Appendix K: consumer controls over platforms' data collection

Review of the choices available to consumers

1. As we explained in our interim report, we are aware of consumers' concerns about the control that they have over the collection and use of their data by online platforms. Whilst many consumers who do not mind seeing ads feel that personalised advertising is preferable to receiving ads they consider irrelevant to them, consumers often feel uncomfortable with the widespread collection of their data to make this personalisation possible.[1]

2. To explore the degree of control that consumers have over their data when they use online platforms, we have examined their experiences of using a range of both search and social platforms. In this appendix, we look at the choices that consumers are given about the collection and use of their data, how easy it is to exercise those choices and how the platforms treat those that do not engage.

3. To do so, we have attempted to replicate the typical 'journey' that consumers will undertake when using the platforms, in either the platforms' desktop, mobile or app versions (as relevant for each of those we reviewed). We have made observations on the scope and presentation of settings and options available to consumers at the different stages of these journeys. To note, these observations may not necessarily represent the only means of adjusting such settings and options on the platforms reviewed.

4. We presented our initial observations in our interim report and have subsequently re-reviewed the journeys for those platforms covered there. We have also extended our review to two additional social media platforms.

5. For the purposes of this review, we chose to focus on three search platforms: Google; Bing; and DuckDuckGo, and six social media platforms: Facebook; Instagram; Pinterest; Snapchat; TikTok and Twitter. Of these platforms, only Pinterest and TikTok were not reviewed for our interim report.

6. The selection of Google and Bing in our review reflects their position as the most popular search engines among UK consumers. Both rely on personalised digital advertising to fund their services. Most UK consumers

[1] For further information, see Appendix L and also: The European Commission (2016c). Special Eurobarometer 447: Online platforms; Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

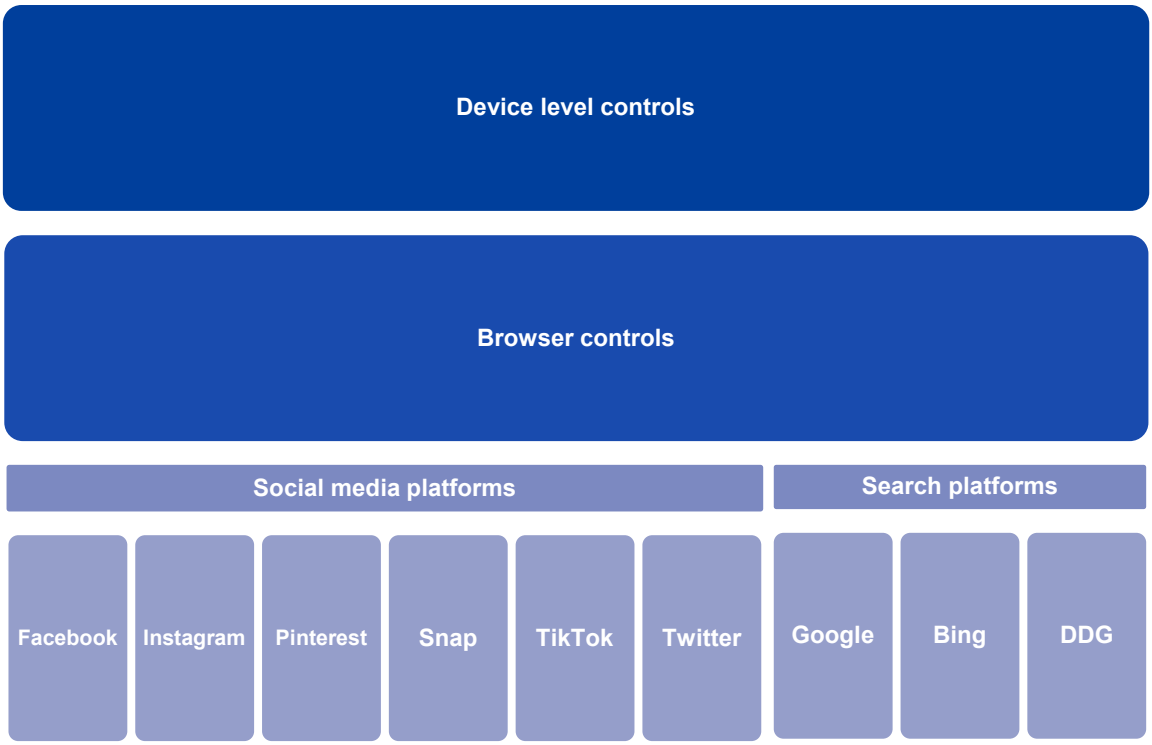
use Google as their primary search engine, either on desktop[2] or mobile. While a much smaller proportion use Bing, which is owned and operated by Microsoft, it is the second most popular.[3] DuckDuckGo is included in our review as it offers an alternative model. It promotes its service as pro-privacy and does not deliver personalised advertising.

7. Facebook, Instagram, Pinterest, Snapchat, TikTok and Twitter are among the most used social media platforms by adults, and all have a minimum age requirement of 13. These platforms allow and encourage consumers to share mixed media content, including photos, videos and text with other consumers. Facebook and Instagram are both owned by Facebook, Inc. Pinterest, Snapchat and Twitter are owned by Pinterest Inc., Snap Inc. and Twitter Inc. respectively. TikTok is a video-sharing service owned by the Chinese internet technology company ByteDance Ltd. All these platforms' services are accessible from either mobile or desktop devices, except for Snapchat and TikTok whose primary services are delivered through their apps.

