Subject: Facebook responses to open questions from the 'Committee on Legal Affairs and Consumer Protection' and the 'Committee on the Digital Agenda'

Date: 27 April 2018

1. Cambridge Analytica

How many other Apps are there that operated in a similar way?

Facebook is taking action to determine whether other apps misused people's data. We will (1) investigate apps that had access to a large amount of information before we changed our policies in 2014; (2) conduct full audits of apps with suspicious activity; (3) ban apps that improperly used personally identifiable data; and (4) notify everyone affected, to the extent possible.

This review will involve tens of thousands of apps that had access to a large amount of information before we changed our policies to dramatically limit the amount of data that app developers could request from people on Facebook.

How many German users are affected by other apps?

See above.

How many German users are affected by Kogan?

We understand that 65 people in Germany installed the App "thisisyourdigitallife" throughout its lifetime on the Facebook Platform (i.e., from November 2013 when the app went live to no later than 17 December 2015), which is 0.02% of the App's total worldwide installs.

We further understand that 309,815 other people in Germany were potentially affected, because those people may have been friends of people who installed the App at the time and did not install the App themselves.

This yields a total of 309,880 potentially affected people in Germany, which is 0.3% of the global number of potentially affected people.

These figures may be significantly larger than the actual count of people whose data was shared with Cambridge Analytica by Dr. Kogan, in part because we have not retained data regarding when individual users installed the app. As a result, we have had to include in these figures anyone who installed the app during its lifetime, and anyone who may have been friends on Facebook with any of those people at the time between when the app first became active on the Facebook Platform in November 2013 and when the app's access to friends' data was limited in May 2015.

These figures may also over count because Dr. Kogan may not have shared all of the information he received with Cambridge Analytica. This understanding is consistent with information that has recently been made public that indicates Dr. Kogan only transferred data to Cambridge Analytica relevant to people in the United States. See the following materials published by the UK Parliament House of Commons Digital, Culture, Media and Sport Committee:

- Page 67 of the contract available here: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Chris%20Wylie%20Background%20papers.pdf.
- The written evidence of Dr. Kogan available here: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Written-evidence-Aleksandr-Kogan.pdf

How does Facebook check those Apps internally? What are the criteria? Is there a task force within Facebook? How many people work on this investigation? How long will it take to get final results?

This answer will address (1) the Facebook App Review process that we implemented in 2014, and (2) steps that we are taking to investigate all apps that had access to large amounts of information before we changed our platform in 2014.

- Facebook App Review: In 2014, we implemented an app review process for apps using Facebook Login. Since then, we have reviewed apps that ask for permissions to access, via Facebook Login, data other than public profile information, email address, and list of friends who also used the app. We recently limited the data an app could ask for without review even further to just include to a person's name, profile picture, and email address. We review to ensure that the requested permissions improve the user experience and that the data obtained is tied to an experience within the app. Only if approved following such review can the app ask for a user's permission to get additional data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate. Please see answers below in "Review Process/API section" for a more detailed overview of the App Review process.

- Pre-2014 investigation: In response to recent events we have initiated an internal investigation of 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. We will also tell people affected by apps that have misused their data. In addition to our

own investigations, on 10 April we launched a Data Abuse Bounty Program to help us uncover potential abuse of people's information by third parties. This program will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence.

2. GDPR / Data Protection

While "MFYF" [Make Facebook Your Facebook] serves rather as an image campaign suggesting people have control over their data, the open question is still: what exactly is it that Facebook does with the data?

Facebook was built to connect users to the information and people that matter to them most. Personalisation is the cornerstone of the service we deliver to them. As people use Facebook, they share information and content – whether it's liking a post, sharing a photo or updating their profile. We use this information to give users a better personalised service. For example, we can show users photos from their closest friends at the top of their News Feed, or show articles about issues that matter most to them, or suggest groups that they might want to join.

Data also helps us show users better and more relevant ads, and lets advertisers reach the right people that might be interested in their product or cause. There are a few ways that advertisers can reach users with ads on Facebook:

1. **Information from users use of Facebook**. When using Facebook, people can choose to share things about themselves like their age, gender, hometown, or friends. They can also engage with and like posts, pages, or articles. We use this information to understand what users might be interested in and to show them ads that are relevant to them. For example, if a bike shop has an offer on ladies' bicycles, and wants to reach female cyclists in Berlin, we can show their ad to women in Berlin who liked a Page about bikes. However, these businesses do not know who the users are. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies users. Users can always see the 'interests' assigned to them in their ad preferences, and if they want, remove them.
2. **Information that an advertiser shares with us**. In this case, advertisers bring *us* the customer information so they can reach those people on Facebook. These advertisers might have users' email address from a purchase a user made, or from some other data source. We find Facebook accounts that match that data, but we don't tell the advertiser who matched. In ad preferences users can see which advertisers with their contact information are currently running campaigns – and users can click the top right corner of any ad to hide all ads from that business.
3. **Signals that websites and apps send to Facebook.** Some of the websites and apps users visit may use Facebook tools to make their content and ads more relevant and better understand the results of their ad campaigns. For example, if

an online retailer is using Facebook Pixel, they can ask Facebook to show ads to people who looked at a certain style of shoe or put a pair of shoes into their shopping cart. If users don't want this data to be used to show them ads, they can turn it off in ad preferences. More detail about how we, and others in the industry, use this information can be found here: https://newsroom.fb.com/news/2018/04/data-off-facebook/

What data does FB collect off platform?

