fake news. People say that associating with media to [downrank] these fake articles is not enough. We are in an election year, here in Mexico. People are worried that there are a lot of apps, a lot of means, that a candidate won’t manipulate the information. What do you say to Mexicans this election year, here almost all internet users have a Facebook account and that they want to see a more active Facebook position to detect and [downrank] fake news?

Mark: This is important. Let me say two things. The first is that 2018 is going to be an important year for protecting election integrity around the world. There’s the Mexican presidential election, there are big presidential elections in India and Brazil, as well as Pakistan and Hungary and a number of other countries, and the US midterms, of course, too. Second, let me talk about how we’re fighting fake news across the board. Right, because there are really three different types of activity that require different strategies for fighting them, so you can understand all of what we’re doing here. The three basic categories, are: economic actors — basically spammers — the second are governments, trying to interfere in elections — that’s a security issue — the third is just polarization and some kind of lack of truthfulness in what you’ve described as the media and in terms of people who are legitimately trying to get the opinion they believe out there. So let’s look at each of these briefly.
So for economic actors, these are folks like the Macedonian trolls who we identified with AI tools leading up to the Alabama special election. What these folks are doing is just an economic game, it’s not ideological at all. They come up with the most

sensational thing they can, try to push it out to social media and the internet to try to get you to click on it so that they can make money on ads. So, we make it so that the economics stop working for them, and they'll move on to something else. I mean, these are the same type of people who were sending you Viagra emails in the 90s. Right, we can attack it both sides: on the revenue side we can make it so that they can't run on the Facebook ad network, and that's important because now they don't make as much money on that because the ad network works well for folks. On the distribution side, we make it so that as we detect the stuff that it gets less distribution on News Feed. So now we just make it so that it's less worth it for them, so that they kind of go and do other stuff and we're seeing that that's working.

The next category are these national security type issues. So that's the Russian election interference, and instead of treating it like spammers, you treat it as a security issue. In order to solve that, what we need to do is identify these bad actors. It's actually less about content, because some of the stuff would've been legitimate speech had someone who is not a bad actor been doing it, but people are setting up these large networks of fake accounts, like the IRA had done, and what we need to do is just track that really carefully in order to be able to remove it from Facebook entirely. What we're seeing is the IRA and organizations like that, are morphing — whether they're media organizations or sanctioned news organizations in Russia, are that when we investigate this closely over time, we're able to prove are completely owned, controlled and operated by the IRA, we take that down and treat it as a security issue.

The third category is about legitimate media. And there, I think there are a few different strategies. The first is doing more fact checking. To your question, in Mexico, we recently launched our fact-checking initiative in Mexico, specifically, leading up to the election, that's an important thing to do. We find that even though the fact-checkers aren't checking millions of things a day, we can show them the highest volume things and that can both be used to show a useful signal on the product, and help inform rankings to flag to people if it's a hoax. But then even beyond that, for stuff that's not just broad hoaxes, there's still a big polarization issue, which is that often even if someone isn't false, they're kind of cherry-picking facts to tell one side of the story, and the aggregate picture ends up not being true even if the specific facts within it might be. And there, the work that you need to do is about promoting broadly-trusted journalism. The folks who people across society are going to take the full picture and show, and do a fair and thorough job. That's the News Feed change we made there, which I think we've gotten relatively good feedback from people using Facebook on that change and the quality of what they're seeing.

So, those three streams, I think that if we can do a good job on each of those, we'll make a big dent in the problem. Not only for the Mexican election this year, but across the world and that's basically the road-map that we're executing.

Casey Newton, The Verge: With respect to some of the measures you're putting into place to protect election integrity, and reduce fake news that you just talked about, how are you evaluating the effectiveness of the changes you're making and how will you communicate regarding any wins and losses in run up to and the aftermath of the next election?

Mark: One of the big things that we're working on now is a major transparency effort to be able to share the prevalence of different types of bad content. Right now, one of the big issues that we see — you know a lot of the debate around things like fake news or hate speech happens through anecdotes. People see something that is bad, that shouldn't be allowed on the service, and they call us out on it. And frankly, they are

right, it shouldn't be there, and we should do a better job of taking that down. What I think is missing from the debate today is the prevalence of the different categories of bad content. Whether it's fake news, and all the different kinds therein, hate speech, bullying, terror content. All of the things that I think we would all agree are bad and that we want to drive down. The most important thing though there is to make sure that the numbers we put out are accurate. We wouldn't be doing anyone a favor by putting out numbers, then coming back a quarter later and saying hey we messed this up. Part of the point of transparency is both to inform the public debate and to build trust. And if we have to go back and restate those because we got it wrong, then I think the calculation internally is that it's much better to take a little longer and make sure we're accurate then to put something out that might be wrong. I [believe] that's going to end up being way we should be held accountable and measured by the public. I think it will help create more informed debates. And my hope over time is that the playbook and scorecard that we put out will also be followed by other internet platforms, so that way there can be a standard measure across the industry about how to measure these important issues.

Barbara Ortutay, AP: Hi. Thank you. So one of the things that you've addressed recently, some of the ways malicious actors are misusing Facebook. So I'm wondering what are you doing differently now to prevent things from happening, and not just respond after the fact? You know, will this be built into your new product launches that you have to think about and, if possible, [misuse] right away once the product is out?

Mark: Yeah. I think going forward, I think a lot of the new product development has already internalized this perspective of the broader responsibility that we need to take to make sure our tools are used well. I can give you a few examples across different work that we're doing. But right now, if you take the election integrity work for example, in 2016 we were behind where we wanted to be. We had a more traditional view of the security threats. We expected Russia and other countries to try do to phishing, and traditional kind of security exploits, but not necessarily kind of misinformation campaign that they did. We were behind. That was a really big miss. So now we want to make sure that we're not behind again. As I mentioned my opening remarks earlier — since then there was the French election, the German election, you know last fall there was the Alabama special election and we've been proactively developing AI tools to detect trolls who are spreading fake news or foreign interference. In the French election and Alabama election, we were able to take down thousands of fake accounts. So that's an example of proactive work we're doing to get ahead, which gives me confidence that on that kind of specific issue, around election integrity, we're making progress. It's not that there's no bad content out there. I don't want to ever promise that we're going to find everything or that we've beaten the enemies into submission. They are still employed, they still have their jobs. We need to strengthen our system. But across the different products and things we're building, I do think that we're starting to internalize a lot more that we have this broader responsibility.
Last thing I'll say on this, I wish that I could snap my fingers and in three or six months have solved all of these issues. But I just think the reality is, given how complex Facebook is and how many systems there we need to rethink our relationship with people and our responsibility there across every single part of what we do. I do think this is a multi-year effort. It doesn't mean its not going to get better, every month. I think it will continue to get better. I think part of the good news is that we've really started

ramping up on this a year ago or more. So we're not getting a cold start, we're probably a year into a massive three-year push. My hope is that by the end of this year, we'll have turned the corner on a lot of these issues and people see that things are getting a lot better. But these are just big issues, this is a big shift for us to take a lot more responsibility for how each of the tools are used, not just the developer platform, not just fake news, not just elections, but everything. And its going to take some time. And we're committed to getting that right and we're going to invest and keep on working until we do.
Thank you all for joining today. What we announced today were some of changes that we need to make. We're going to keep on looking for things, we're going to keep on finding more, and we'll update you then. Thanks for joining and talking to us about this. We look forward to keeping you updated on our progress.

Download
Complete Call Audio

7. **Communiqué de presse du 14 mai 2018**

An Update on Our App Investigation and Audit

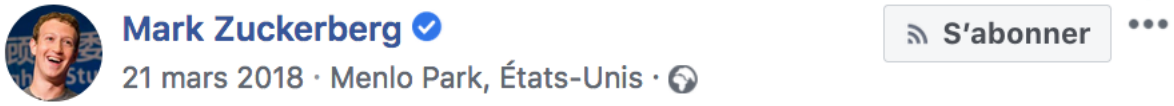
May 14, 2018

By Ime Archibong, VP of Product Partnerships

Here is an update on the app investigation and audit that Mark Zuckerberg promised on March 21.

