Taking control of personal information on social media platforms: Information and guidance for the public

Background

In March 2017 the ICO announced a broad investigation into the use of personal data and analytics by political campaigns, parties, social media companies and other commercial actors. We are currently investigating 30 organisations, including Facebook.

One part of this investigation is looking at how data was collected from a third party app on Facebook called "thisisyourdigitallife" and shared with an organisation called Cambridge Analytica. Facebook recently confirmed that information relating to up to 87 million people was captured by the app, with approximately 1 million of these people being UK citizens.

So how do I find out if my details were captured by the "thisisyourdigitallife" app?

On Monday 9 April 2018 Facebook notified all those whose details were involved via a message on their Facebook Newsfeed.

If my details were involved do I need to tell someone or complain?

Not at this stage. As part of our formal investigation we have requested and seized a great deal of information. We are currently progressing a number of lines of inquiry, including if Facebook has complied with their legal obligations. We don't currently need further information from those whose personal information may have been involved, but we are here to help people to protect their personal information and will be updating this factsheet to help keep people informed.

Would you recommend I delete my social media accounts?

The decision whether to delete a social media account is a personal one for each user, but we would certainly encourage all users of social media platforms to review their privacy settings to make sure they are comfortable with the way their information is being used and shared.

As well as telling people if their personal information was harvested by the "thisisyourdigitallife" app, Facebook are also notifying people, via each person's Newsfeed, which apps they are using. It is very important to note that deleting/removing one of these apps, or deleting your Facebook account, does not automatically delete any data held on the app. Specific steps need to be taken within each app to request the deletion of any personal information it may hold.

Those responsible for social media platforms have a continuous responsibility to earn and maintain the trust and confidence of their service users. As the UK's information rights regulator we will continue to act in the interests of UK citizens by holding those responsible for processing personal data to account and by progressing our investigation into this matter as quickly as possible. Any criminal or civil enforcement action our investigation leads to will be vigorously pursued.

So how can you help me if I want to keep using social media whilst being confident my personal information is only being used in ways I'm comfortable with?

The privacy settings on social media apps and websites should give you control over how your personal information is used. We always advise those who use social media to check their privacy settings before using a particular service and to review them regularly, particularly after any new settings are introduced.

In common with some other Data Protection Authorities we have produced the following guide to help explain how to control the way social media platforms use and share personal information for advertising and other purposes. We hope this guide is helpful, but please do call our helpline on 03031231113 if you would like any further advice.

What is social media?

Social media refers to a variety of online internet applications that enable you to create your own content and interact with other users. Examples of social

media providers are Facebook, Google, Instagram, LinkedIn and Twitter. Users of social media can interact with other users in many ways including by:

- Creating a public profile which may include your interests, hobbies and your current activities.
- Sharing your photos, videos and posts.
- Sharing links to content you are interested in which has been produced by third-parties (such as sharing a news article).
- Commenting on photos, videos and links shared by your friends and third-parties.
- Interacting with third-party applications and providing your personal data to these third-party applications.

What is micro targeting and how do advertisers use it?

Micro targeting is a form of online targeted advertising which analyses personal data to identify the interests of a specific audience or individual in order to influence their actions. Micro targeting may be used to offer a personalised message to an individual or audience using an online service such as social media.

Micro targeting may determine what and how relevant content is delivered to an individual online and is sometimes used to market goods or services and for political marketing. For example, if you express an interest in the social network presence of a certain political party or ideology, personalised advertisements related to that party or ideology may be displayed to you.

The main benefit of micro targeting to advertisers and individuals is that advertisements displayed to individuals will be more relevant and personalised.

Micro targeting works through the use of electronic tools including Cookies, 'Social Plugins' and 'Tracking Pixels'. These electronic tools typically track your browsing habits, likes and social interactions across the internet in order to build up a profile about you. This profile is used to tailor advertisements to your specific interests. Social media providers may include these electronic tools within their environments and on other websites interested in audience interactions and engagement.

Individuals may be targeted **both** by social media providers and third-parties operating on social media. For example, if you are researching buying a new car, you may receive micro targeted advertisements from third-party car

manufacturers, organisations selling cars, or organisations selling car insurance products based on your research activities.