Many websites and apps use Facebook services to make their content and ads more engaging and relevant. These services include:

- Social plugins, such as our Like and Share buttons, which make other sites more social and help users share content on Facebook;
- Facebook Login, which lets users use their Facebook account to log into another website or apps;
- Facebook Analytics, which helps websites and apps better understand how people use their services; and
- Facebook ads and measurement tools, which enable websites and apps to show ads from Facebook advertisers, to run their own ads on Facebook or elsewhere, and to understand the effectiveness of their ads.

When users visit a site or app that uses our services, we receive information even if that user logged out or does not have a Facebook account. This is because other apps and sites do not know who is using Facebook. The information we receive includes things like a user's IP address, information about a user's browser and operating system, device identifiers, cookies, and the website or app a user is using.

We require websites and apps that use our tools to tell users that they are collecting and have a sufficient legal basis to do so. We also give users a number of controls over the way this data is used to provide more relevant content and ads, like News Feed preferences, which lets users choose which content they see in their News Feed and how, and ad preferences, which allow users to stop seeing specific advertisers' ads. Users can also opt out of certain ads entirely and control whether their Facebook interests are used to serve them ads.

Does Facebook create shadow profiles?

No, we don't create shadow profiles. We do get information about nonusers in some limited cases as a part of the services we provide. Facebook receives information from websites and apps that choose to download Facebook services (e.g., social plugins, Facebook Login). We will receive this information even if the individual does not have a Facebook account. This is because we can't tell whether the person has a Facebook account – or they are logged in – until we get that information. The time for which we store the data we receive depends on the tool that the app or site is using.

You can find more information about this
here https://newsroom.fb.com/news/2018/04/data-off-facebook.

Will user data be removed after a profile is deleted by a user?

If people decide to leave Facebook and delete their account, then the personal data associated with this account will be deleted from Facebook's servers. Generally, due to technical reasons, deletion processes might take a maximum of 90 days to be fully executed. Furthermore, there are certain exceptions, for example sent messages in an inbox of a friend that are not deleted unless that friend deletes them.

If people delete any content they have posted in their profile, Facebook will also delete this content from its servers. However, like most websites we maintain standard logging for the activities of our servers. Certain log data may refer to content that is ultimately deleted, such as the date and time when a photo was uploaded, but would not include the content of that photo. This log data would be retained and could be associated with a person's account until the entire account is deleted.

Does Facebook plan to start Facial Recognition in Europe and Germany?

We have begun offering people in Europe the opportunity to decide whether or not they wish to enable facial recognition on Facebook, but facial recognition feature is turned OFF by default in the EU. We will only create a facial recognition template for people who decide they want to use this feature.

Facial recognition allows users to manage their identity on Facebook in a number of ways such as by allowing people to be more easily tagged, and to find photos of themselves even when they aren't tagged in them. They may also know when someone is using their image as a profile photo — which can help stop impersonation.

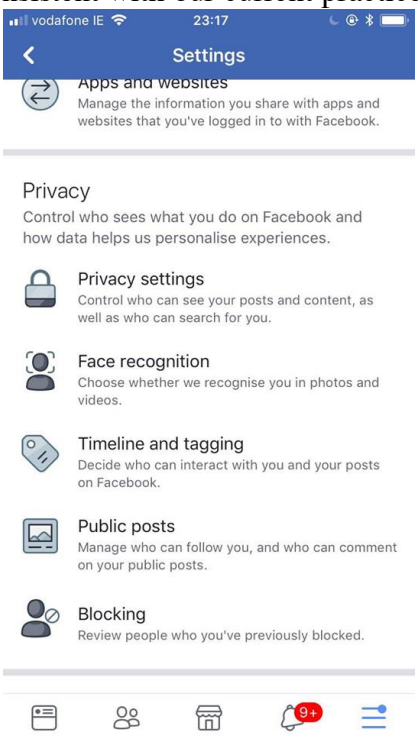
How will Facebook handle pictures in which non-users are being shown or users that have not given their consent to FR?

As part of Facebook's facial recognition features, which have been available in other parts of the world and which we recently announced in Europe, we do not recognise someone depicted in a photo if that person has not explicitly consented to Face Recognition by turning on the Face Recognition setting.

Specifically, when a user explicitly consents to Face Recognition, we create a face template for that user. This template is linked to the user's Facebook user ID. The face template underpins the face recognition process, and Facebook cannot identify a data subject from an image unless it has a face template linked to a Facebook user ID for the data subject appearing in the image.

Users who have chosen to use Face Recognition may withdraw their consent at any time by turning off face recognition in their account settings (see below). When a user

switches off Face Recognition, their face template will be deleted, and will not be available to be used for any purpose. Users who are under the age of 18 cannot opt-in to face recognition, which is consistent with our current practice globally.