As Mark explained, Facebook will investigate all the apps that had access to large amounts of information before we changed our platform policies in 2014 — significantly reducing the data apps could access. He also made clear that where we had concerns about individual apps we would audit them — and any app that either refused or failed an audit would be banned from Facebook.
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 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 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 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 notify people via this website. It will show people if they or their friends installed an app that misused data before 2015 — just as we did for Cambridge Analytica.
There is a lot more work to be done to find all the apps that may have misused people's Facebook data – and it will take time. We are investing heavily to make sure this investigation is as thorough and timely as possible. We will keep you updated on our progress.

8. **Publication de Mark Zuckerberg du 21 mars 2018**



I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue.

We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again. The good news is that the most important actions to prevent this from happening again today we have already taken years ago. But we also made mistakes, there's more to do, and we need to step up and do it.

Here's a timeline of the events:

In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who shared their data as well as some of their friends' data. Given the way our platform worked at the time this meant Kogan was able to access tens of millions of their friends' data.

In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today.

In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. They provided these certifications.

Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We're also working with regulators as they investigate what happened.

This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.

In this case, we already took the most important steps a few years ago in 2014 to prevent bad actors from accessing people's information in this way. But there's more we need to do and I'll outline those steps here:

First, we will investigate all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014, and we will conduct a full audit of any app with suspicious activity. We will ban any developer from our platform that does not agree to a thorough audit. And if we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps. That includes people whose data Kogan misused here as well.

Second, we will restrict developers' data access even further to prevent other kinds of abuse. For example, we will remove developers' access to your data if you haven't used their app in 3 months. We will reduce the data you give an app when you sign in -- to only your name, profile photo, and email address. We'll require developers to not only get approval but also sign a contract in order to ask anyone for access to their posts or other private data. And we'll have more changes to share in the next few days.

Third, we want to make sure you understand which apps you've allowed to access your data. In the next month, we will show everyone a tool at the top of your News Feed with the apps you've used and an easy way to revoke those apps' permissions to your data. We already have a tool to do this in your privacy settings, and now we will put this tool at the top of your News Feed to make sure everyone sees it.

Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform.

I started Facebook, and at the end of the day I'm responsible for what happens on our platform. I'm serious about doing what it takes to protect our community. While this specific issue involving Cambridge Analytica should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward.

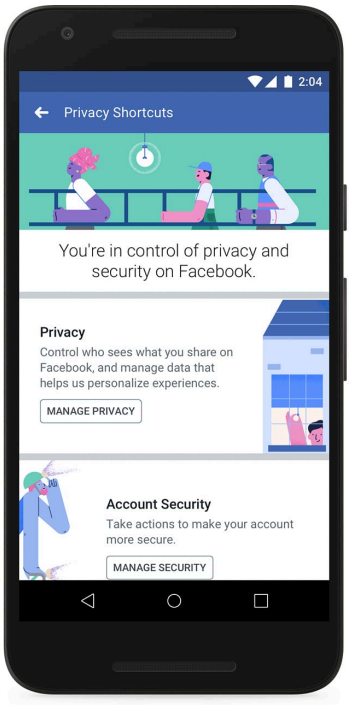
I want to thank all of you who continue to believe in our mission and work to build this community together. I know it takes longer to fix all these issues than we'd like, but I promise you we'll work through this and build a better service over the long term.

274 K 53 K commentaires 68 K partages

9. Publication de Mark Zuckerberg du 28 mars 2018

Mark Zuckerberg
28 mars 2018 ·

A lot of you are asking how to control what information you share on Facebook, who has access to it, and how to remove it. We recently put all your privacy and security settings in one place called Privacy Shortcuts to make it easier to use. We're going to put this in front of everyone over the next few weeks. We're also going to put a tool with all the platform apps you've signed into in at the top of your News Feed so you can easily remove any apps you no longer use.



175 K 19 K commentaires 17 K partages

10. **Interview de Mark Zuckerberg 21 mars 2018 (CNN)**

Mark Zuckerberg in his own words: The CNN interview

March 21, 2018: 11:35 PM ET

Mark Zuckerberg sat down for an exclusive interview with CNN's Laurie Segall on Wednesday, days after news broke that Cambridge Analytica, a data firm with ties to President Donald Trump's 2016 campaign, accessed information from 50 million Facebook users without their knowledge.

Zuckerberg apologized for the scandal, discussed Facebook's efforts to prevent bad actors for meddling in the 2018 midterm elections and shared his regrets. Read excerpts from the emotional interview below.

What went wrong

Laurie Segall: I'm gonna start with just a basic question, Mark, what happened? What went

wrong?

Mark Zuckerberg: So this was a major breach of trust and I'm really sorry that this happened. You know we have a basic responsibility to protect people's data and if we can't do that then we don't deserve to have the opportunity to serve people. So our responsibility now is to make sure that this doesn't happen again. And there are a few basic things that I think we need to do to ensure that. One is making sure that developers like Aleksandr Kogan, who got access to a lot of information and then improperly used it, just don't get access to as much information going forward. So we are doing a set of things to restrict the amount of access that developers can get going forward. But the other is we need to make sure that there aren't any other Cambridge Analyticas out there. Right, or folks who have improperly accessed data. So we're gonna go now and investigate every app that has access to a large amount of information from before we locked down our platform. And if we detect any suspicious activity we're gonna do a full forensic audit.

What Facebook's doing now

Zuckerberg: We're going to review thousands of apps. So, this is gonna be an intensive process, but this is important. I mean this is something that in retrospect we

clearly should have done, upfront, with Cambridge Analytica. We should not have trusted the certification that they gave us. And we're not gonna make that mistake again. I mean this is our responsibility to our community, is to make sure that we secure the data that they're sharing with us.

Segall: Will you take legal action against Cambridge Analytica?

Zuckerberg: Well the first thing that we need to do is actually understand what happened. So, you know, right now we have the report from the Times and the Guardian and Channel 4 that said that they thought that Cambridge Analytica might have access to data still. But the first thing that we need to do is complete our audit there... the short answer is that if we go in and find that Cambridge Analytica still has access to the data, we're gonna take all legal steps that we can to make that the data of people in our community is protected.

CNN Exclusive: Zuckerberg apologizes

What he regrets

Segall: Respond to the users who say you didn't get in front of it because we're here talking

about it today.

Zuckerberg: Well, clearly I wish we'd taken those steps earlier. I mean, that, that I think is probably the biggest mistake that we made here ... the feedback from the community and the world has overwhelmingly been, that, if you balance these two values of being able to take your data and some data from friends to be able to have social experiences on other apps on the one hand, this ideal of kind of data portability. And on the other hand, making sure that your data's always locked down. Guaranteeing that it never goes anywhere. You know I think we've started off a little bit on the idealistic, and maybe naive side, right, of thinking that that vision around data portability and enabling social apps was gonna be what our community preferred, and I think what we've learned over time very clearly is that the most important thing always is making sure that people's data is locked down. And that's a mistake that ... we fixed a few years back and I don't expect us to make again.

On 'selling data'

Segall: Is your business model on trial here?

Zuckerberg: You know, one of the big misconceptions about Facebook is this idea that we somehow sell data. We don't sell any data to anyone and that's actually a really key part of the model. Both for protecting people's personal data and privacy, but also because, you know the competitive advantage of a lot of our services, whether that's ranking News Feed or ranking search or even ranking ads is that people do share a lot of information on Facebook and therefore we can build better services. So we don't want data to be able to get out. When that happens, that's not good for people in our community, that's not good for our business. So, that's not actually how ads work on the service and it actually has never been. An advertiser can come to us and say, "Hey,

I'd like to reach women within this age range" and if we understand who is in that then we can show that ad but none of that information goes to the advertiser.

