Written Responses to EDRi Questions

1. Facebook's new policy is based on opt-in for facial recognition being applied to inform Facebook users of their faces appearing on photos uploaded by other users. Does this mean that Facebook will index all facial profiles on any photo uploaded, regardless of any consent by any person depicted? Please answer with "yes" or "no" and explain.

No, Facebook does not index all facial profiles – or 'create and maintain a face template', in our terminology – on any photo uploaded regardless of consent by any person depicted. Over the past two months, we rolled out a notice to every Facebook user in Ireland asking if they would like to participate in face recognition features for use on Facebook; we only create a face template for each of these users if he or she explicitly consents.

At that point, we use the person's profile photo and images he or she is tagged in to create a face template for him or her. This template is linked to the user's Facebook user ID. Facebook does not use face recognition to identify a person from an image unless that image matches a face template linked to a Facebook user ID, which would only be created if the person chose to enable face recognition.

1b. More specifically, will Facebook refrain from analysing any photograph uploaded by any user for biometric data about persons depicted on those photos until it has received an opt-in by every person depicted on those photos? Please answer with "yes" or "no".

When users upload images to share on Facebook, Facebook will analyse images and videos to detect whether they contain human faces. If they do, then Facebook will determine whether any of those faces correspond to a pre-existing face template (which are only created with explicit consent of the user). These initial steps do not involve the analysis or processing of biometric data. Facebook will only identify and process biometric data for those individuals within a photo who have opted-in to our face recognition technology for use on Facebook. Indeed, the identification process will

simply fail if a person's face recognition setting is off because we have not created a reference template for that person.

So, although as described above, we do analyse the photograph, we do not analyse biometric data about persons depicted in photographs unless they have explicitly consented to this processing. Indeed, GDPR specifically classifies information as biometric data only if the processing of that data "allow or confirm the unique identification of [a] natural person" (emphasis added). Facebook only uniquely identifies an individual depicted in a photograph using face recognition (i.e., process biometric data) if we have a face template for that individual (created only in respect of users who have face recognition enabled).

In general, we note that GDPR permits the processing of biometric data under several different legal bases, not only consent (as anticipated in your question), such as to protect the vital interests of the data subject or where necessary for reasons of substantial public interest. If in the future Facebook relied on other legal bases for processing of face recognition data, we would of course, do so only in a way that fully conformed with our legal obligations.

2. You state the following: "Second, we'll ask people who've previously chosen to share their political, religious, and "interested in" information in their profile to check that they want to continue to share it."

Does the above mean that any of the above data will be deleted if Facebook does not receive an explicit consent to retain it? Please answer with "yes" or "no".

If "yes", what will be the cut-off date before Facebook starts deleting such data?

Yes, if we do not have explicit consent from people to retain the information they chose to add to these profile fields, it will be deleted from their profile fields and from our servers.

As laid out in the question, if people have chosen to share political or religious views, or whom they are “interested in”, on their profile, as part of our GDPR “user engagement experience” we’ll ask if they want to continue sharing this information with others on Facebook and for it to be used to personalise product experiences on Facebook (e.g. to suggest a Facebook page or a Facebook group).

2.b If by “sharing” it is meant that the scope of the discontinuation is limited to sharing with other Facebook users and/or Facebook affiliates, how does Facebook consider that this complies with the requirements of art. 9 GDPR for processing these special categories of data?

The discontinuation is not limited to sharing with other Facebook users / affiliates; if people do not wish to consent to Facebook's processing of their special category data, their information is deleted and not further processed by Facebook Ireland.

Our consent flow for use of sensitive personal data (“special categories of data”) complies with Art. 9 of the GDPR. Specifically:

- We comply with Art. 9 by asking individuals for explicit consent to share their political, religious, or “interested in” information in their profile fields and for it to be used to personalise product experiences on Facebook.
- If people decide not to provide explicit consent and to remove the information, the information is deleted.
- If people choose to provide explicit consent to continue to share the information, they also select with whom they want to share it with on Facebook, which can be anything from public, to friends, to 'only me'. Their selected audience can be amended at any time, and they can delete or amend the information as they wish.
- Finally, again, this special category profile information is not used for the purpose of serving targeted advertisements. It is, however, used to personalise product experiences on Facebook (e.g. to suggest a Facebook page or a Facebook group), as described in

the user experience through which users' may give their explicit consent.

3. Privacy International created a new Facebook profile to test default settings. By default, everyone can see your friends list & look you up using the phone number you provided. This is not what proactive privacy protections looks like. How does this protect users by design and by default?