What data does Facebook give to third parties (in the past and now)? And does Facebook make money with this?

Facebook's terms of service (clause 2(3)) explain that when users use a third-party application, the application may ask for their permission to access content and information. The user's agreement with the application (including the privacy policy that an app is required to put in place with its users) controls how the application can use, store and transfer that content and information. Third-party app developers operate independently to Facebook in this context. However we nonetheless seek to ensure that they observe appropriate standards. App developers using Facebook Login are subject to the Facebook terms of service. Additionally, we have always imposed the terms of our Platform policy on all developers; and under the changes that we made to our Platform in 2014, we have also subjected apps requesting more than basic information to App Review, as explained below.

Facebook does not tell advertisers who users are or sell information to anyone. That has always been true. We think relevant advertising and privacy are not in conflict, and we are committed to doing both well. When an advertiser runs an ad, we provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we do not share information that personally identifies the user (information such as name or email address that by itself can be used to contact a user or identifies who the users are) unless the user gives us permission. For example, we provide general

demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led a user to make a purchase or take an action with an advertiser.

Our Data Policy describes certain other situations where other entities, including our service providers and research partners, may have access to certain data. The Data Policy also explains that we impose strict data protection limitations on entities that can access data in these ways.

We also respond to valid law enforcement requests for user data. We access, preserve and share user information in response to a legal request (like a search warrant, court order or subpoena) in accordance with our terms of service and applicable law. You can find more information about this here https://transparency.facebook.com/.

How will users get information about what data is stored with third party members?

Facebook users can use the app dashboard that appears within our Settings to see what apps they have previously authorized and to see the info they provide to these apps.

As indicated above, Facebook does not tell advertisers who people are or sell people's information to anyone.

Did users of "thisisyourdigitallife" give consent not just for transferring their own but also their friends data - especially for profiling? How is it possible that Facebook makes people data controllers of their friends?

In line with Facebook's terms in 2013, which people agreed to as a part of creating their Facebook accounts, apps had the capacity to obtain (subject to and consistent with the App users' friends' own privacy settings) some data relating to the installing user's friends. People explicitly accepted these terms in our data policy and saw reminders of this behavior whenever they themselves used apps.

In 2014, after hearing feedback from the Facebook community that people were sometimes worried about sharing information with apps and wanted more choice and control over what personal information apps receive, Facebook made an update to management of the Platform, including:

- Introducing proactive app review;
- Updating Facebook Login to V2, which did not allow apps to ask for detailed information about a person's friends;
- Providing more granular control over permissions.

These changes significantly restricted the data that apps were able to access via Login. Importantly, apps like the one in question here could no longer ask for detailed

information about a person's friends. We also required developers to get approval from us before they could request certain other kinds of data from the users of their app.

Which subsidiaries,
or companies or apps since acquired by Facebook, allow third parties to gain access to user data in a similar way to the Cambridge Analytica cases?

Facebook offers a number of APIs that enable third parties to interact with other Facebook services. As we describe in more detail below, we took action in 2014 – and again this month – to restrict access to data to a number of these APIs so that third parties could no longer gain access to user data in a similar way to the Cambridge Analytica case. More information can be found here:
https://newsroom.fb.com/news/2018/04/restricting-data-access/

We also announced that we are deprecating Instagram's API in July.

(a) For many years, Facebook has made it possible for third parties to access the personal data of its users via Facebook Connect, Open Graph API and other available interfaces, as well as by granting relevant authorization from the respective users. How many and which third party players have received access to the following personal data of respective users from 2008 to 2018?

- E-mail address
- Sexual orientation
- Work history
- Likes (interests, music, movies, books, pages they like etc.)
- Non-public posts
- Private messages
- List of friends
- Other information about friends

(b) Please break this down by year and above-mentioned data category according to:

- Number of third parties
- Type of third parties (categorized by type of app i.e. intended purpose)
- Origin/country of third party: percentages

(c) How many of these third parties have received the data of up to [1000, 10,000, 100,000, 1 million, 10 million, 100 million, more] affected users?

Answers to (a), (b), and (c): As explained above, Facebook is taking action to determine whether other apps misused people's data. We will (1) investigate apps that had access to a large amount of information before we changed our policies in 2014; (2) conduct full audits of apps with suspicious activity; (3) ban apps that improperly used personally identifiable data; and (4) notify everyone affected, to the extent possible.

This review will involve tens of thousands of apps that had access to a large amount of information before we changed our policies to dramatically limit the amount of data that app developers could request from people on Facebook.

Between 2012 and 2018, did Facebook share personal information about users with third parties in any way that extended beyond publicly available features like Facebook Connect, Open Graph API, and other publicly available interfaces? If so, how many third parties were there and what was transferred?

In addition to public APIs, Facebook also has some APIs that are available only to certain partners for specific uses. Generally these APIs provide access to public information, such as to enable news and media organizations to follow breaking news.

Facebook also has device-integrated APIs that enable partners to provide Facebook experiences under partnership agreements. A device-integrated API would be a Blackberry-built Facebook app or an integration that allowed people to call their Facebook friends using their phone. We are working on winding down many of these partnerships. More information is available here: https://developers.facebook.com/blog/post/2018/04/24/new-facebook-platform-product-changes-policy-updates/.