Using your privacy preferences to limit micro targeting on social media

Social media providers offer a suite of tools to assist users in tailoring their interaction and information sharing when using social media, including the ability to limit micro targeting. These tools are typically offered under headings such as "**Settings**" or "**Account Settings**".

This guidance outlines how you can view, update and amend your privacy settings on:

A. Facebook;
B. Google;
C. Instagram;
D. LinkedIn; and
E. Twitter

For other social media you may use, you should familiarise yourself with settings that may be adjusted according to your preferences. Note that with the introduction of the General Data Protection Regulation ("**GDPR**") on 25 May 2018, the location, formatting and/or choice of settings available to you on social media may be updated. Should you have any queries about how to adjust your privacy settings or exercise your advertising preferences, you should contact the provider of the social media you are using.

Protecting your privacy online

When signing-up for and using social media, you should carefully consider the personal data you share on social media and with social media providers as well as reviewing the privacy policy, the terms of use of that social media service and information provided about cookies. In particular, the privacy policy and cookies information available on the service should inform you how that social media service is using your personal data and for what purpose(s).

You should also regularly review your personal data that may be collected on an ongoing basis by and on social media, including reviewing apps that make use of social media log-in services or ask for permissions to access your social media profile and your personal data.

It is advisable to regularly review and re-visit privacy settings and controls of any social media service that you are using in order to ensure that you exercise your preferences to control the way your personal data is processed online. This includes reviewing both your advertising settings / preferences and the permissions you give to third-party apps that make use of your personal data associated with your social media profile.

If you remove or delete an app on your phone, this does not necessarily mean that the app deletes personal data it has already collected about you. Prior and in addition to deleting the app, you may need to consult the controls in the app, the controls on your phone and/or contact the app vendor to clarify how your personal data may be processed if you decide to delete the app. The app should provide you with the relevant contact details of the app vendor.

The examples presented in this guidance illustrate how to modify your privacy settings on a mobile device using the Android operating system. In some instances, you may also wish to access further privacy settings from a desktop environment. If you are using another mobile operating system or accessing from a desktop browser, there will be some visual differences, but the settings should be located under similar headings.

The settings presented in this guidance are applicable as of the date of publication of this guidance and are subject to change by the social media provider.

Modifying settings on specific social media platforms

A. Facebook

Privacy settings within Facebook

Within the Facebook mobile platform, select **Menu** and scroll to **Account Settings**. Here users can modify their **Privacy** Settings. For example, you can retroactively **Limit who can see past posts** you have made, **Who can see your future posts**, and decide **Do you want Search engines outside of Facebook to link to your profile**.

Under **Account Settings**, you can select **Ads** to view **Ad Preferences**. Here you can view information such as **Advertisers you have interacted with** and **Your Information**, including **Your categories**, which you have been placed in for the purpose of serving personalised advertisements to you.

You can amend how Facebook personalises ads it displays to you in **Account Settings**. Navigate to **Ads**, here you can amend your **Ad Preferences** by selecting **Ad settings** where you can turn off interest-based ads by selecting **Ads based on my use of websites and apps** and selecting '**Off'**. You can also choose to turn off other forms of personalisation by using the controls available to you under **Ad Settings**.

Privacy settings and Facebook apps

Facebook apps are pieces of software developed by Facebook and third-party organisations which you can use while using Facebook. When using Facebook, you have control over what personal data is shared by and with apps.

Personal data shared by and with apps may include your **Birthday**, **Hometown**, and **Interests**, among other pieces of your personal data. Not every app offers the same degree of control over your personal data and if you are using Facebook apps, you should regularly check each app's individual settings as you would all other privacy settings.