As part of our recent privacy reviews, we have already suspended the ability to search for people by phone number in the Facebook search bar. Prior to this, we had permitted people to look up phone numbers on Facebook, and also gave them the choice to opt-out of this if they wished to. We have shut down this tool so that look-ups are no longer permitted.

More generally, we develop our approach to settings in a way that is privacy protective and that also recognises that people join Facebook specifically in support of their goal of connecting with others. For example, we believe that knowing whether you have mutual friends with someone is an important signal in deciding whether a friend request — that is, a request to connect with you and access information that you have shared only with friends — that you receive is legitimate. We hope that people will scrutinise friend requests if they note that they do not share any friends with the requester. However, we realise that we cannot share information about mutual friendships unless a person's friend list is publicly visible.

Of course, people can always control the audiences that see the information they choose to share. They can also control the audience for their friend list itself. Specifically, we offer everyone a granular control which they can use to tailor who can see their list of friends -- ranging from public to friends to a customised audience, or 'only me'. This setting is easily accessible from your Settings and in-line when viewing your own friends' list.

We've updated our Settings and Privacy Shortcuts so people can easily access their information, understand how it is shared on Facebook, and make the privacy choices that are right for them.

4. According to your notification, a "small number of people who logged into 'This Is Your Digital Life' also shared their own News Feed, timeline, posts and messages which may have included posts and messages from you". Why was this not notified to the appropriate national authorities immediately? Are other apps also able to share / receive messages from me?

The people who shared their messages and posts with Kogan's app expressly consented to do so after a clear notification. Users were not able to provide apps with access to their friends' NewsFeed or Message inbox. Because access to NewsFeed and Message Inbox only occurred with the authorisation of the user, there was no unauthorised access to data.

With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their newsfeed.

5. If a similar situation to the one involving Cambridge Analytica were, despite your efforts, to arise again, who would be responsible, Facebook Inc or Facebook Ireland?

Facebook did not permit or agree to the transfer of Facebook user data obtained through the app by Dr. Kogan onward to Cambridge Analytica. Any onward data sharing that happened was in violation of Facebook's Platform Policy, and the potential misuse of that data by Dr. Kogan and Cambridge Analytica is being investigated on an ongoing basis both by Facebook and responsible data protection authorities. Accordingly, while we have taken steps to make it harder for third parties to misuse Facebook's systems in the future, we consider that Dr. Kogan, Cambridge Analytica, and their related parties are responsible in the first instance for what happened in this case.

With regard to Facebook's own data processing (or processing in respect of which it is the responsible entity under applicable law), Facebook Ireland is

the responsible entity for individuals based within Europe, and Facebook, Inc. is the responsible entity for those individuals based outside Europe.

6. Why do privacy settings continue to only focus on what friends can & can't see? If the recent FB scandal has showed one thing, it is that FB's ad policies have far-reaching consequences for users' privacy. When are you going to treat ad settings as privacy settings?

While we believe it is important to give people control over who sees what they share, we do treat ads settings as privacy settings. We've recently updated our Settings tool to make it even easier for people to access their privacy settings, including for ads. In fact, the Privacy Shortcuts tool that we recently launched has an entire section devoted to advertising controls.

Among the ads settings we offer is the Ad Preferences tool, which is directly accessible from our new centralised Settings and Privacy Shortcuts, and includes the following controls:

- Manage Preferences
- See and delete advertisers a user interacted with
- Manage whether FB can show ads based on the following profile fields: relationship status, employer, Job title, education
- Decide whether FB can show ads based on data from partners
- Decide whether FB can show ads based on the user's activity on Facebook Company Products that he/she sees elsewhere
- Decide who can see ads that include the user's social actions
- Hide advertisement topics

This tool also includes clear information about how advertisement works on Facebook:
https://www.facebook.com/ads/about/?entry_product=ad_preferences

These controls can also be accessed via every ad a user sees on the platform.

7. The GDPR includes new provisions on profiling and automated decision-making. How are you going to change your ad targeting practices to be compliant?

Facebook does not carry out any automated decision-making with legal (or "similarly significant") effects pursuant to Article 22 of the GDPR. If Facebook were to carry such type of automated decision-making in the future, it would comply with the requirements of Article 22 of the GDPR. The Article 29 Working Party has clearly established in its guidelines that, "In many typical cases, the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'"

We are transparent in our Data Policy about the type of data we collect, and how it is used, as part of the Facebook service.