Between 2012 and 2018, did Facebook allow third parties to use personal data from Facebook on the platform in a way that extended beyond publicly known features like data import, linking, analysis, targeting? If so, how many third parties, and in what capacity?

The primary way third parties can obtain identifiable personal data about Facebook users is through the Facebook service (for example, by logging into Facebook and browsing) or through Facebook Platform.

We also work with third parties in certain other situations, such as when third parties provide services to Facebook. Our Data Policy describes these situations and the privacy restrictions that apply to them in more detail.

What personal data about German residents and households did Facebook receive from Acxiom in 2017?

Many businesses work with independent data providers like Acxiom, Oracle Data Cloud (formerly DLX), Epsilon, Experian and Quantium for their marketing efforts. For example, to customize an offer to people who may want a new car, an auto dealer may work with one of these providers to identify and reach those customers.

Facebook has enabled advertisers to use categories that are built by data providers to reach people on Facebook. We call these categories "Partner Categories." For example, a data provider (such as Acxiom) could give Facebook a category that helps us connect advertisers with people on Facebook who are interested in buying a new car. Advertisers

can select that category when running an ad on Facebook. The advertiser does not receive personal information about anyone in the category. Using the new "Ads based on data from partners" control, anyone can choose whether we use these categories to show them ads.

As we announced this past month, we are eliminating our Partner Categories program globally. This process will take place over the next few months, in order to minimize disruption to advertisers and to allow time for them to update their targeting choices. For more information, please see: https://newsroom.fb.com/news/h/shutting-down-partner-categories/.

Why won´t FB implement GDPR worldwide after all?

The GDPR and EU consumer law set out specific rules for terms and data policies which we have incorporated for EU users. The GDPR also contains provisions for the appointment of a lead supervisory data protection authority, which is appropriate within the context of the EU but may not be appropriate worldwide.

We have been clear that we believe everyone who uses Facebook, no matter where they live, deserves strong privacy protections, and so we are offering everyone who uses Facebook the same types of privacy controls and settings that we are building for GDPR.

Data sharing with WhatsApp? Does Facebook plan to change this?

In Europe, WhatsApp has only ever shared data with Facebook (which acts strictly in the capacity as a service provider) to support WhatsApp in areas such as infrastructure, analytics and data hosting. Following the commencement of the GDPR, WhatsApp and Facebook will share data for safety and security purposes to protect our users across the Facebook Company Products. We are not currently sharing WhatsApp account information to improve the product and ads experience on Facebook. As we have said in the past, we want to work more closely with other Facebook companies in the future and we will keep you updated as we develop our plans.

Which currently installed Facebook or other apps can only be installed by users if they agree to the use of their contacts' data? (Contacts stored in address books off Facebook as well as Facebook 'friend" contacts, etc.)

The Facebook, Messenger, and Instagram services are fundamentally about enabling people to connect and share with the people who are important to them. Accordingly, each service maintains a "friend" or "connection" concept that governs what content people are able to see and who they communicate with as a part of each service. People can, of course, choose not to establish friendships. In order to communicate with people, WhatsApp requires people to share their contacts because WhatsApp identifies and connects them to users by connecting to their address book. WhatsApp does not share user's contacts with Facebook. In our other apps, people can choose to import their

contact lists, and doing so improves their ability to make connections on our services, but this is optional.

How does Facebook operate with regards to contact uploads? Clearly legally violating (The Greens)

As a way of finding friends on Facebook, people can choose to sync their contacts and call or text logs to Facebook. This upload is optional; it occurs only if people specifically choose to enable it, and it can be turned off at any time in the app settings.

Further, a user may also request the deletion of all their contacts here which also results in the deletion of all Call/SMS log data (from both Messenger Android and FBLite). Such data is additionally made viewable to the user in Download Your Information.

Is telephone and SMS metadata stored any differently from the data users receive from Facebook when they download their own Facebook information, as described here https://de-de.facebook.com/help/212802592074644?

Facebook provides the information we receive via call and text history sync in Download Your Information.

3. Elections/CA

Did the affected data play a role in the German election? If so, in what way?

We are seeking to investigate how any data obtained via Dr. Kogan's app was used and are consulting with relevant regulators in that regard, including the ICO which is investigating Cambridge Analytica's activities in the UK (it being a UK based company). Our investigation necessarily cedes to that of ICO but once completed we will determine appropriate next steps.

It may be relevant to note that Facebook obtained deletion certifications from Dr. Kogan and GSR, as well as from the third parties they identified as having received Facebook user data obtained via the app. This included a deletion certificate from SCL Limited as Cambridge Analytica's parent company. In that deletion certification SCL Limited confirmed that they deleted all data received from Dr. Kogan after they were contacted by Facebook in December 2015. If that is the case, Cambridge Analytica would have deleted the data far in advance of the German election. Our review of this matter is ongoing. We have hired a forensic auditor to understand what information Cambridge Analytica had and whether it has been destroyed.