8. We have reviewed the tools that are available to consumers to manage the collection and use of data for the purposes of personalised advertising, including the design, ease-of-use and effectiveness of those tools.[4] We have considered the controls provided by online platforms, including the default settings for those controls, as well as the controls that an average consumer might engage with in their browsers and on their device. The combination of controls at platform, browser and operating system level is illustrated in Figure K.1.

[2] ie a laptop or desktop computer
[3] As set out in chapter 3, Google's share of supply for general search across both desktop and mobile devices has been between 89% and 93% throughout the last ten years, whilst Bing (previously known as MSN Search) overtook Yahoo as the second most used platform for general search in 2009 and has retained this position ever since.
[4] We have not explored in detail the use of tools that require consumers to take additional action to access, such as signing up to a Virtual Private Network (VPN) or the TOR browser technology.

Figure K.1: The range of choices available to consumers at different levels



Source: CMA.

Overview of consumer control over data collection and use

9. With consumer perspectives in mind, this section contains an overview of the controls offered by search and social media platforms which allow consumers some choice over the collection and use of their data for personalised advertising.

Search platforms

10. Consumers do not need an account to search the internet; they can simply visit a search engine, type their query and be directed to suitable websites. However, some search engines give consumers the ability to set up an account, which can offer additional services such as an email account, calendar, and document and photo storage.

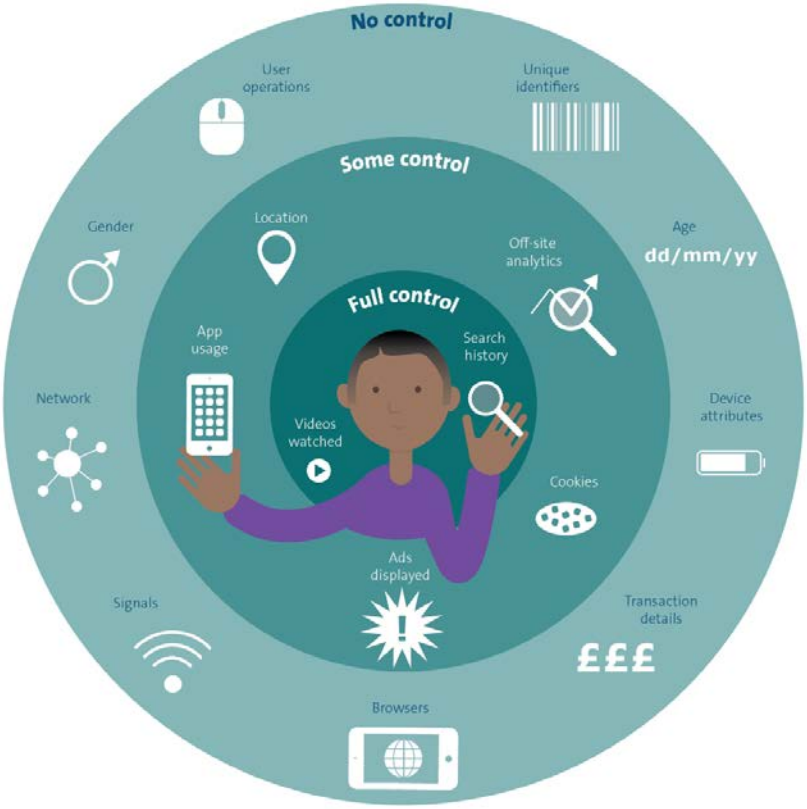
11. We found that the availability of controls offered by the different search engines varies according to whether consumers are logged into associated accounts. To create an account, consumers need to provide more information

such as their name, email address and date of birth. However, being logged-in gives consumers more control over how their data is used.[5]

12. Figures K.2 and K.3 provide an illustrative representation of the types of information that consumers can control and the levels of control that they have when logged-in to an associated Google account and when not. More details regarding the information collected is contained in Figure K.4.

[5] Logged-in consumers are also referred to as 'authenticated users'.

Figure K.2: Illustrative levels of control over information collected by Google – logged-out



Source: CMA analysis of information controls available to consumers on Google.

Figure K.3: Illustrative levels of control over information collected by Google – logged-in

Source: CMA analysis of information controls available to consumers on Google.

Figure K.4: Table of control over information

	Unable to control
	Some control
	Controllable

	Google Search		
	Logged-out		Logged-in
Initially provided info	No need to provide info		Name
			Password/Phone
			D.O.B
			Gender
			Email
Collected info	Search history (search and audio)		Search history (search and audio)
	Videos watched		Videos watched
	Cookies		Password/username
	Off-site analytics (3rd party ads and transactional data (customer matching and store sales))		Gender
	App Usage (Preferences/settings)		Your content (emails sent and received/photos/videos/documents and files/comments and blogs)
	Ads displayed		Name
	Location (IP address/GPS and sensors/ inputs)		Email/phone
	Age (Range) & Gender		Age (Date of birth)
	Gender		Cookies
	Transaction details (Payment info/content of shopping baskets)		Off-site analytics (3rd party ads and transactional data (customer matching and store sales))
	Device Attributes (type/settings/language/screen size/ OS version/device events/hardware settings/battery/volume)		App Usage (Preferences/settings)
	Browsers (Browser type/settings/URLs visited and referrals/timestamps)		Transaction details (Payment info/content of shopping baskets)
	Unique Identifiers (IP address/device identifiers/ Ad identifiers)		Ads displayed (Ads displayed/some demographic info/interests)
	Network (Network operator/phone numbers/call times and durations)		Location (IP address/GPS and sensors/ inputs/location history)
	Consumer interactions (clicks/taps/hovers)		Device Attributes (type/settings/language/screen size/ OS version/device events/hardware settings/battery/volume)
	Signals (Cell towers/Wi-Fi/Bluetooth signals)		Browsers (Browser type/settings/URLs visited and referrals/timestamps)
			Unique Identifiers (IP address/device identifiers/ Ad identifiers)
			Network (Network operator/phone numbers/call times and durations)
			Consumer interactions (clicks/taps/hovers)
			Signals (Cell towers/Wi-Fi/Bluetooth signals)

Source: CMA analysis of information controls available to consumers on Google.