How Facebook is fighting election meddling

Zuckerberg: I think what's clear is that in 2016, we were not as on top of a number of issues as we should have [been] whether it was Russian interference or fake news. But what we have seen since then is, a number of months later there was a major French election, and there we deployed some AI tools that did a much better job of identifying Russian bots and basically Russian potential interference and weeding that out of the platform ahead of the election. And we were much happier with how that went. In 2017, last year, during the special election, the senate seat in Alabama, we deployed some new AI tools that we built to detect fake accounts that were trying to spread false news and we found a lot of different accounts coming from Macedonia. So, I think the reality here is that this isn't rocket science. Right? And there's a lot of hard work that we need to do to make it harder for nation-states like Russia to do election interference, to make it so that trolls and other folks can't spread fake news, but we can get in front of this. And we have a responsibility to do this, not only for the 2018 midterms in the U.S., which are going to be a huge deal this year and that's just a huge focus for us but there's a big election in India this year, there's a big election in Brazil, there are big elections around the world, and you can bet that we are really committed to doing everything that we need to to make sure that the integrity of those elections on Facebook is secured.

Related: The fake news machine: Inside a Macedonian town gearing up for 2020

On attempts to manipulate the midterm elections

Segall: Do you think that bad actors are using Facebook at this moment to meddle with the U.S.

midterm elections?

Zuckerberg: I'm sure someone's trying. Right? I'm sure that there's V2, version two of whatever the Russian effort was in 2016, I'm sure they're working on that and there are going to be some new tactics that we need to make sure that we observe and get in front of --

Segall: Do you know what the -- speaking of getting in front of them, do you know what they are?

Zuckerberg: Yes, and I think we have some sense of the different things that we need to get in front of and we have a lot of different folks in the company, both building technology and, a lot of this stuff requires people to review things and that's one of the big commitments that we've made this year is to double the number of people working on security at the company. We're going to have 20,000 people working on security and content review in this company by the end of this year. We have about 15,000 people working on security and content review now. So I think the combination of building the right tools to identify different patterns across all of our products and having people to review them at the scale and speed that we need is going to be a good

formula, but you know, security isn't a problem that you ever fully solve. You can get to the level where you're better than your adversaries and they continue evolving, so we're going to be working on this forever, as long as this community remains an important thing in the world.

Segall: Are you specifically seeing bad actors trying to meddle with the U.S. election now?

Zuckerberg: What we see are a lot of folks trying to sew division. Right? So that was a major tactic that we saw Russia try to use in the 2016 election. Actually most of what they did was not directly, as far as we can tell from the data that we've seen, was not directly about the election, but was more about just dividing people. You know, so they'd run a group for pro- immigration reform and they'd run another group against immigration reform to just try to pit people against each other. And a lot of this was done with fake accounts that we could do a better job of tracing and using AI tools to be able to scan and observe a lot of what is going on and I'm confident that we're going to do a much better job. Now the reality is with a community of two billion people, I can't promise that we're going to find everything. But what I can commit to is that we're going to make it as hard as possible for these adversaries to do that and I think that we're going to do a much better job.

Related: 'I'm sure someone's trying' to disrupt 2018 midterm elections

Testifying before Congress

Segall: Lawmakers in the United States and the UK are asking you to testify. Everybody wants

you to show up. Will you testify before Congress?

Zuckerberg: So, the short answer is I'm happy to, if it's the right thing to do. Facebook testifies in Congress regularly on a number of topics, some high profile and some not. And our objective is always to provide Congress, who does an extremely important job, to have the most information that they can. We see a small slice of activity on Facebook, but Congress gets to have access to the information across Facebook and all other companies and the intelligence community and everything. So what we try to do is send the person at Facebook who will have the most knowledge about what Congress is trying to learn. So if that's me, then I am happy to go. What I think we've found so far is that typically there are people whose whole job is focused on an area, but I would imagine at some point that there would be a topic where I am the sole authority on and that would make sense for me to do and I'll be happy to do it at that point.

Zuckerberg: 'Happy' to testify before Congress

Whether Facebook should be regulated

Segall: Given the stakes here, why shouldn't Facebook be regulated?

Zuckerberg: I actually am not sure we shouldn't be regulated. I think in general technology is an increasingly important trend in the world and I actually think the question is more, what is the right regulation rather than "Yes or no, should it be regulated?"

Segall: What's the right regulation?

Zuckerberg: Well there's some basic things, then I think there are some big intellectual debates. On the basic side, I think there are things like ads transparency regulation that I would love to see. If you look at how much regulation there is around advertising on TV and print, it's just not clear why there should be less on the internet. We should have the same level of transparency required. And I don't know if the bill is going to pass. I know a couple of senators are working really hard on this, but we're committed and we've actually already started rolling out ad transparency tools that accomplish most of the things that are in all the bills that people are talking about today because this is an important thing. People should know who is buying the ads that they see on Facebook, and you should be able to go on any page and see all the ads that people are running to different audiences. So we actually already have this running in Canada as a test and our goal is to get this running here well before the 2018 midterms, so that way we'll have that new, higher standard of transparency in place for the 2018 midterms in the U.S. There are broader regulation questions as well, but that's actually an easy one.

Growing pains

Segall: So you've been the leader of Facebook for 14 years. Looking back on all your time, because we don't get to hear Mark, personal Mark that often, do you have any moments that you look at that are regrets? If you could look at one moment as something you regretted that you really wish now you could have changed or you could have done, what would it be?

Zuckerberg: Oh, I don't know. I mean, there are so many mistakes that I've made. I started this company when I was 19. I was a kid.

Segall: What do you say to your 19-year-old self in a dorm room?

Zuckerberg: I think a pretty common question is "What mistake do you wish you'd not made?" but the reality is you can make a ton of mistakes in your life, no matter what you do and you know, I've made, I've made every kind of mistake that you can make. I mean I started this when I was so young and inexperienced, right? I made technical errors and business errors. I hired the wrong people. I trusted the wrong people. I've probably launched more products that have failed than most people will in their lifetime. But you know I think the thing that makes Facebook work for people, is not that there weren't mistakes; it's that we learned from them. Right, and that's the commitment that I try to have inside our company and for our community is that yeah, maybe you're not gonna get everything right. The world changes. There are gonna be new challenges that come up.

Related: 'I'm really sorry that this happened'

How being a father changed him

Segall: How has being a father changed your commitment to users, changed your commitment

to their future and what a kinder Facebook looks like? **Zuckerberg:** Well, I think, having kids changes a lot. And- **Segall:** Like what?

Zuckerberg: Well, you know I used to think that the most important thing to me by far was, you know my having the greatest positive impact across the world that I can and, now I really just care about building something that my girls are gonna grow up and be proud of me for. And that's what is kind of my guiding philosophy at this point is and you know I come and work on a lot of hard things during the day and I go home and just ask will my girls be proud of what I did today?

— *CNN's Rob McLean and Danielle Wiener-Bronner contributed.*

CNNMoney (New York) First published March 21, 2018: 11:35 PM ET

(RECORDE)

Here’s the transcript of Recode’s interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more

“I think we let the community down, and I feel really bad and I’m sorry about that,” he said.

By Kara Swisher and Kurt Wagner Mar 22, 2018, 3:49am EDT

Facebook CEO Mark Zuckerberg gave interviews yesterday to several news organizations, including **Recode**, in an attempt to stem the fast-growing controversy about misuse of user data by a third-party developer, Cambridge Analytica.

In a wide-ranging interview, he admitted the social networking giant may have made mistakes in opening up its network so much a decade ago and that it led to the recent problems. Zuckerberg said that fixing those issues will now cost the company “many millions” of dollars.

As Facebook’s stock continued to get hammered because of Wall Street worries about the impact in its business, Zuckerberg also said he was “open” to testifying to Congress, even as legislators ever more loudly call for his appearance in hearings.

And that is not all Silicon Valley's most famous mogul said, which is why we are posting the transcript of the 20-minute interview, which was conducted by Kara Swisher and Kurt Wagner of **Recode**.

A short amount of cross-talk about setting up the taping of the interview at the start was removed, but here is the interview (with some small adjustments to explain references made).

Kara Swisher: As you know from us emailing, I’m very interested in tough substantive discussions and questions about this, so that’s why I’ve been so adamant. So let’s just get started. Talk a little bit about the things you announced today. Let’s have you explain each of them very briefly.