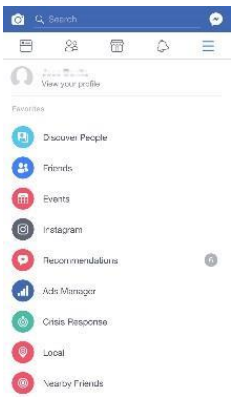


Figure 1

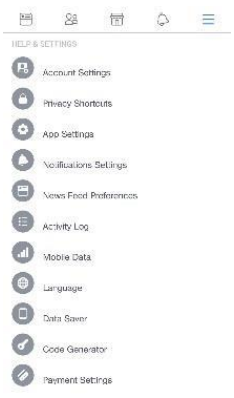


Figure 2

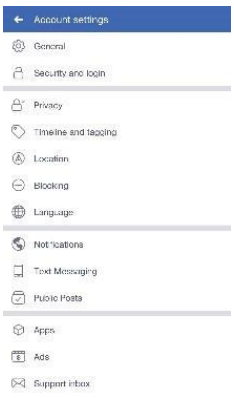


Figure 3

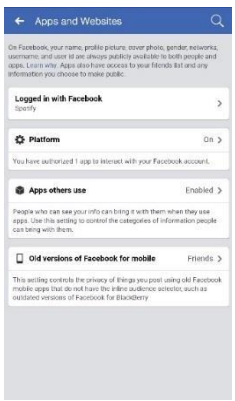


Figure 4

Facebook provides its users with functionality to manage the apps that you give permission to access your personal data. You can see what information apps are collecting by entering **Facebook** and selecting the **Menu**.(*Figure 1)* Looking under **Account Settings** (*Figure 2)* and **Apps** *(Figure 3)***.** You will be able to see apps that are **Logged in with Facebook** *(Figure 4)* and see what personal data they collect from you. You can also **Remove** individual apps.

You may restrict third-party apps from accessing your personal data by disabling their ability to interact with your Facebook profile. To restrict third-party apps, enter the **Facebook app**, select **Menu**.(*Figure 1)*, scroll to **Account Settings** (*Figure 2)*, select **Apps** *(Figure 3)*, select **Platform** *(Figure 4)*, select **Edit** and select **Turn Off Platform**. This will turn off all third party

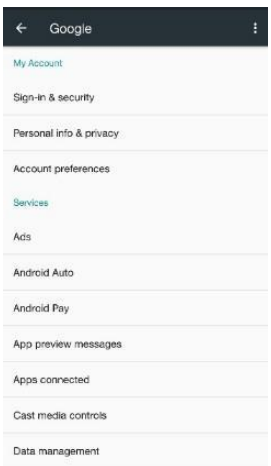
application access to your personal data associated with your Facebook account.

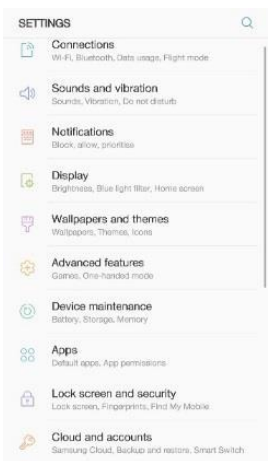
B. Google

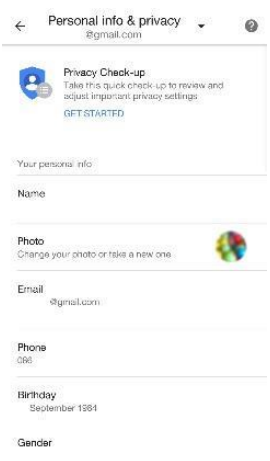
Privacy settings for your Google Account

Google offers a suite of tools to assist users in tailoring their interaction and information sharing when using its services. These tools are offered under a number of headings which can be accessed on a mobile device (using the Android operating system) by opening your device's **settings** *(Figure 5)* and scrolling to **Google** *(Figure 6).*

Note: Privacy settings for certain Google products, such as YouTube and Google Earth are amended within those specific services, not within Google's own account settings.







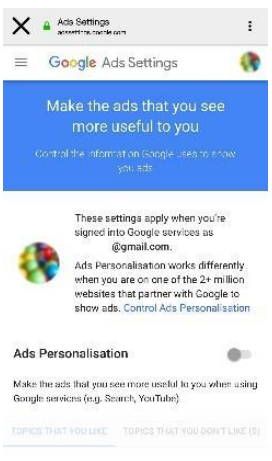


Figure 5 Figure 6 Figure 7 Figure 8

Under **Google,** subheadings allow you to amend privacy settings and review your activity on Google's services. For example, under **Personal info & Privacy** *(Figure 7)* scroll to **Ads settings** *(Figure 8).* Here, you can manage **Ads personalisation** and modify **Topics you like** and **Your profile** to personalise the ads Google displays to you.