13. Whether consumers are logged-in or not, the default settings allow for the collection of user data and for the personalisation of advertising shown to the consumer. For example, the default settings for both Google and Bing are set to deliver personalised ads.

14. Because consumers can use search platforms when either logged-in or logged-out of an account, we describe these separately below.

Consumers that use search engines without logging into an account

15. We found that the controls available to consumers vary by platform. Google and Bing enable some control over ad personalisation and Google includes search personalisation settings. However, neither platform allows consumers to fully control the use of location data or unique identifiers.[6] The 'ad personalisation' control switches off personalisation but not data collection, and Google states that consumers will still see ads based on the website that they are viewing and their general location. Figure K.5 shows the different levels of control available to consumers on each of the search engines we reviewed.

Figure K.5: Search engine consumer controls for non-logged in consumers

Control	Google	Bing	DuckDuckGo
Ad personalisation	✓ [7]	✓	N/A
Search personalisation	✓	✗	N/A
Other platform controls	✓ [8]	None	✓ [9]
Information and links to non-platform controls	✓	✓	✓

Source: CMA analysis of controls available to non-logged in consumers on these platforms

16. The way consumers access controls also differ across platforms. For example, Google provides non-logged-in consumers with control settings via a prominent 'Privacy Reminder'. As well as this, a less prominent link to its privacy policy and controls is provided on each page. Bing's controls can be reached via a menu button, as well as an unobtrusive privacy and cookies link

[6] Unique identifiers are reference numbers that identify a browser, app, or device. There are a number of types of these identifiers and they vary in their permanence; common unique identifiers are generated in cookie files, advertising ids and device serial numbers. When consumers are not signed-in, the major search platforms store the information they collect using these unique identifiers tied to the browser, application, or device. In this way they are able to personalise ads and maintain site settings and preferences.
[7] These relate to Google Ads and stop personalised Ads being served but not location-specific contextual Ads: 'Ads you see may be based on the website that you're viewing and your general location'.
[8] Control whether YouTube experience is affected by previous YouTube search and watch activity.
[9] Options relating to https encryption, search request format and redirects, and video playback.

on each page. DuckDuckGo's privacy settings on desktop devices are behind a notice promoting use of its browser extension. These are arguably less relevant as, by default, this platform collects minimal search data.

Consumers that use search engines while logged-in to their associated accounts

17. Consumers typically have a greater amount of control over the use of their data including for personalised advertising when they are logged into their associated accounts. For example, when consumers are logged-in to their Google accounts, they can access a greater amount of controls in the 'Data & Personalization' area of the website where they can access settings and view some of their data. On this page there is also a 'Privacy Checkup' facility which is described as a step-by-step guide that 'helps you choose the privacy settings that are right for you'.

18. The 'Privacy Checkup' provides settings across five themes, with around 15 options in total across all of these themes combined:[10]

    - Activity controls reviewed:

      (i) Web and App activity (x2 options)

      (ii) Location History (x3 options)

      (iii) YouTube History (x2 options)

    - Manage your Google Photos settings (x2 options)

    - Help people connect with you (x3 options)

    - Control what others see about you (x2 options, plus additional individual controls relating to consumers' personal information under 'Edit what others see about you')

    - Make ads more relevant to you (x1 option)

19. We consider an example journey to 'Make ads more relevant to you' in the section 'How easy is it to exercise choice', below.

20. For Bing, logged-in consumers can use a 'Privacy Dashboard' comprising 10 areas that primarily enable consumers to view and clear data in each section:

    - Browsing history;

[10] Based on our review of Google's Privacy Manager on 15 June 2020.

- Search history;
- Location activity;
- Voice activity;
- Media activity;
- Product and service activity;
- Product and service performance;
- Cortana's Notebook; and
- Product-specific data for LinkedIn and Health Vault.

21. Eight additional links to settings are provided on this page: Windows, Apps and services, Xbox, Office, Skype, Ad settings, Promotional communications, Other Microsoft products, and information for contacting the privacy team.

22. The impact of control settings and how they relate to other controls is not always clear. For example, Google provides a 'Location History' control. By default, it is 'paused' and the explanation alongside is: 'Saves where you go with your devices, even when you aren't using a specific Google service, to give you personalized maps, recommendations based on places you've visited, and more.' However, if a consumer selects a link to 'Learn more' they will be told that adjusting the setting will not change location services on their device, and that location data may continue to be saved in other settings, like Web & App Activity.

Social media platforms

23. Social media platforms provide some controls for managing the collection and use of data for personalised advertising. These controls generally do not prevent data being collected, rather they allow consumers to influence the way that their data is used and what ads they will be shown.