Additionally, information that has recently been made public suggests Dr. Kogan only transferred data to Cambridge Analytica relevant to people in the United States. See the following materials published by the UK Parliament House of Commons Digital, Culture, Media and Sport Committee:

- Page 67 of the contract available here: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Chris%20Wylie%20Background%20papers.pdf.
- The written evidence of Dr. Kogan available here: https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Written-evidence-Aleksandr-Kogan.pdf

How much did Facebook earn in 2017 from ads in Germany that were paid for in Russian currency?

It is common for people to buy ads cross-border and so not unusual for there to be ads purchased in many different currencies. We do not publish such a breakdown by currency and consider this information to be commercially confidential. We can confirm that a very small proportion of ads served in Germany are bought in Russian rubles and that we have seen no unusual patterns of spending in this currency.

We have focused our efforts on detecting and removing inauthentic accounts. On 3 April, we took down almost three hundred Pages and profiles controlled by the IRA that were primarily engaged with public debate in Russia and nearby countries. Among the Pages was one Page called Russen in Deutschland, which was in Russian, and had 1336 followers.

There is more information about this takedown on our blog: https://newsroom.fb.com/news/2018/04/authenticity-matters/

Is Facebook aware whether, and if so, which companies used Facebook user data to support election campaigns?

There is no way for Facebook to know where individual election campaigns source their data from. However, entities running election campaigns are covered by German law, and pursuant to our terms all advertisers must comply with applicable laws. Where we are aware they are not meeting their obligations, we will take enforcement action.

Why do you allow to run dark ads? Will you continue to make this possible?

Facebook is committed to making advertising more transparent. In summer 2018, we will roll out a feature called "view ads" globally. This will enable users to see all of the ads every page is running on Facebook at the same time. We hope this will bring greater transparency to ads.

We have also announced a number of efforts to bring even greater transparency to political advertising on Facebook. In October 2017, we announced that only authorized advertisers will be able to run electoral ads on Facebook or Instagram in the U.S. We have now extended that requirement to include "issue ads"— political topics that are being debated. We are working with third parties to develop a list of key issues, which we will refine over time. Once an advertiser completes the process, its political ads will be

shown with a label that says “Political Ad” in the top left corner of the ad, with “paid for by” information next to it. We plan to expand the process to additional countries in the future.

Does this kind of use happen in Germany?

See above.

What is the result of investigation around Russian ads and interference?

On 3 April, we took down almost three hundred Pages and profiles controlled by the IRA that were primarily engaged with public debate in Russia and nearby countries. This was as a result of our continuous efforts to detect and remove inauthentic accounts. Among the Pages was one Page called Russen in Deutschland, which was in Russian, and had 1336 followers.

There is more information about this takedown on our blog:
https://newsroom.fb.com/news/2018/04/authenticity-matters/

4. Review Process/API

How exactly does the Review Process work (vs pre 2014)?

Facebook Login provides an interface through which app developers request permission to seek consent from their users to access certain Facebook data relating to the user. Developers act as independent data controllers regarding the data accessed by their apps, and independently determine the purposes for which, and the manner in which, that data is processed by their app. A list of access permissions which app developers may currently seek from their apps’ users via Facebook Login (subject to App Review and the terms of our Platform policy) are available at: https://developers.facebook.com/docs/facebook-login/permissions. Please note that these current permissions are undergoing review in light of recent events. To be clear, these are permissions which allow app developers to ask users of their app for permission to access their data. Whether or not app developers can in fact access any of that data is dependent on whether the user consents to provide that data.

While app developers act as independent data controllers with regard to the information that users permit them to access, we nonetheless seek to ensure that they observe appropriate standards. This includes by imposing the terms of our Platform policy on all developers and subjecting to App Review apps that request more than basic user data. Throughout the relevant time period and through to today, Facebook’s policies regarding third-party usage of its Platform technologies have prohibited — and continue to prohibit — those third-party app providers from sharing with other parties any user information accessed from Facebook. For example, our Platform policy (which was recently updated to provide greater clarity) imposes the following obligations on app developers:

- 2(4)(a) Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.
- 2(4)(b) Your privacy policy must not modify, supersede, or be inconsistent with Facebook policies. For example, user data obtained from us cannot be transferred to a data broker or sold, even if you disclose this in your privacy policy.
- 2(4)(e) Comply with your privacy policy.
- 2(5) You may use Account Information in accordance with your privacy policy and other Facebook policies. All other data may not be transferred outside your app, except to your service provider (per, Section 3.7) who needs that information to provide services to your app. With the exception of Account Information, you may only maintain user data obtained from us for as long as necessary for your business purpose
- 2(6) Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information identifying a specific person could be inferred or created from it.
- 2(7) Obtain consent from people before using their data in any ad.
- 3(3) Only use friend data (including friends list) in the person's experience in your app.
- 3(9) Don't sell, license, or purchase any data obtained from us or our services.
- 3(10) Don't directly or indirectly transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service. By "indirectly" we mean you aren't allowed to, for example, transfer data to a third party who then transfers the data to an ad network.
- 3(13) If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep Account Information if you have presented your privacy policy within your app.
- 8(4) Request only the data and publishing permissions your app needs to provide a good user experience.