In a desktop environment, you can access your privacy and ad preference settings from the **Google Home Page**. Click **Privacy** click **My Account.** Under **Personal info & privacy** Google provides a number of settings that you can use to tailor Google's processing of your personal data.

Google also provides additional privacy and ad preference settings that a user

not logged into a Google account can tailor.

Accessed from the **Google Home Page**, click **Privacy** and click **My Account.** Under **Personal info & privacy** scroll to **Tools you can use now** where you will find a number of settings under headings including **Google Search personalisation, Ads settings** and Opting out of **Google Analytics.**

Privacy settings and Google apps

Google apps are pieces of software developed by Google and third-party organisations that you can use while using Google. Authorising these apps will allow them to access all or part of your personal data associated with your Google Account. Personal data shared with apps may include your birthday, location and phone number, among other pieces of personal data. The app vendor may also request additional information from you, such as your location. When using Google, you have control over whether personal data is shared with apps. Under **Sign-in & security** you can view **Apps with access to your account** and remove apps you do not recognise or no longer require.

C. Instagram

Privacy settings within Instagram

Instagram offers a number of settings to assist its users in tailoring their interaction and information sharing when using Instagram. Within the Instagram mobile platform, navigate to your **Profile** *(Figure 9)* under the **Menu** *(Figure 10)* users can modify their privacy settings. For example, you can set your account to be a **Private Account** and modify who can see when you were last active on Instagram under **Show Activity Status**.

Figure 9

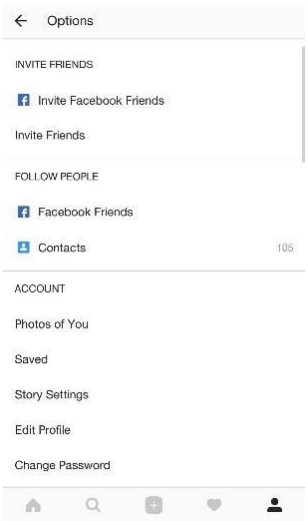


Figure 10

Privacy settings and Instagram apps

Instagram provides its users with functionality to manage the apps that you may have given permission to access your personal data. You can see what personal data these apps are collecting by entering **Instagram** from a desktop environment and selecting your **username** and clicking **Edit Profile**. Here you will be presented with the ability to view the **Authorized Applications** for your account and you can also **Revoke** access to individual apps.

D. LinkedIn

Privacy Settings within LinkedIn

LinkedIn offers a suite of tools to assist its users in tailoring their interaction and information sharing when using the platform. These tools can be accessed on a mobile device by entering **LinkedIn**, and selecting your **Profile Picture** *(Figure 11)*.

Selecting the **Settings** wheel *(Figure 12)*, you will be presented with subheadings named **Account**, **Privacy**, **Ads** and **Communications** *(Figure 13)*. Each presents a number of options that you can modify to amend your privacy settings.