24. Social media platforms offer limited functionality for consumers who either do not have an account with the relevant platform or are not logged-in to their account. This is because social media platforms rely on consumers to provide content to attract other consumers to use these platforms. On the platforms we reviewed, controls available to consumers who do not have an account or are not logged-in are very limited. However, consumers may be able to limit the data they share using off-platform controls, for example those available in

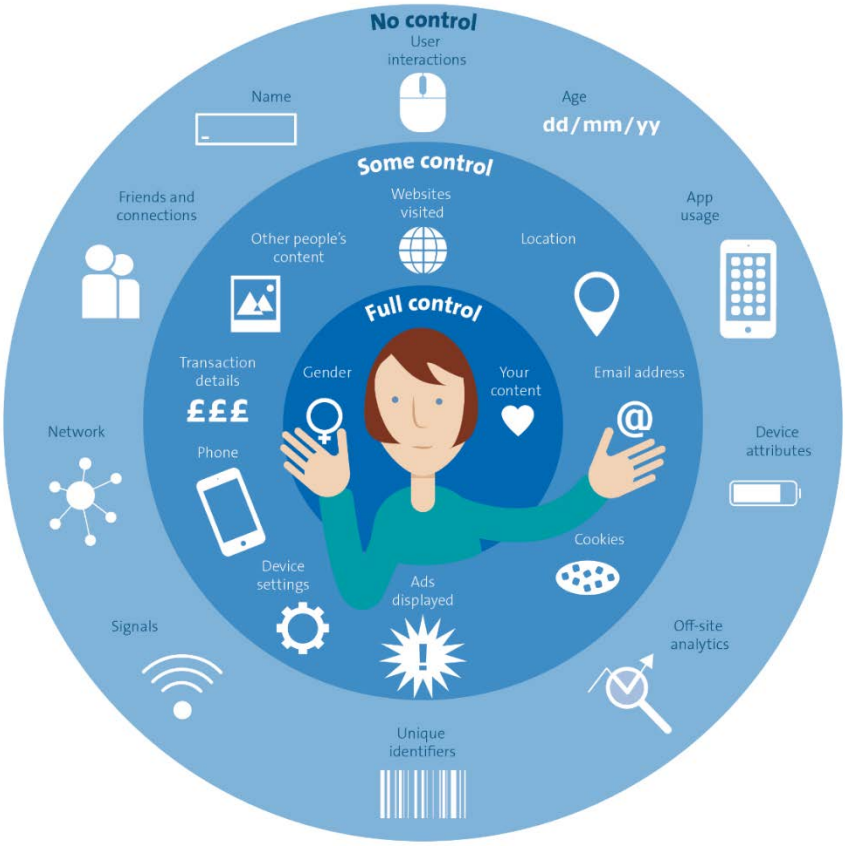
their browsers. Our focus when reviewing social media platforms was therefore on controls that consumers have when logged-in to their accounts.

Controls for logged-in consumers

25. Social media platforms require consumers to provide certain pieces of information to create an account. At minimum, for the platforms reviewed, consumers need to provide their full name or a unique username, email address or telephone number. Some additional information may be provided voluntarily by the consumer, whilst other information is collected automatically by the platform without consumers' consent. Consumers therefore have varying degrees of control over different categories of information.

26. Figure K.6 illustrates the extent to which consumers using Facebook have control over their information by category. As shown, consumers have no control over the collection of information such as their age and unique identifiers (assuming they sign-up to use the platform) but have more control over the collection of other data, such as location.

Figure K.6: Extent of consumer control over different categories of information on Facebook



Source: CMA analysis of information controls available to consumers on Facebook

Figure K.7: Information required from consumers at sign up and during ongoing use, with an indication of the level of control available to consumers on Facebook

	Unable to control
	Some control
	Controllable

	Facebook
	Logged-in
Information required from consumer at	**Name**
	Phone[11]
	Email Address
	D.O.B.
	Gender[12]
Information collected from consumer during use of services	***Consumers' Content*** *(incl. posted content and communications with other consumers)*[13]
	Friends and groups *(incl. consumers' friends (once made), Facebook pages visited, groups joined, hashtags posted)*
	Consumers' app usage (incl. Facebook products) *(incl. apps, features and other Facebook created content)*
	Transaction details *(incl. payment card details, billing/delivery addresses)*
	Other people's content *(incl. posted content, comments/shares, tags)*
	Device attributes *(incl. OS version, hardware, browser type, plugins, battery level)*
	Consumer interactions *(incl. foregrounding/backgrounding of windows, mouse movements)*
	Identifiers *(incl. unique identifiers, device IDs, identifiers from apps, games and accounts used)*
	Signals *(incl. Bluetooth signals, wi-fi access points, mobile phone triangulation relating to a consumer's device)*
	Device settings *(incl. GPS location, camera and photos)*
	Network *(incl. mobile network provider, ISP, language, time zone, IP address, connection speed)*
	Cookies
	Off-site analytics *(incl. third party websites visited/services used, ads displayed)*

Source: CMA analysis of information controls available to consumers on Facebook

Consumer controls on an ongoing basis

27. Whilst consumers can influence, to a certain extent, the nature and content of the personalised adverts they see both on and off the social media platforms

[11] Only one of either a consumer's mobile telephone number or email address is required to sign up. A consumer can provide both pieces of information if they wish.
[12] It is optional for consumers to provide their gender information, but they must provide a pronoun (he, she or they).
[13] Controllable to the extent that consumers can choose whether to post content.

they use, they are generally not able to opt out or prevent the platforms from using their data for advertising purposes.