Developers are reminded during the App Review process that they must follow our best practices and must comply with our Platform policy. App Review is required for any app using Login that requests permission to access anything other than name, profile photo and email address. If an app that requests additional permissions is not approved, or does not submit for review, the app cannot obtain access to the additional categories of information. During the App Review Process, we review the permissions requested by the app developer based on the following criteria:

- the access permissions an app is seeking must improve the user experience;
- the data gained from any permission must be tied to a current and direct use in the app;
- the app only requests the permissions it really needs;
- the app makes proper use of any write permissions, i.e., permissions to post content on a user's behalf.

How do you enforce the general technical and legal restrictions on third party access and copying of user profiles using open interfaces (APIs)?

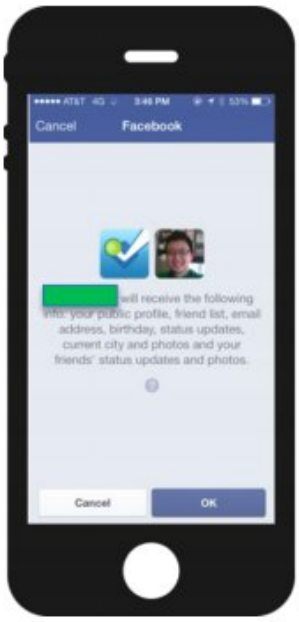
Our Platform policy (which was recently updated to provide greater clarity) contains a number of enforcement provisions which apply after an app has been reviewed and approved, including:

- 7(9): We or an independent auditor acting on our behalf may audit your app, systems, and records to ensure your use of Platform and data you receive from us is safe and complies with our Terms, and that you've complied with our requests and requests from people who use Facebook to delete user data obtained through our Platform. If requested, you must provide us with proof that your app complies with our terms.
- 7(17): We may enforce against your app or website if we conclude you have violated our terms or are negatively impacting the Platform, and we may suspend your app or website, with or without advance notice, while we investigate suspected violations of our terms. We may or may not notify you in advance.
- 7(18): Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

We use a variety of signals in order to determine whether apps are violating our policies, including by reviewing user reports. When we detect violations of our policies we use the enforcement tools available to us - from removing access to our Platform, to taking legal action, to requiring data deletion where it makes sense to do so.

Before changes to interface access to Facebook contacts were made in 2015, was it technically and legally possible for third party providers targeting EU markets to access Facebook users' contacts on German/European user profiles, to the extent that they could also access or copy them on a massive scale?

In November 2013, Dr. Kogan launched his website "thisisyourdigitallife", using Facebook Login on Platform V1. Using Login on Platform V1, apps and websites could only access users' information through Login if those users gave the developer their consent to do so. These apps and websites also had the capacity to obtain (subject to and consistent with the app users' friends' own privacy settings) some data relating to the installing user's friends. Users were told the data points the service wanted to access and could then decide whether to consent or not to that access – per screen similar to those in the screenshots below:



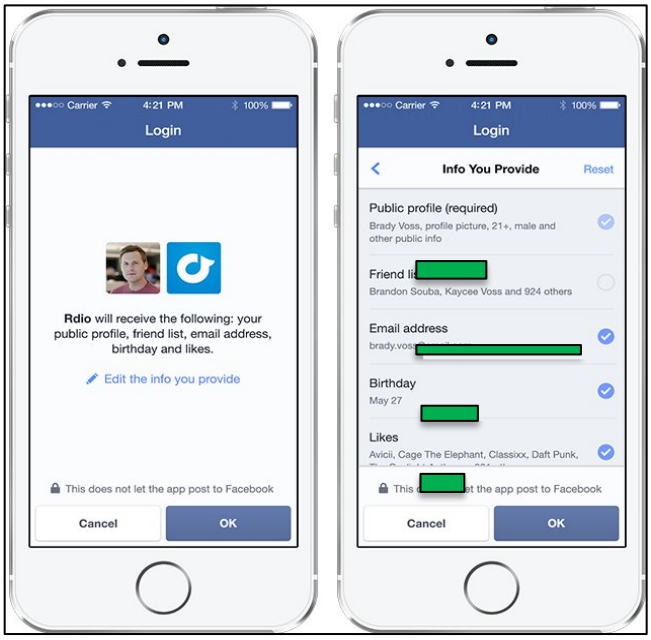
App developers' access was at all times subject to the provisions of our Platform policy. On April 30, 2014, Facebook introduced Platform V2, which removed the ability for users to grant apps such extensive access to their friend's data. Pre-existing apps had a grace period of up to one year (until May 2015) to migrate to Platform V2 and become subject to these changes. Changes to Login included:

1. Introducing proactive app review;
2. Removing apps' ability to ask for detailed information about people's friends.
3. In most cases, restricting, even with the user's permission, the lists of friends to friends who also use the app.
4. Providing more granular control over the permissions apps could be given by users.

The granular controls allowed users to opt-out of providing information on an item-by-item basis. The only compulsory information that a user could not opt-out of providing the app in this way was a selection of information from a users' public Facebook profile (including name and profile picture). If the user did not want to provide the app with this public profile information, the user's choice was to not use the app. These changes significantly restricted the data that apps such as Dr Kogan's were able to access via Login.