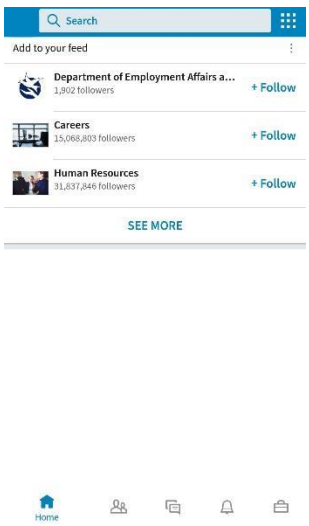


Figure 11

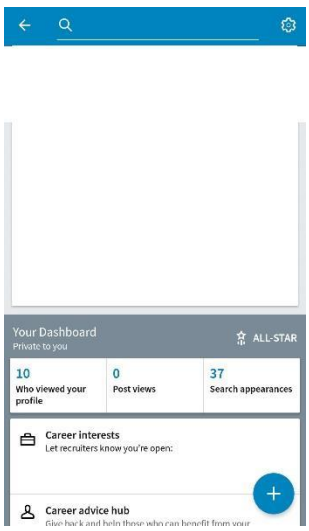


Figure 12

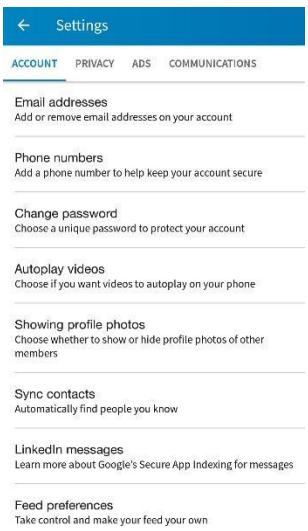


Figure 13

Under the **Privacy** heading, you can view and modify settings such as **Who can see your email address** and **Who can follow you**. These are only a few examples of settings which you can modify to enhance your privacy on LinkedIn.

Privacy settings and LinkedIn Apps

Under the **Account** heading you may check which apps have permission to access personal data associated with your LinkedIn account. To do so, scroll to **Permitted services.** Here you can view and remove apps which have permission to interact with your LinkedIn profile.

E. Twitter

Privacy settings within Twitter

Twitter offers a number of settings to assist its users in tailoring their interaction and information sharing when using the platform. These tools can be accessed on a mobile device by entering **Twitter**, selecting your **Profile picture** *(Figure 14),* selecting **Settings and privacy** *(Figure 15)* and **Privacy and safety** *(Figure 16)*. Users can modify their privacy settings, for example, you can **Protect your Tweets**, restrict **Photo Tagging**, **Block accounts** and restrict settings related to **Personalisation and Data** *(Figure 17).*

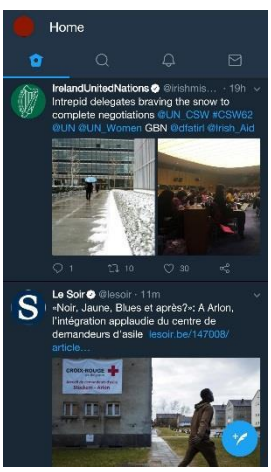


Figure 14

Figure 15

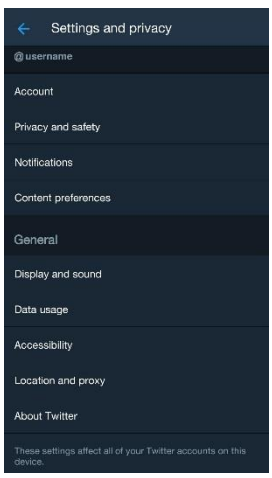


Figure 16

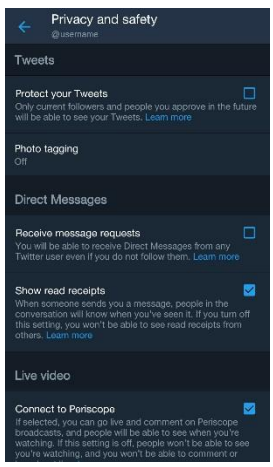


Figure 17

Also under **Personalisation and data**, if turned on, you can personalise the way Twitter will present you with targeted advertising. Here you can amend and tailor settings, such as **Personalise your preferences across all your devices**, **Personalise your settings based on the places you've been** and how your personal data may be shared within Twitter select partnerships. These are only a few examples of settings that you can modify to enhance your privacy on Twitter.

Privacy settings and Twitter Apps

Twitter apps are pieces of software developed by third-party organisations that you can use in conjunction with Twitter. When you connect a third-party

application to your Twitter account, you may be granting that application access to use your personal data. Depending on the apps' permissions, the app may be able to use your account in various ways, including reading your Tweets, seeing who you follow, updating your profile, posting Tweets on your behalf, accessing your Direct Messages, or seeing your email address.

Twitter provides its users with functionality to manage the apps that you may have given permission to access your personal data. You can see what information apps are collecting by entering **Twitter** from a desktop environment and selecting the **Profile and Settings Menu**. Looking under **Settings** and **Privacy**, navigate to **Your Twitter Data,** here you can review and edit your profile information and data associated with your account and **Apps on your devices**. You can also **Revoke access** to individual apps and view the permissions of apps that access your personal data by navigating to **Other Data** and selecting **Connected Apps.**