Facebook

28. Facebook told us that consumers, can utilise the 'Your Online Choices' website operated by the European Interactive Digital Advertising Alliance (DAA),[14] to control their online behavioural advertising preferences, including choosing whether browser cookies are set and whether to delete those cookies.

29. Consumers can also choose: whether off-platform data is used to advertise to them on Facebook's ad-supported services; whether their Facebook interests are used to advertise to them off Facebook's platforms; and whether their personal 'Likes' are displayed in adverts.

30. Facebook told us that consumers' choice of whether to activate its 'Hide Ad' control, does not affect the information that Facebook will process to personalise ads.

Snapchat

31. Consumers must download and be logged into the Snapchat app in order to use its services. This limits the ability of consumers to implement controls outside of the Snapchat ecosystem. For example, consumers' browser settings (including cookie blocking) will have no effect within the Snapchat app.

32. Consumers can choose to opt out of receiving Audience-Based and Activity-Based ads (which are turned on for all consumers by default) from Snapchat yet continue to use the platform. Consumers can also opt out of Third-Party Ad Networks (which consumers are again opted-in to by default) and continue to use Snapchat.

Twitter

33. In its privacy policy, Twitter states that it does not support the Do Not Track (DNT) browser option.[15]

---

[14] Homepage of the European Interactive Digital Advertising Alliance's 'Your Online Choices'.
[15] We note that the Tracking Protection Working Group, which was responsible for developing and demonstrating the viability of the Tracking Preference Expression specification which underpins the DNT function has discontinued this work and closed on 17 January 2019. The Tracking Protection Working Group stated that this was due to the fact that: 'there has not been sufficient deployment of these [DNT] extensions (as defined) to

34. In its privacy policy, Twitter also states that it respects the DAA's consumer choice tool for consumers to opt out of interest-based advertising, whilst allowing consumers to continue using its services.[16]

35. Consumers can opt out of certain forms of personalisation on Twitter, however they are unable to prevent Twitter from: displaying ads based on their Twitter activity; personalising their experience based on information they have provided or devices they've used to log-in; and displaying content based on consumers' current location and the location where they signed-up.

36. Twitter told us that the settings and controls available to consumers who are not logged-in are more limited than for those who are logged-in, but that this was commensurate with the more limited functionality available to logged-out consumers.

Pinterest

37. Pinterest states in its privacy policy that consumers can choose whether:

    (a) Pinterest ads delivered to them on other platforms, sites or apps are customised using information about their account activities.

    (b) Pinterest shares information about their activity on Pinterest for ads performance reporting.

38. Pinterest states that it also supports settings such as Limit ad tracking on iOS, Ad personalisation on Android devices and Do Not Track in browsers.

39. Pinterest also states that consumers have choices available to them through the device or software they use to access Pinterest. Consumers can for example control cookies or other types of local data storage through their browser or use their mobile device to choose how and whether their precise location, photos and contacts are shared with Pinterest.

40. However, consumers cannot opt out of Pinterest automatically collecting and processing certain information about them, including log data, consumer searches on Pinterest, their browser type, settings and information on how they use Pinterest.

---

justify further advancement, nor have there been indications of planned support among user agents, third parties, and the ecosystem at large.' Apple removed the Do Not Track option from all versions of Safari from version 12.1 later in 2019.

[16] The DAA's 'YourAdChoices' tool.

TikTok

41. TikTok primarily collects data directly from consumers, but also receives some data from third parties such as business partners, advertisers and advertising networks.

42. TikTok told us that personalised advertising is switched off by default and data collected for the purpose of optimising such advertising is only used to serve personalised advertising on a consumer if actively switched on by that consumer.

43. Whilst some external data sharing is controllable by TikTok users (ie it is only triggered if a consumer makes use of a particular function on the app, such as purchasing coins or opting in to personalised advertising), other external data sharing (such as data sharing with TikTok's cloud service provider) is considered necessary by TikTok for the functionality of its platform and is not subject to consumer controls.

44. TikTok's privacy policy states that it may share consumers' information with a parent, subsidiary, or other affiliate of its corporate group.[17] Within TikTok's settings, there are no controls available to consumers to limit TikTok sharing their data in this way.

Default settings

45. All the social media platforms we reviewed, except for TikTok, have default settings which enable some degree of personalised advertising to be shown to consumers. For example:

- On Facebook, consumers' activity can be used to personalise ads served by Facebook on other websites and apps by default. Consumers can prevent Facebook from showing them some of these ads but cannot prevent Facebook from processing their data in the manner which informs this process. However, by default consumers are not shown ads based on data provided by Facebook's partners.[18]

- Consumers using Snapchat for the first time will have each of its 'Audience-Based' and 'Activity-Based' ads, and 'Third-Party Ad Networks enabled by default. These all facilitate Snapchat serving personalised ads to them.

[17] TikTok's Privacy Policy.
[18] Consumers using Facebook can enable this type of advertising via a setting on Facebook's 'Ad Preferences' page.

- Twitter enables personalised ads for consumers using the platform for the first time by default. Consumers must visit Twitter's 'Personalization and data' settings and make an active choice to adjust these. By default, Twitter always show ads to consumers which are personalised, at minimum based on information from their activity on Twitter (for example, a consumer's tweets, who they follow and what type of phone they use).[19]

- Pinterest will, by default, use information regarding a consumer which has been provided by its partner organisations to personalise that consumer's experience on the platform, including to show them personalised ads.

46. By default, personalised ads are not shown to consumers on TikTok. Consumers are prompted to review this setting the first time they use the app.