For an example of our current Facebook Login flow, please see the screenshots below which show a user using Facebook Login in order to choose to give an app access to specific Facebook information (in this case consisting of profile information that he has chosen to make publicly available on Facebook), while also choosing not to give access

to other information requested by the app (namely his friends list and email address). We have redacted information which could identify this user or the app concerned.



At all times, app developers act as independent data controllers with regard to the information that users permit them to access. However we nonetheless seek to ensure that they observe appropriate standards. App developers using Facebook Login are subject to the Facebook terms of service. Additionally, we have always imposed the terms of our Platform policy on all developers; and under V2 we have also subjected apps seeking access to more than basic user information to App Review, as explained above. Throughout the relevant time period and through to today, Facebook's policies regarding third-party usage of its Platform technologies have prohibited—and continue to prohibit—those third-party app developers from sharing with other parties any user information accessed via Facebook. For example, our Platform policy (which was recently updated to provide greater clarity) imposes the following obligations on app developers:

- 2(4)(a) Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.
- 2(4)(b) Your privacy policy must not modify, supersede, or be inconsistent with Facebook policies. For example, user data obtained from us cannot be transferred to a data broker or sold, even if you disclose this in your privacy policy.
- 2(4)(e) Comply with your privacy policy.
- 2(6) Delete all of a person's data you have received from us (including friend data) if that person asks you to, unless you are required to keep it by law, regulation, or separate agreement with us. You may keep aggregated data only if no information identifying a specific person could be inferred or created from it.
- 2(7) Obtain consent from people before using their data in any ad.
- 3(3) Only use friend data (including friends list) in the person's experience in your app.

- 3(9) Don't sell, license, or purchase any data obtained from us or our services.
- 3(10) Don't directly or indirectly transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service. By “indirectly” we mean you aren’t allowed to, for example, transfer data to a third party who then transfers the data to an ad network.
- 3(13) If you stop using Platform, promptly delete all user data you have received from us (absent explicit consent from people). You can keep Account Information if you have presented your privacy policy within your app.
- 8(4) request only the data and publishing permissions your app needs to provide a good user experience.

Our Platform policy also contains a number of enforcement provisions which apply after an app has been reviewed and approved. These provisions include:

- 7(9): We or an independent auditor acting on our behalf may audit your app, systems, and records to ensure your use of Platform and data you receive from us is safe and complies with our Terms, and that you've complied with our requests and requests from people who use Facebook to delete user data obtained through our Platform. If requested, you must provide us with proof that your app complies with our terms.
- 7(17): We may enforce against your app or website if we conclude you have violated our terms or are negatively impacting the Platform, and we may suspend your app or website, with our without advance notice, while we investigate suspected violations of our terms. We may or may not notify you in advance.
- 7(18): Enforcement is both automated and manual, and can include disabling your app, restricting you and your app’s access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

We use a variety of signals in order to determine whether apps are violating our policies, including by reviewing user reports. When we detect violations of our policies we use the enforcement tools available to us - from removing access to our Platform, to taking legal action, to requiring data deletion where it makes sense to do so.

We have recently put additional protections in place on Facebook Login. Access to a person's list of friends who use the app now requires review. Additionally, we are going even further and protecting sensitive permissions, so access to check-ins, likes, photos, posts, videos, Events, and Groups, will require prior approval by Facebook. We will also no longer allow apps even to ask their users 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. We have also 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.

5. Competition

Facebook is a social media monopolist and needs to be broken up.

The statement does not acknowledge the intense competitive pressure that we face. While Facebook is popular, the reality is that we are still just one small part of how people connect with friends, family and the world around us. In Germany, half of internet users have chosen not to use Facebook, while the other half has, often alongside other free communications apps. Hundreds of other popular messaging services and photo and video sharing apps are widely available and free to use. The average person now uses eight different services to connect and communicate (twice as many as five years ago).

Companies, big and small, also have more options than ever when it comes to advertising – from established TV and radio platforms, to newer platforms such as Spotify, Google, Twitter, YouTube, Amazon, or Snapchat to name just a few.

In fact, in this highly competitive environment Facebook represents a small part (6%) of this diverse and expanding $653bn global media ecosystem and our success in this ecosystem has been built on helping small businesses – many of whom could never have previously afforded newspaper or TV ads – to cost-effectively reach a global audience. Today 1 in 3 German businesses are using Facebook (1.2 million total), and over 270 million people from around the world are using Facebook to connect to a small business in Germany.

Is Facebook willing to allow interoperability (in the light of the GDPR)?

Yes. Facebook has offered interoperability through its APIs and portability through its Download Your Information tool, both of which have enabled people to take their data to other apps and services.

In response to the GDPR, we announced on 28 March that we are launching improvements to the Download Your Information tool, such as providing easier access to more information that people share with Facebook. We stated that "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." As a part of this change, we are making it easier for people to customise their data exports and enabling them to download data in a machine-readable format.