Mark Zuckerberg: Sure. At a high level, this is a major breach of trust issue, and our high-level responsibility is to make sure that this doesn’t happen again. So, if you look at the problem, it kind of breaks down into a couple of areas. One is making sure that going forward, developers can’t get access to more data than they should. The good news there is that actually the most important changes to the platform we made in 2014, three or four years ago, to restrict apps like [researcher Aleksandr Kogan’s] from being able to access a person’s “friends” data in addition to theirs.

So that was the most important thing, but then what we did on our platform is we also are closing down a number of other policies. Like, for example, if you haven’t used an app in three months, the app will lose the ability to clear your data without you reconfirming it, and a number of things like that. So, that’s kind of category 1 going forward. And again, the good news there is that as of three or four years ago, new apps weren’t able to do what happened here. So this is largely ... this issue is resolved going forward for a while.

Then there’s going backwards, which is before 2014, what are all the apps that got access to more data than people would be comfortable with? And which of them were good actors, like legitimate companies, good intent developers, and which one of them were scams, right? Like, what Aleksandr Kogan was doing, basically using the platform to gather a bunch of information, sell it or share it in some sketchy way. So what we announced there is, we’re going to do a full investigation of every single app that had access to a large amount of people’s data, before 2014 when we lost out the platform,

and if we detect anything suspicious, we're basically going to send in a team to do a full forensic audit, to confirm that no Facebook data is being used in an improper way.

Well, I don't think it's engineers.

KS: Well, whatever. People [at Facebook].

So, in 2007 we launched the platform.

KS: Yep.

The vision, if you remember is to help make apps social.

KS: Right.

So, the examples we had were, you know, your calendar should have your friend's birthday. Your address book should have your friend's picture. In order to do that, you basically need to make it so a person can log into an app and not just port their own data over, but also be able to bring some data from their friends as well. That was the vision, and a bunch of good stuff got created. There were a bunch of games that people liked. Music experiences, things like Spotify Travel, you know, things like Airbnb they were using it. But there was also a lot of scammy stuff.

There's this values tension playing out between the value of data portability, right? Being able to take your data and some social data ... To be able to create new experiences on the one hand, and privacy on the other hand, and just making sure that everything is as locked down as possible.

You know, frankly, I just got that wrong. I was maybe too idealistic on the side of data portability, that it would create more good experiences. And it created some, but I think what the clear feedback was from our community was that people value privacy a lot more. And they would rather have their data locked down and be sure that nothing bad will ever happen to it than be able to easily take it and have social experiences in other places. So, over time, we have been just kind of narrowing it down. And 2014 was a really big ...

KS: I get that. 2014 you absolutely did that. But I'm talking about the ... You know — and I've argued with [Facebook executives] about this — this anticipation of problems, of possible bad actors on this platform. Do you all

And of course, any developer that isn't comfortable with that, then we'll just ban them from the platform. If we find anything that is bad, then we'll of course also ban the developer, but we will then also notify and tell people, everyone whose data has been affected. Which we're also going to do here.

KS: So that begs the question ... this started off in 2007, 2008 when you were [launching] Facebook Connect, a lot of this stuff started very early, and I remember being at that event where you talked about this. Open and sharing,

and it was helpful to growing your platform, obviously. Why wasn't this done before? What's in the mentality of your engineers of Facebook where you didn't suspect this could be a problem?

Well, I don't think it's engineers.

KS: Well, whatever. People [at Facebook].

So, in 2007 we launched the platform.

KS: Yep.

The vision, if you remember is to help make apps social.

KS: Right.

So, the examples we had were, you know, your calendar should have your friend's birthday. Your address book should have your friend's picture. In order to do that, you basically need to make it so a person can log into an app and not just port their own data over, but also be able to bring some data from their friends as well. That was the vision, and a bunch of good stuff got created. There were a bunch of games that people liked. Music experiences, things like Spotify Travel, you know, things like Airbnb they were using it. But there was also a lot of scammy stuff.

There's this values tension playing out between the value of data portability, right? Being able to take your data and some social data ... To be able to create new experiences on the one hand, and privacy on the other hand, and just making sure that everything is as locked down as possible.

You know, frankly, I just got that wrong. I was maybe too idealistic on the side of data portability, that it would create more good experiences. And it created some, but I think what the clear feedback was from our community was that people value privacy a lot more. And they would rather have their data locked down and be sure that nothing bad will ever happen to it than be able to easily take it and have social experiences in other places. So, over time, we have been just kind of narrowing it down. And 2014 was a really big ...

KS: I get that. 2014 you absolutely did that. But I'm talking about the ... You know — and I've argued with [Facebook executives] about this — this anticipation of problems, of possible bad actors on this platform. Do you all have enough mentality, or do you not see ... I want to understand what happens within Facebook that you don't see that this is so subject to abuse. How do you think about that, and what is your responsibility?

Yeah. Well, I hope we're getting there. I think we remain idealistic, but I think also understand what our responsibility is to protect people now. And I think the reality is is that in the past we had a good enough appreciation of some of this stuff. And some of it was that we were a smaller company, so some of the issues and some of these bad actors just targeted us less, because we were smaller. But we certainly weren't in a

target of nation states trying to influence elections back when we only had 100 million people in the community.

But I do think part of this comes from these idealistic values of openness and data portability and things that I think the tech community holds really dear, but are in some conflict with some of these other values, are in protecting people privately, right? And a lot of the most sensitive issues that we faced today are conflicts between our real values, right? Freedom of speech and hate speech and offensive content. Where is the line, right? And the reality is that different people are drawn to different places, we serve people in a lot of countries around the world, a lot of different opinions on that.

KS: Right, so where's your opinion right now? Sorry to interrupt.

On that one specifically?

KS: Yeah.

You know, what I would really like to do is find a way to get our policies set in the way that reflects the values of the community so I'm not the one making those decisions. Right? I feel fundamentally uncomfortable sitting here in California at an office, making content policy decisions for people around the world. So there are going to be things that we never allow, right, like terrorist recruitment and ... We do, I think, in terms of the different issues that come up, a relatively very good job on making sure that terrorist content is off the platform. But things like where is the line on hate speech? I mean, who chose me to be the person that ...

KS: Well. Okay ...

I have to, because [I lead Facebook], but I'd rather not.

KS: I'm going to push back on that, because values are what we argue about. And companies have values, and they have, you know, the New York Times has a set of values that they won't cross and they make decisions. Why are you so uncomfortable making those value decisions? You run the platform. It is more than just a benign platform that is neutral. It just isn't. I don't know, we can disagree on that, we obviously disagree on this. But why are you uncomfortable doing that?

Well, I just want to make the decisions as well as possible, and I think that there is likely a better process, which I haven't figured out yet. So, for now, it's my job, right? And I am responsible for it. But I just wish that there were a way ... a process where we could more accurately reflect the values of the community in different places. And then in the community standards, have that be more dynamic in different places. But I haven't figured it out yet. So I'm just giving this as an example of attention that we debate internally, but clearly until we come up with a reasonable way to do that, that is our job, and I do well in that.

Kurt Wagner: Hey, Mark, this is Kurt. I'm curious, you talked about going back and trying to figure out if there were other developers that had used your API before 2014, and checking were there any other bad actors that maybe you guys

missed at the time. I'm curious how you actually go about doing that, and if it's actually possible at this point to go out and detect, you know, if someone collected data in 2012, if that data still exists.

Well, the short answer is the data isn't on our servers so it would require us sending out forensic auditors to different apps. The basic process that we've worked out — and this is a lot of what we were trying to figure out over the last couple of days and why it took a little while to get this post out — is we do know all the apps that registered for Facebook and all the people who are on Facebook who register for those apps and have a log of the different data requests that the developer has made.

So we can get a sense of what are reputable companies, what are companies that were doing unusual things ... Like, that either requested data in spurts, or requested more data than it seemed like they needed to have. And anyone who either has a ton of data or something unusual, we're going to take the next step of having them go through an audit. And that is not a process that we can control, they will have to sign up for it. But we'll send in teams, who will go through their servers and just see how they're handling data. If they still have access to data that they're not supposed to, then we'll shut them down and notify ... and tell everyone whose data was affected.