47. Consumers generally have greater control over other aspects such as the use of their location information (for example, to further personalise ads or the platform's content, or for sharing with other consumers using the platform). The default setting for all the platforms reviewed was to have the use of location information turned off. For example, Twitter has a setting which allows it to personalise content for consumers based on places they have been, and this is turned off by default for new consumers. Similarly, by default Facebook's device-based location settings are turned off and Snapchat will not share a consumer's location with other consumers.

48. None of the platforms reviewed require consumers to provide any information classified as belonging to a special category of data as a condition of creating an account. However, such information may be collected during a consumer's use of the platforms if, for example, consumers include this in content they post.

49. All the social media platforms reviewed told us that when their terms of service or privacy policies are updated, consumers will receive a prompt explaining the significance of the updates, and a request to make an active choice regarding any affected settings.

Consumer experience when signing up to and using search platforms

50. In this section, we review the experience of consumers using search platforms, with and without logging-in to an account, and set out:

[19] Twitter's Online Help Center - 'Your privacy controls for personalized ads'.

- how clearly the search platforms set out the fact that they monetise consumer data by selling personalised advertising;
- how the search platforms present consumers with information, including terms and conditions; and
- how easy it is for consumers to exercise choice over their settings.

Nature of the relationship

51. The major search engines offer their services to consumers at no monetary cost because they gain consumers' attention and data, which they monetise through the sale of advertising.[20] The search engines we reviewed acknowledge that their services are supported by advertising, but the prominence of those acknowledgements varied.

- Google sets out the features of its service in a section of its website: 'How Search works'.[21] This includes statements that: 'We sell advertising, not search results' and 'Google's commercial relationships have no impact on algorithmic Search changes, and partner advertisers do not receive special treatment in resolving organic search issues or requests'. By clicking through from here, consumers can reach a page 'How We Make Money with Advertising'.[22] This explains that Google's main source of revenue is advertising and provides an overview of its advertising business, both on and off its own platform.
- For Bing, we found information about the features of the search engine and funding by navigating via the menu to Microsoft's privacy statement.[23] This includes a section on advertising that states: 'Some of Microsoft's services are supported by advertising. To show ads you're more likely to be interested in, we use data like your location, Bing web searches, Microsoft or advertiser web pages you view, demographics, and things you've favorited.'
- DuckDuckGo is marketed as a pro-privacy search engine and promotes this on the front page and throughout the site. In its help pages DuckDuckGo includes information about features of the site and

[20] Privacy-focussed search engines tend to gain funding from one or a combination of contextual advertising, affiliation programmes and donations.
[21] How Google search works.
[22] How Google makes money from advertising.
[23] Microsoft privacy statement.

information sources, as well as its funding model, which is based on contextual advertising and affiliate programmes with e-commerce sites.[24]

Consumer experience when not signed up or logged-in

Data collection

52. Both Google and Bing can be used by those who have no account or who have an account but are not logged into it, and other search engines exist that have no linked account. For all the search engines that we reviewed a consumer can begin using the services immediately. Although consumers may not sign in to use a search engine, data is still collected and stored against unique identifiers ie numbers that are used to identify a browser, app, or device.

Google

53. A consumer visiting Google's search page for the first time will see a prominent statement on privacy, the 'Privacy Reminder' (as well as less prominent Privacy/Terms/Settings links available on each page). The Privacy Reminder can be:

- Ignored – without impacting use of the site. After three days, the consumer will be required to acknowledge the Privacy Reminder before continuing.
- Postponed – by clicking 'Remind me later'
- Reviewed – which provides information about Google's Privacy Policy and options for the consumer to exert some control.

54. Once a consumer engages with the Privacy Reminder section, they are provided with summary information about the processing of information by Google, why it is processed (including to 'Deliver ads based on your interests'), that data may be combined and that privacy controls are available.

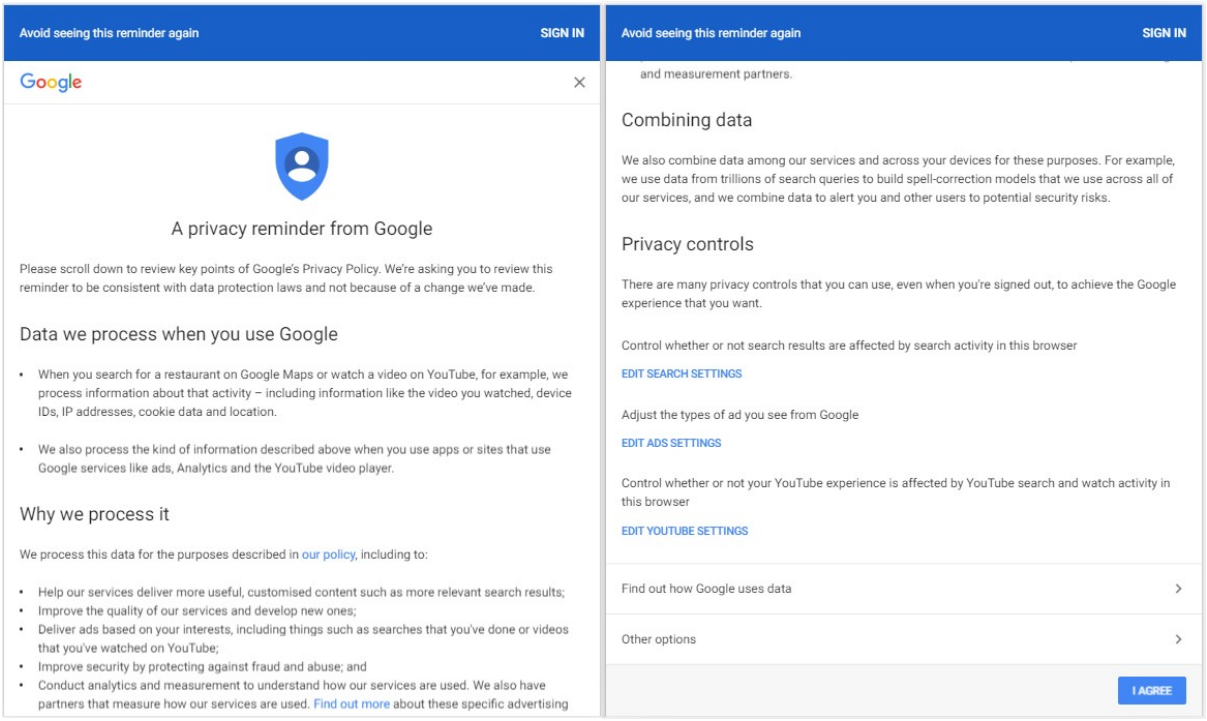
55. Controls are discussed more fully above but, in brief, settings are provided to:

- Control whether or not search results are affected by search activity in this browser
- Adjust the types of ad you see from Google

[24] DuckDuckGo Help Pages – 'Advertising and Affiliates'.

- Control whether or not your YouTube experience is affected by YouTube search and watch activity in this browser.

Figure K.8: Google Privacy Reminder



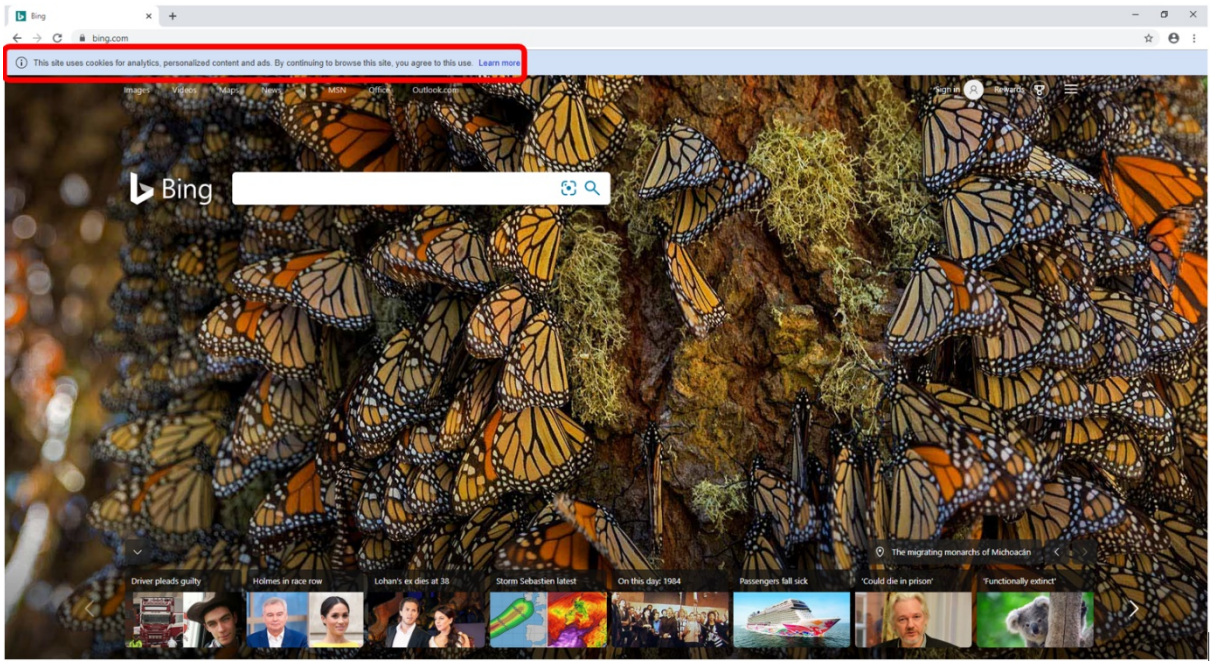
Source: Screenshots of Google's privacy reminder as viewed on a mobile device

56. The Privacy Reminder adopts a summary approach to displaying information and provides some choice to consumers. We note (a) the positive framing of the language and choice architecture encouraging acceptance and (b) encouragement to use an account, which provides more functionality such as control over preferences, but involves volunteering more information.

Bing

57. A consumer visiting Bing's search page for the first time will see an initial cookie notice displayed. The notice is more prominent in mobile displays than on desktop, but on both disappears without active engagement from the consumer as the site is used.

Figure K.9: Bing Cookie notice on desktop



Source: Screenshot of Bing.com as viewed on a desktop computer

58. Consumers are able to access privacy information via a menu button or a 'Privacy and Cookies' link available on each page. As discussed above, Bing collects consumers' information by default and, while a control to opt out of being shown personalised ads is provided, consumers may not be aware of its existence.

DuckDuckGo

59. A consumer visiting DuckDuckGo's home page can begin searching immediately. A range of messages that promote the site's pro-privacy approach are displayed, as is an option to install a browser add-on. The format of the display varies according to device and browser format. DuckDuckGo does not collect consumer's information by default.

Private browsing

60. Signed-out consumers also have the option to use a private mode available on most web browsers to access search engines. These options prevent cookies, browsing history, search records and passwords from being stored on the consumer device at the end of their session.