However, as we have seen in the recent discussion around third parties misusing information they received from our APIs, interoperability carries risks as well, and companies like ours have taken action to better protect the information that is accessible through APIs. To address these risks, we need collaboration across the tech industry to identify an approach that provides user-friendly interoperability, while also protecting the

data that people share with tech services. A viable solution must also protect companies' intellectual property and work for companies of all sizes.

Would Facebook allow interoperability with other social networks?

Yes. See above.

6. Algorithms

Would a project like Datenspende be possible with FB?

We understand the goal of the Datenspende project was to improve transparency and accountability about Google's search results. At Facebook, we are also committed to working both internally and with external partners to ensure greater transparency and accountability of algorithms. We would be happy to discuss these efforts in more detail with the **Datenspende** team.

At Facebook, we use algorithms to improve our products, offer customized user experiences, and help us achieve our mission of building a global and informed community. Of note, we use algorithms to help organize the content people choose to see in their News Feed (by "friending" someone or following a Page or joining a Group). To improve transparency and accountability, we have a number of efforts underway:

- **We are publishing more information about how our algorithms work.** For example, we publish a series of blog posts called News Feed FYI that explains how News Feed works, highlights major updates to News Feed and details the thinking behind them. We also recently launched a new website feature called "Inside Feed' that provides an even deeper dive into the way systems work and the way to evaluate changes.
- **We are increasing users' control over their experience.** On News Feed, users have total control over who they choose to friend and follow — that's what determines what's in their News Feed — but there's also a tool to let users select people to "See First" so they are always at the top of their Feed. We are committed to building more such controls in the future.
- **We are promoting a series of AI educational initiatives and campaigns** to help people learn about the technology that underlies our various products and features, which includes AI and Machine Learning. A good example of this is the video that our FAIR (Facebook Artificial Intelligence Research) Lab published to explain what Machine Learning algorithms are and how we use them at Facebook.
- **We have a dedicated team working specifically on the intersection of AI & Ethics**. This includes conducting research and study ethical questions posed by AI, namely transparency and explainability, but also fairness, discrimination, etc.
- **We are working with external stakeholders on the ethical issues raised by algorithms and AI.** We are part of various multistakeholder consortia working on issues of algorithmic fairness, transparency and accountability. These include:

- The Partnership on AI, a collaborative and multi-stakeholder organization that we co-founded and that was established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society.
- AI4 People, the first global forum in Europe on the social impacts of artificial intelligence. This consortium, comprised by representatives of governments, European institutions, civil society organisations, and leading businesses, is tasked with designing a European ethical framework for a "good AI society", and to develop a Corporate Charter of ethical principles for tech firms working with AI and related technologies, and a Global Mark of Compliance, which will be a quality certification mark certifying ethically sound uses of AI.

7. Other Questions

Does Facebook listen to phone calls?

No. Call and message logs are part of an opt-in function for users who use Messenger or Facebook Lite on the Android operating system, but this information includes the fact that a call occurred — not its content. Syncing contact books and call and message logs is optional — it must be explicitly enabled by each user — and it helps you find other people and stay connected with them. On 4 April, we announced that we would delete all call and SMS logs older than one year, and, in the future, we will only retrieve the information necessary to offer this function and nothing exceeding that data, like the time of the call.

Facebook does not use the user's telephone microphone to obtain information for ads. A few recent articles have suggested that we listen to people's conversations to show them relevant advertising. That is not the case. We show ads based on people's interest and other profile information – not on the basis of what they talk about.

We only access users' microphones if they have given us permission and when they actively use certain features which require audio function. This might include recording a video or the use of optional features to integrate music or other audio capabilities into the user's status updates.

Does Facebook know whether there are German companies who have received or stored user data that could be used in a similar manner to that described here by SAP in 2014 https://blogs.sap.com/2014/08/20/social-intelligence-using-sap-hana/? If so, what data, how, and when?

There are many application developers in Germany who connect their applications with Facebook. We expect them all to respect our terms of service and to use data only for permitted purposes.

Which German companies use Facebook apps to store Facebook user data in order to create profiles, either anonymized or not anonymized?

German companies are fully covered by German law, and we have an expectation they meet their legal and policy obligations — and our terms make that clear. Where we are aware they are not meeting their obligations, then we will take enforcement action.

To help us uncover potential abuse of people's information by third parties, on 10 April Facebook launched a Data Abuse Bounty Program. This program will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence. Just like the bug bounty program, we will reward based on the impact of each report. While there is no maximum, high impact bug reports have garnered as much as $40,000 for people who bring them to our attention.

We'll review all legitimate reports and respond as quickly as possible when we identify a credible threat to people's information. If we confirm data abuse, we will shut down the offending app and take legal action against the company selling or buying the data, if necessary. We will pay the person who reported the issue, and we'll also alert those we believe to be affected. For more information, you can visit: facebook.com/data-abuse

How many of them are usable if the user only agrees to limited use of their data?

Our terms make it clear that app developers should only ask for data that is necessary. As part of our App Review process, we ensure that the requested permissions improve the user experience and that the data obtained is tied to an experience within the app. Only if approved following such review can the app ask for a user's permission to get additional data.

How many of them even offer the option not to use certain requested data?

See above.