8. The Economist recently reported on how difficult it is for Europeans to download their personal data from Facebook, and Mark Zuckerberg's testimony described your systems as more transparent than they actually are. How and when, if at all, do you plan to address these issues?

Download Your Information or "DYI" tool is Facebook's data portability tool. It was first launched in 2010 to let people download many types of information that we maintain about them, with a focus on data that a person may wish to bring with them to another online service, and we have upgraded it in preparation for GDPR. Users now are able to select the data they want to download, as well as the date range, the format of the file (HTML or JSON) and the quality of the file. The data in DYI includes all of the data each user has provided to us, as per the requirements set out under the GDPR.

In preparation for the GDPR we've also introduced a new Access Your Information ("AYI") tool.

With AYI, people can access and manage (edit or delete) their data. This new tool is, like DYI, structured to show you (1) Your Information and (2) Information about you.

These updated tools make it much easier to access, delete, manage, and download your data. We are continuing our efforts to give people more transparency and control over their data.

We have also just announced our plans to build a new tool called 'Clear History'. This feature will enable people to see the websites and apps that send us information when people use them, delete this information from their account, and turn off our ability to store it associated with their account going forward**.**

9. You claim to offer a way for users to download their data with one click. Can you confirm that the downloaded files contain all the data that Facebook holds on each user?

You claim to offer a single place to control your privacy. This does not seem to include ways to opt out of ad targeting or to avoid being tracked outside Facebook. Will you offer a single place where users can control every privacy aspect of Facebook, even for people who have no Facebook account?

We do offer a single place to manage your privacy settings. Specifically, we updated our Settings for GDPR to make it easier to find privacy and other controls in one place. And we also launched a new Privacy Shortcuts tool that provides centralised access to the most important privacy controls.

Like many ad-supported services, advertising is central not only to our ability to operate Facebook, but to the core service that we provide, so we do not offer the ability to disable advertising altogether. But our privacy options include industry-leading controls over advertising — including the ability to opt out of seeing ads based on certain interests or to turn off ads based on apps and websites you visit off of Facebook.

10. The GDPR gives individuals the right to access and verify their profiles, including marketing profiles based on so called derived data (data that were not disclosed by the user but interpreted from his/her behaviour). Is Facebook going to give its users full access to their marketing profiles? Please answer with "yes" or "no" and explain.

Yes. In our Ads Preferences tool, people on Facebook can access and manage the ad targeting interests associated with their user account.

11. Speaking about derived data and marketing profiles, does Facebook process for marketing purposes any data that reveal (directly or indirectly) political opinions of its users? Please answer with "yes" or "no" and explain.

No. Facebook does not process data about any user's political opinions for marketing purposes in the EU.

If a Facebook user 'likes' the Facebook Page of a political party/parties or a political representative/s, which would allow the owner of the Page to see who liked their Page, Facebook does not take that as an indication of their political opinion, but rather an interest in the topic represented by the Page. Additionally, we do not give advertisers the personal information (e.g. name and email address) of people who see their advertisements on Facebook, unless person explicitly directs us to do so.

Also, where an individual provides explicit consent to Facebook's sharing and use of their political opinion as published in their profile for product personalisation (e.g. to suggest a Facebook page or a Facebook group), this data will not be used to inform advertising targeted to that user.

12. Do Facebook apps use smartphone microphones in any way, without this being made clear to the user? If this were to happen, would you consider that lawful?

Facebook does not use your phone's microphone to inform ads or to change what you see in News Feed. Some recent articles have suggested that we must be listening to people's conversations in order to show them relevant ads. This is not true. We show ads based on people's interests and other profile information – not what you're talking out loud about.

We only access your microphone if you have given our app permission and if you are actively using a specific feature that requires audio. This might include recording a video or using an optional feature we introduced two years ago to include music or other audio in your status updates.

13. Facebook has voluntary agreements with the Swedish intelligence services to share data. How do you reconcile that with the GDPR?

The Swedish intelligence agency has no special relationship with Facebook, and our response to law enforcement access requests fully complies with applicable laws.

We take seriously our responsibility to maintain the safety and security of our platform, and the privacy of those using it, and are committed to being transparent in the way that we do this. We also recognise that there are many situations where it is in the interests of people using our service that their governments carry out an investigation into suspected criminal activity.

We publish details of content restrictions made pursuant to local law, as well as details of our process for handling these requests, in our Transparency Report.