This is a complex process. It's not going to be overnight. It's going to be expensive for us to run, and it's going to take a while. But look, given the situation here, that we had a developer that signed a legal certification saying that they deleted the data, now two years later we're back here and it seems like they didn't, what choice do we have? This is our responsibility to our community is to make sure that we go out and do this. So, even though it's going to be hard and not something that our engineers can just do sitting in their offices here, I still think we have to go do this.

KW: Did you ever think of doing these kinds of audits before 2014? Or even when you got that signed contract from ... or, excuse me, signed statement I guess, from Cambridge Analytica, did you think, "Well, we need to actually go out and check to make sure that they're telling us the truth." Why didn't you do this kind of stuff earlier, or did you think about doing this earlier?

In retrospect, it was clearly a mistake. Right? The basic chronology here is in 2015, a journalist from the Guardian pointed out to us that it seemed like the developer Aleksandr Kogan had sold shared data to Cambridge Analytica and a few other firms. So as soon as we learned that, we took down the app, and we demanded that Kogan, Cambridge Analytica and all the other folks give up the formal, legal certification that they didn't have any other data. And, at the time, Cambridge Analytica told us that not only do we not have the data and it's deleted, but so we actually never got access to raw Facebook data. Right? What they said was, this app that Kogan built, it was a personality quiz app, and instead of raw data they got access to some derived data, some personality scores for people. And they said that they used it in some models and it ended up not being useful so they just got rid of it.

So, given that, that they said that they never had the data and deleted what derivative data that they had, at the time it didn't seem like we needed to go further on that. But look, in retrospect it was clearly a mistake. I'm explaining to you the situation at the time and the actions that we took, but I'm not trying to say it was the right thing to do.

I think given what we know now, we clearly should have followed up, and we're never going to make that mistake again.

I think we let the community down, and I feel really bad and I'm sorry about that. So that's why we're going to go and do these broad audits.

KS: All right, when you think about that idea of ... it's not exactly a "mistakes were made" kind of argument, but you are kind of making that. That idea. I want to understand, what systems are going to be in place, but it's sort of, you know, the horses are out of the barn door. Can you actually go get that data from them? Are you ... It's everywhere, I would assume. I've been told by many, many people that have access to your data, I was thinking of companies like RockYou and all kinds of things from a million years ago that have a lot of your data ... Can you actually get it back? I don't think you can. I can't imagine you can.

Not always. But the goal isn't to get the data back from RockYou. You know, people gave their data to RockYou. So RockYou has the right to have the data. What RockYou does not have the right to do is share the data or sell it to someone without people's consent. And part of the audits and what we're going to do is see whether those business practices were in place, and if so we can kind of follow that trail and make sure that developers who might be downstream of that comply or they're going to get banned from our platform overall.

It isn't perfect. But I do think that this is going to be a major deterrent going backwards. I think it will clean up a lot of data, and going forward the more important thing is just preventing this from happening in the first place, and that's going to be solved by restricting the amount of data that developers can have access to. So I feel more confident that that's going to work, starting in 2014 and going forward. Again, for the last few years already it hasn't been possible for developers to get access to that much.

KS: Let me ask just two more quick questions.

[Here, there is logistical cross-talk with a person on his staff, since Zuckerberg had to head to an employee meeting.]

All right, I'm talking to you while walking over there for Q&A.

KS: All right, the cost of this? And are you going to testify in front of Congress? And if so, when?

You know, I'm open to doing that. I think that the way that we look at testifying in front of Congress is that ... We actually do this fairly regularly, right? There are high-profile ones like the Russian investigation, but there are lots of different topics that Congress needs and wants to know about. And the way that we approach it is that our responsibility is to make sure that they have access to all the information that they need to have. So I'm open to doing it.

KS: What is "open"? Is that a "yes" or a "no"?

Well.

KS: They want you, Mark.

Well look, I am not 100 percent sure that's right. But the point of congressional testimony is to make sure that Congress gets the data in the information context that they need. Typically, there is someone at Facebook whose full-time job is going to be focused on whatever the area is. Whether it's legal compliance, or security. So I think most of the time if what they're really focused on is getting access to the person who is going to be most knowledgeable on that thing, there will be someone better. But I'm sure that someday, there will be a topic that I am the person who has the most knowledge on it, and I would be happy to do it then.

KW: Mark, can you give us a sense of the timing and cost for this? Like, the audits that you're talking about. Is there any sense of how quickly you could do it and what kind of cost it would be to the company?

I think it depends on what we find. But we're going to be investigating and reviewing tens of thousands of apps from before 2014, and assuming that there's some suspicious activity we're probably going to be doing a number of formal audits, so I think this is going to be pretty expensive. You know, the conversations we have been having internally on this is, "Are there enough people who are trained auditors in the world to do the number of audits that we're going to need quickly?" But I think this is going to cost many millions of dollars and take a number of months and hopefully not longer than that in order to get this fully complete.

KS: Okay, last question Mark, and then you can go. How badly do you think Facebook has been hurt by this, and you yourself, the reputation of Facebook?

I think it's been a pretty big deal. The No. 1 thing that people care about is privacy and the handling of their data. You know, if you think about it, the most fundamental thing that our services are, whether it's Facebook or Whatsapp or Instagram, is this question of, "Can I put content into it?" Right? Whether it's a photo or a video or a text message. And will that go to the people I want to send it to and only those people? And whenever there is a breach of that, that undermines the fundamental point of these services. So I think it's a pretty big deal, and that's why we're trying to make sure we fully understand what's going on, and make sure that this doesn't happen again. I'm sure there will be different mistakes in the future, but let's not make this one again.

KS: Yes, let's not. Okay, Mark, I really appreciate you talking to us. KW: Okay, Mark.
KS: Thank you so much, I know you have to talk to your employees ... I'm walking into my Q&A now. All right, see ya.

(THE NEW YORK TIMES)

The New York Times

Mark Zuckerberg's Reckoning: 'This Is a Major Trust Issue'

By Kevin Roose and Sheera Frenkel March 21, 2018

For much of the past week, Facebook has been embroiled in a controversy involving Cambridge Analytica, a political consulting firm with ties to Donald J. Trump's 2016 presidential campaign, and how the firm improperly obtained and exploited personal data from 50 million Facebook users.

On Wednesday, following widespread questions about his whereabouts, Mark Zuckerberg, the chief executive of Facebook, spoke with two New York Times reporters, Sheera Frenkel and Kevin Roose, about the controversy and the steps he was taking to make the social network less prone to abuse.

Below is a transcript of the conversation, edited for length and clarity.

Sheera Frenkel: Did it come as a surprise to you, the user response to the news that Cambridge Analytica had accessed this trove of data?

Mark Zuckerberg: Privacy issues have always been incredibly important to people. One of our biggest responsibilities is to protect data. If you think about what our services are, at their most basic level, you put some content into a service, whether it's a photo or a video or a text message — whether it's Facebook or WhatsApp or Instagram — and you're trusting that that content is going to be shared with the people you want to share it with. Whenever there's an issue where someone's data gets passed to someone who the rules of the system shouldn't have allowed it to, that's rightfully a big issue and deserves to be a big uproar.

Frenkel: It took quite a few days for your response to come out. Is that because you were weighing these three action points that you noted in your post?

Zuckerberg: The first thing is, I really wanted to make sure we had a full and accurate understanding of everything that happened. I know that there was a lot of pressure to speak sooner, but my assessment was that it was more important that what we said was fully accurate.

The second thing is, the most important thing is that we fix this system so that issues like this don't happen again. It's not like there aren't going to be other different kind of things we'll also have to fix. But when there's a certain problem, we have a responsibility to at least make sure we resolve that problem.

So the actions here that we're going to do involve first, dramatically reducing the amount of data that developers have access to, so that apps and developers can't do what Kogan did here. The most important actions there we actually took three or four years ago, in 2014. But when we examined the systems this week, there were certainly other things we felt we should lock down, too. So we're going ahead and doing that.

Even if you solve the problem going forward, there's still this issue of: Are there other Cambridge Analyticas out there, or other Kogans who, when the platform worked a certain way in the past, were there apps which could have gotten access to more information, and potentially sold it without us knowing, or done something that violated people's trust? We also need to make sure we get that under control. That's why we

spent a lot of time figuring out, O.K. here's what it's going to take to do a full investigation of every app that got access to a large amount of information before we changed the platform policies to dramatically reduce the data access that developers had. For any app that we uncover that has any suspicious activity, we're going to go do a full forensic audit, and make sure we have the capacity to do that, to make sure that other developers aren't doing what Kogan did here.

The third thing is, it's really important that people know what apps they've authorized. A lot of people have been on Facebook now for five or 10 years, and sometimes you signed into an app a long time ago and you may have forgotten about that. So one of the steps we're taking is making it so apps can no longer access data after you haven't used them for three months.

But it's also just really important to put in front of people a tool of, here are all the apps you've connected to and authorized, here's an easy way to deauthorize them, to revoke their permission to get access to your activity.

Kevin Roose: Is Facebook planning to notify the 50 million users whose data was shared with Cambridge Analytica?

Zuckerberg: Yes. We're going to tell anyone whose data may have been shared.

Now, there's a question of whether we have the exact record in our systems today of who your friends were on that day when there was access three and a half or four years ago, so we're going to be conservative on that and try to tell anyone whose data may have been affected, even if we don't know for certain that they were. It's likely that we'll build a tool like we did with the Russian misinformation investigation, that anyone can go to it and see if their data was affected by this.

Roose: Do you have a preliminary estimate of how many apps you'll be investigating?

Zuckerberg: It will be in the thousands.
Frenkel: Were those app developers notified that you'll be investigating this

yet?
Zuckerberg: Just when I posted. And we'll be reaching out in the near term.

Frenkel: Are you going to be hiring people to help conduct those investigations?

Zuckerberg: Yes, I would imagine we're going to have to grow the team to work on this.

Roose: You mentioned a contract that developers will have to sign in order to ask anyone for access to broader profile information. What will be the terms of that contract, and what will be the penalties for violating it?

Zuckerberg: So, the important thing there is that it's a high-touch process. The specific point we were trying to make is that it's not going to be some terms of service that a

developer can sign up for just on their computer when developing something. I guess technically, that would be a contract as well.

The point of what we're trying to do here is to create a situation where we have a real person-to-person relationship with any developer who is asking for the most sensitive data. That doesn't mean that — if you're a developer and you want to put Facebook Login on your website, you can do that. If you want to get access to ask people for their religious affiliation, or their sexual orientation, for data that could be very sensitive, we want to make sure we have a clear relationship with those people.

Frenkel: We understood that Cambridge Analytica had reached out to Facebook and asked that its ban on the platform be reconsidered. Are you giving any thought to allowing Cambridge Analytica back in?

Zuckerberg: The first thing we need to do is conduct this full forensic audit of the firm, that they don't have any people's data from our community and that they've deleted anything, including derivative data, that they might have. We're working with the regulator in the U.K. on this, so our forensic audit was actually paused in the near term to cede the way for the ICO there to do their own government investigation. We're certainly not going to consider letting them back onto the platform until we have full confirmation that there's no wrongdoing here.

Roose: There were reports as far back as 2015 that Cambridge Analytica had access to this data set. Why didn't you suspend them then?

Zuckerberg: So, we actually heard, I think it was at the end of 2015 — some journalists from The Guardian reached out to us and told us what you just said. And it was not just about Cambridge Analytica, it was about this developer, Aleksandr Kogan, who had shared data with them.

We took action immediately at that point. We banned Kogan's app from the platform, we demanded that Kogan and Cambridge Analytica and a couple other parties that Kogan had shared the data with would legally certify that they didn't have the data, and weren't using it in any of their operations. They gave us that formal certification. At the time, they told us they never had gotten access to raw Facebook data, so we made that decision.

Frenkel: In retrospect, do you wish you had demanded proof that the data had been deleted?

Zuckerberg: Yes. They gave us a formal and legal certification, and it seems at this point that that was false.

Again, we haven't done our full investigation and audit yet so I can't say definitively that they actually have data. I've just read all the same reports that you have, including in The New York Times, that says that journalists have seen evidence that they have the data, which is a strong enough signal for us to go on, and take action here.

That's the basic driver behind us now needing to go and do a full investigation into any app that had access to a large amount of data before we locked down the platform

policies in 2014. Just having folks tell us that they were using the data correctly, I think, does not satisfy our responsibility to our community to protect their data.

Frenkel: Are you actively looking at some of these dark web data brokers that have been in news reports recently, that say that other independent researchers are potentially trading in this data?

Zuckerberg: Yes, we're investigating that too.

Roose: Are you worried about the #DeleteFacebook campaign that's been going around? Have you seen meaningful numbers of people deleting their accounts, and are you worried that will be a trend?

Zuckerberg: I don't think we've seen a meaningful number of people act on that, but, you know, it's not good. I think it's a clear signal that this is a major trust issue for people, and I understand that. And whether people delete their app over it or just don't feel good about using Facebook, that's a big issue that I think we have a responsibility to rectify.

Frenkel: We're now heading into the 2018 midterms. Could you speak about what Facebook is going to do ahead of the 2018 midterms to make people feel more confident that the platform won't be used this way again?

Zuckerberg: This is an incredibly important point. There's no doubt that in 2016, there were a number of issues including foreign interference and false news that we did not have as much of a handle on as we feel a responsibility to for our community.

Now, the good news here is that these problems aren't necessarily rocket science. They're hard, but they're things that if you invest and work on making it harder for adversaries to do what they're trying to do, you can really reduce the amount of false news, make it harder for foreign governments to interfere.

One of the things that gives me confidence is that we've seen a number of elections at this point where this has gone a lot better. In the months after the 2016 election, there was the French election. The new A.I. tools we built after the 2016 elections found, I think, more than 30,000 fake accounts that we believe were linked to Russian sources who were trying to do the same kind of tactics they did in the U.S. in the 2016 election. We were able to disable them and prevent that from happening on a large scale in France.

In last year, in 2017 with the special election in Alabama, we deployed some new A.I. tools to identify fake accounts and false news, and we found a significant number of Macedonian accounts that were trying to spread false news, and were able to eliminate those. And that, actually, is something I haven't talked about publicly before, so you're the first people I'm telling about that.

I feel a lot better about the systems now. At the same time, I think Russia and other governments are going to get more sophisticated in what they do, too. So we need to make sure that we up our game. This is a massive focus for us to make sure we're dialed in for not only the 2018 elections in the U.S., but the Indian elections, the

Brazilian elections, and a number of other elections that are going on this year that are really important.

Frenkel: The Times reported that [Facebook chief security officer Alex] Stamos will be leaving toward the end of this year. Is there a broader plan for how Facebook is going to structure security on its platform ahead of all these important elections?

Zuckerberg: Sure. One of the important things we've done is, we want to unify all of our security efforts. And you reported on a reorg around Alex Stamos, and I'll say something about him in a second. He's been a very valuable contributor here and was a really central figure in helping us identify the foreign interference with Russia. And I think he has done very good work, and I'm hopeful he'll be engaged for a while here on that.

One of the big things we needed to do is coordinate our efforts a lot better across the whole company. It's not all A.I., right? There's certainly a lot that A.I. can do, we can train classifiers to identify content, but most of what we do is identify things that people should look at. So we're going to double the amount of people working on security this year. We'll have more than 20,000 people working on security and community operations by the end of the year, I think we have about 15,000 now. So it's really the technical systems we have working with the people in our operations functions that make the biggest deal.

The last thing I'd add on this. Take things like false news. You know, a lot of it is really spam, if you think about it. It's the same people who might have been sending you Viagra emails in the '90s, now they're trying to come up with sensational content and push it into Facebook and other apps in order to get you to click on it and see ads. There are some pretty basic policy decisions we've made, like O.K., if you're anywhere close to being a fake news site, you can't put Facebook ads on your site, right? So then suddenly, it becomes harder for them to make money. If you make it hard enough for them to make money, they just kind of go and do something else.

Roose: Is the basic economic model of Facebook, in which users provide data that Facebook uses to help advertisers and developers to better target potential customers and users — do you feel like that works, given what we now know about the risks?

Zuckerberg: Yeah, so this is a really important question. The thing about the ad model that is really important that aligns with our mission is that — our mission is to build a community for everyone in the world and to bring the world closer together. And a really important part of that is making a service that people can afford. A lot of the people, once you get past the first billion people, can't afford to pay a lot. Therefore, having it be free and have a business model that is ad-supported ends up being really important and aligned.

Now, over time, might there be ways for people who can afford it to pay a different way? That's certainly something we've thought about over time. But I don't think the ad model is going to go away, because I think fundamentally, it's important to have a service like this that everyone in the world can use, and the only way to do that is to have it be very cheap or free.

Roose: Adam Mosseri, Facebook's head of News Feed, recently said he had lost some sleep over Facebook's role in the violence in Myanmar. You've said you're "outraged" about what happened with Cambridge Analytica, but when you think about the many things that are happening with Facebook all over the world, are you losing any sleep? Do you feel any guilt about the role Facebook is playing in the world?

Zuckerberg: That's a good question. I think, you know, we're doing something here which is unprecedented, in terms of building a community for people all over the world to be able to share what matters to them, and connect across boundaries. I think what we're seeing is, there are new challenges that I don't think anyone had anticipated before.

If you had asked me, when I got started with Facebook, if one of the central things I'd need to work on now is preventing governments from interfering in each other's elections, there's no way I thought that's what I'd be doing, if we talked in 2004 in my dorm room.

I don't know that it's possible to know every issue that you're going to face down the road. But we have a real responsibility to take all these issues seriously as they come up, and work with experts and people around the world to make sure we solve them, and do a good job for our community.

It's certainly true that, over the course of Facebook, I've made all kinds of different mistakes, whether that's technical mistakes or business mistakes or hiring mistakes. We've launched product after product that didn't work. I spend most of my time looking forward, trying to figure out how to solve the issues that people are having today, because I think that's what people in our community would want.

Follow Kevin Roose and Sheera Frenkel on Twitter: @kevinroose and @sheeraf

(WIRED)

Nicholas Thompson / business

03.21.18 / 09:00 pm

Mark Zuckerberg Talks to WIRED About Facebook's Privacy Problem

Mark Zuckerberg says Facebook will investigate "every single app that was operating" before the company changed its data-handling policies in 2014.
Josh Edelson/AFP/Getty Images

For the past four days, Facebook has been taken to the woodshed by critics, the stock market, and regulators after it was reported that the data-science firm Cambridge Analytica obtained the data of 50 million Facebook users. Until Wednesday, Mark Zuckerberg had stayed silent. On Wednesday afternoon, though, he addressed the problem in a personal Facebook post and laid out some of the solutions he will introduce.

He then gave an interview to WIRED in which he discussed the recent crisis, the mistakes Facebook made, and different models for how the company could be regulated. He also discussed the possibility that another—Russian—shoe could drop. Here is a transcript of that conversation:

Nicholas Thompson: You learned about the Cambridge Analytica breach in late 2015, and you got them to sign a legal document saying the Facebook data they had misappropriated had been deleted. But in the two years since, there were all kinds of stories in the press that could have made one doubt and mistrust them. Why didn't you dig deeper to see if they had misused Facebook data?

Mark Zuckerberg: So in 2015, when we heard from journalists at *The Guardian* that Aleksandr Kogan seemed to have shared data with Cambridge Analytica and a few other parties, the immediate actions that we took were to ban Kogan's app and to demand a legal certification from Kogan and all the other folks who he shared it with. We got those certifications, and Cambridge Analytica had actually told us that they actually hadn't received raw Facebook data at all. It was some kind of derivative data, but they had deleted it and weren't [making] any use of it.

In retrospect, though, I think that what you're pointing out here is one of the biggest mistakes that we made. And that's why the first action that we now need to go take is to not just rely on certifications that we've gotten from developers, but [we] actually need to go and do a full investigation of every single app that was operating before we had the more restrictive platform policies—that had access to a lot of data—and for any app that has any suspicious activity, we're going to go in and do a full forensic audit. And any developer who won't sign up for that we're going to kick off the platform. So, yes, I think the short answer to this is that's the step that I think we should have done for Cambridge Analytica, and we're now going to go do it for every developer who is on the platform who had access to a large amount of data before we locked things down in 2014.

NT: OK, great. I did write a piece this week saying I thought that was the main mistake Facebook made.

MZ: The good news here is that the big actions that we needed to take to prevent this from happening today we took three or four years ago. But had we taken them five or six years ago, we wouldn't be here right now. So I do think early on on the platform we had this very idealistic vision around how data portability would allow all these different new experiences, and I think the feedback that we've gotten from our community and from the world is that privacy and having the data locked down is more important to people than maybe making it easier to bring more data and have different kinds of experiences. And I think if we'd internalized that sooner and had made these changes that we made in 2014 in, say, 2012 or 2010 then I also think we could have avoided a lot of harm.

NT: And that's a super interesting philosophical change, because what interests me the most about this story is that there are hard tradeoffs in everything. The critique of Facebook two weeks ago was that you need to be more open with your data, and now it's that certain data needs to be closed off. You can encrypt data more, but if you encrypt data more it makes it less useful. So tell me the other philosophical changes that have been going through your mind during the past 72 hours as you've been digging into this.

MZ: Well that's the big one, but I think that that's been decided pretty clearly at this point. I think the feedback that we've gotten from people—not only in this episode but for years—is that people value having less access to their data above having the ability to more easily bring social experiences with their friends' data to other places. And I don't know, I mean, part of that might be philosophical, it may just be in practice what developers are able to build over the platform, and the practical value exchange, that's certainly been a big one. And I agree. I think at the heart of a lot of these issues we face are tradeoffs between real values that people care about. You know, when you

think about issues like fake news or hate speech, right, it's a tradeoff between free speech and free expression and safety and having an informed community. These are all the challenging situations that I think we are working to try to navigate as best we can.

NT: So is it safe to assume that, as you went through the process over the past few days, you've been talking about the tradeoffs, looking at a wide range of solutions, and you picked four or five of them that are really good, that are solid, that few people are going to dispute? But that there's a whole other suite of changes that are more complicated that we may hear about from you in the next few weeks?

MZ: There are definitely other things that we're thinking about that are longer term. But there's also a lot of nuance on this, right? So there are probably 15 changes that we're making to the platform to further restrict data, and I didn't list them all, because a lot of them are kind of nuanced and hard to explain—so I kind of tried to paint in broad strokes what the issues are, which were first, going forward, making sure developers can't get access to this kind of data. The good news there is that the most important changes there had been made in 2014. But there are still several other things that, upon examination, it made sense to do now. And then the other is just that we want to make sure that there aren't other Cambridge Analyticas out there. And if they were able to skate by giving us, say, fraudulent legal certification, I just think our responsibility to our community is greater than to just rely on that from a bunch of different actors who might have signals, as you say, of doing suspicious things. So I think our responsibility is to now go and look at every single app and to, any time there's anything suspicious, get into more detail and do a full audit of them. Those, I think, are the biggest pieces.

NT: Got it. We're learning a lot every day about Cambridge Analytica, and we're learning what they did. How confident are you that Facebook data didn't get into the hands of Russian operatives—into the Internet Research Agency, or even into other groups that we may not have found yet?

MZ: I can't really say that. I hope that we will know that more certainly after we do an audit. You know, for what it's worth on this, the report in 2015 was that Kogan had shared data with Cambridge Analytica and others. When we demanded the certification from Cambridge Analytica, what they came back with was saying: *Actually, we never actually received raw Facebook data. We got maybe some personality scores or some derivative data from Kogan, but actually that wasn't useful in any of the models, so we'd already deleted it and weren't using it in anything. So yes, we'll basically confirm that we'll fully expunge it all and be done with this.*

So I'm not actually sure where this is going to go. I certainly think the *New York Times* and *Guardian* and Channel 4 reports that we received last week suggested that Cambridge Analytica still had access to the data. I mean, those sounded credible enough that we needed to take major action based on it. But, you know, I don't want to jump to conclusions about what is going to be turned up once we complete this audit. And the other thing I'd say is that we have temporarily paused the audit to cede to the UK regulator, the ICO [Information Commissioner's Office], so that they can do a government investigation—I think it might be a criminal investigation, but it's a government investigation at a minimum. So we'll let them go first. But we certainly want

to make sure that we understand how all this data was used and fully confirm that no Facebook community data is out there.

NT: But presumably there's a second level of analysis you could do, which would be to look at the known stuff from the Internet Research Agency, to look at data signatures from files you know Kogan had, and to see through your own data, not through the audited data, whether there's a potential that that information was passed to the IRA. Is that investigation something that's ongoing?

MZ: You know, we've certainly looked into the IRA's ad spending and use in a lot of detail. The data that Kogan's app got, it wasn't watermarked in any way. And if he passed along data to Cambridge Analytica that was some kind of derivative data based on personality scores or something, we wouldn't have known that, or ever seen that data. So it would be hard to do that analysis. But we're certainly looking into what the IRA did on an ongoing basis. The more important thing, though, that I think we're doing there is just trying to make the sure government has all the access to the content that they need. So they've given us certain warrants, we're cooperating as much as we can with those investigations, and my view, at least, is that the US government and special counsel are going to have a much broader view of all the different signals in the system than we're going to—including, for example, money transfers and things like that that we just won't have access to be able to understand. So I think that that's probably the best bet of coming up with a link like that. And nothing that we've done internally so far has found a link—doesn't mean that there isn't one—but we haven't identified any.

NT: Speaking of Congress, there are a lot of questions about whether you will go and testify voluntarily, or whether you'll be asked in a more formal sense than a tweet. Are you planning to go?

MZ: So, here's how we think about this. Facebook regularly testifies before Congress on a number of topics, most of which are not as high profile as the Russia investigation one recently. And our philosophy on this is: Our job is to get the government and Congress as much information as we can about anything that we know so they have a full picture, across companies, across the intelligence community, they can put that together and do what they need to do. So, if it is ever the case that I am the most informed person at Facebook in the best position to testify, I will happily do that. But the reason why we haven't done that so far is because there are people at the company whose full jobs are to deal with legal compliance or some of these different things, and they're just fundamentally more in the details on those things. So as long as it's a substantive testimony where what folks are trying to get is as much content as possible, I'm not sure when I'll be the right person. But I would be happy to if I were.

NT: OK. When you think about regulatory models, there's a whole spectrum. There are kind of simple, limited things, like the Honest Ads Act, which would be more openness on ads. There's the much more intense German model, or what France has certainly talked about. Or there's the ultimate extreme, like Sri Lanka, which just shut social media down. So when you think about the different models for regulation, how do you think about what would be good for Facebook, for its users, and for civic society?

MZ: Well, I mean, I think you're framing this the right away, because the question isn't "Should there be regulation or shouldn't there be?" It's "How do you do it?" And some of the ones, I think, are more straightforward. So take the Honest Ads Act. Most of the stuff in there, from what I've seen, is good. We support it. We're building full ad transparency tools; even though it doesn't necessarily seem like that specific bill is going to pass, we're going to go implement most of it anyway. And that's just because I think it will end up being good for our community and good for the internet if internet services live up to a lot of the same standards, and even go further than TV and traditional media have had to in advertising—that just seems logical.

There are some really nuanced questions, though, about how to regulate which I think are extremely interesting intellectually. So the biggest one that I've been thinking about is this question of: To what extent should companies have a responsibility to use AI tools to kind of self-regulate content? Here, let me kind of take a step back on this. When we got started in 2004 in a dorm room, there were two big differences about how we governed content on the service. Basically, back then people shared stuff and then they flagged it and we tried to look at it. But no one was saying, "Hey, you should be able to proactively know every time someone posts something bad," because the AI tech was much less evolved, and we were a couple of people in a dorm room. So I think people understood that we didn't have a full operation that can go deal with this. But now you fast-forward almost 15 years and AI is not solved, but it is improving to the point where we can proactively identify a lot of content—not all of it, you know; some really nuanced hate speech and bullying, it's still going to be years before we can get at—but, you know, nudity, a lot of terrorist content, we can proactively determine a lot of the time. And at the same time we're a successful enough company that we can employ 15,000 people to work on security and all of the different forms of community [operations]. So I think there's this really interesting question of: Now that companies increasingly over the next five to 10 years, as AI tools get better and better, will be able to proactively determine what might be offensive content or violate some rules, what therefore is the responsibility and legal responsibility of companies to do that? That, I think, is probably one of the most interesting intellectual and social debates around how you regulate this. I don't know that it's going to look like the US model with Honest Ads or any of the specific models that you brought up, but I think that getting that right is going to be one of the key things for the internet and AI going forward.

NT: So how does government even get close to getting that right, given that it takes years to make laws and then they're in place for more years, and AI will be completely different in two years from what it is now? Do they just set you guidelines? Do they require a certain amount of transparency? What can be done, or what can the government do, to help guide you in this process?

MZ: I actually think it's both of the things that you just said. So I think what tends to work well are transparency, which I think is an area where we need to do a lot better and are working on that and are going to have a number of big announcements this year, over the course of the year, about transparency around content. And I think guidelines are much better than dictating specific processes.

So my understanding with food safety is there's a certain amount of dust that can get into the chicken as it's going through the processing, and it's not a large amount—it

needs to be a very small amount—and I think there's some understanding that you're not going to be able to fully solve every single issue if you're trying to feed hundreds of millions of people—or, in our case, build a community of 2 billion people—but that it should be a very high standard, and people should expect that we're going to do a good job getting the hate speech out. And that, I think, is probably the right way to do it—to give companies the right flexibility in how to execute that. I think when you start getting into micromanagement, of "Oh, you need to have this specific queue or this," which I think what you were saying is the German model—you have to handle hate speech in this way—in some ways that's actually backfired. Because now we are handling hate speech in Germany in a specific way, for Germany, and our processes for the rest of the world have far surpassed our ability to handle, to do that. But we're still doing it in Germany the way that it's mandated that we do it there. So I think guidelines are probably going to be a lot better. But this, I think, is going to be an interesting conversation to have over the coming years, maybe, more than today. But it's going to be an interesting question.

NT: Last question. You've had a lot of big changes: The meaningful interactions was a huge change; the changes in the ways that you've found and stopped the spread of misinformation; the changes today, in the way you work with developers. Big changes, right. Lots of stuff happening. When you think back at how you set up Facebook, are there things, choices, directional choices, you wish you had done a little differently that would have prevented us from being in this situation?

MZ: I don't know; that's tough. To some degree, if the community—if we hadn't served a lot of people, then I think that some of this stuff would be less relevant. But that's not a change I would want to go back and reverse. You know, I think the world is changing quickly. And I think social norms are changing quickly, and people's definitions around what is hate speech, what is false news—which is a concept people weren't as focused on before a couple of years ago—people's trust and fear of governments and different institutions is rapidly evolving, and I think when you're trying to build services for a community of 2 billion people all over the world, with different social norms, I think it's pretty unlikely that you can navigate that in a way where you're not going to face some thorny tradeoffs between values, and need to shift and adjust your systems, and do a better job on a lot of stuff. So I don't begrudge that. I think that we have a serious responsibility. I want to make sure that we take it as seriously as it should be taken. I'm grateful for the feedback that we get from journalists who criticize us and teach us important things about what we need to do, because we need to get this right. It's important. There's no way that sitting in a dorm in 2004 you're going to solve everything upfront. It's an inherently iterative process, so I don't tend to look at these things as: Oh, I wish we had not made that mistake. I mean, of course I wish we didn't make the mistakes, but it wouldn't be possible to avoid the mistakes. It's just about, how do you learn from that and improve things and try to serve the community going forward?