Experience when consumers sign up for an account

61. Whether consumers use search engines in association with an account may reflect their broader engagement with other products offered by online

platforms. Search functions do not look fundamentally different to consumers whether they are logged-in to an account or not. But an account is normally needed to use other products. While some consumers may want to keep their searches separate from other online activity, others will value the way that, for example, a platform can link a search for a music event with their previous activity and location, facilitating the purchase of tickets and putting a reminder in a calendar without having to use several different accounts.

62. Google describes its accounts in the following terms: 'Sign in to your Google Account, and get the most out of all the Google services you use. Your account helps you do more by personalizing your Google experience and offering easy access to your most important information from anywhere.'[25]

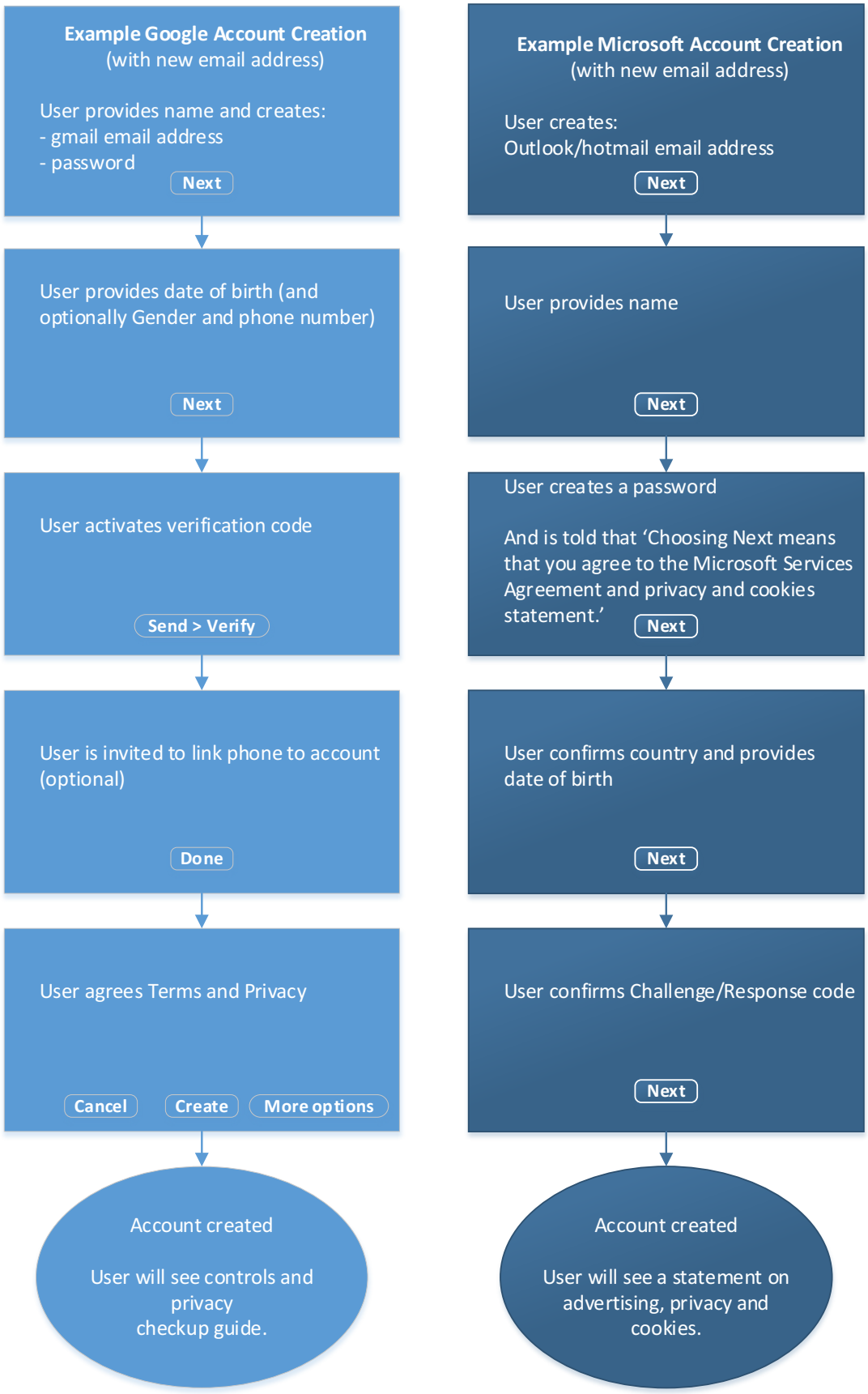
63. Microsoft refers to its accounts as 'One account for all things Microsoft' and while privacy is mentioned, note the inter-connection it provides: 'Access your favourite Microsoft products and services with just one login. From Office and Windows to Xbox and Skype, one username and password connects you to the files, photos, people and content you care about most.'[26]

Sign up process

64. Both Google and Bing make it easy for consumers to create accounts. The initial information required is a name and date of birth, in addition to a country for Microsoft. In Figure K.10, below, we illustrate the process consumers go through when setting up an account with both Google and Microsoft. As shown, the process is relatively simple and quick to complete.

[25] Google Account Overview.
[26] Microsoft Account Page.

Figure K.10: Illustrative Sign-up flow for Google and Microsoft Accounts



Source: CMA analysis of the sign-up process for Google and Microsoft accounts

65. When consumers sign up to create an account, many platforms use clickwrap agreements to confirm the consumer acceptance of the terms and conditions.

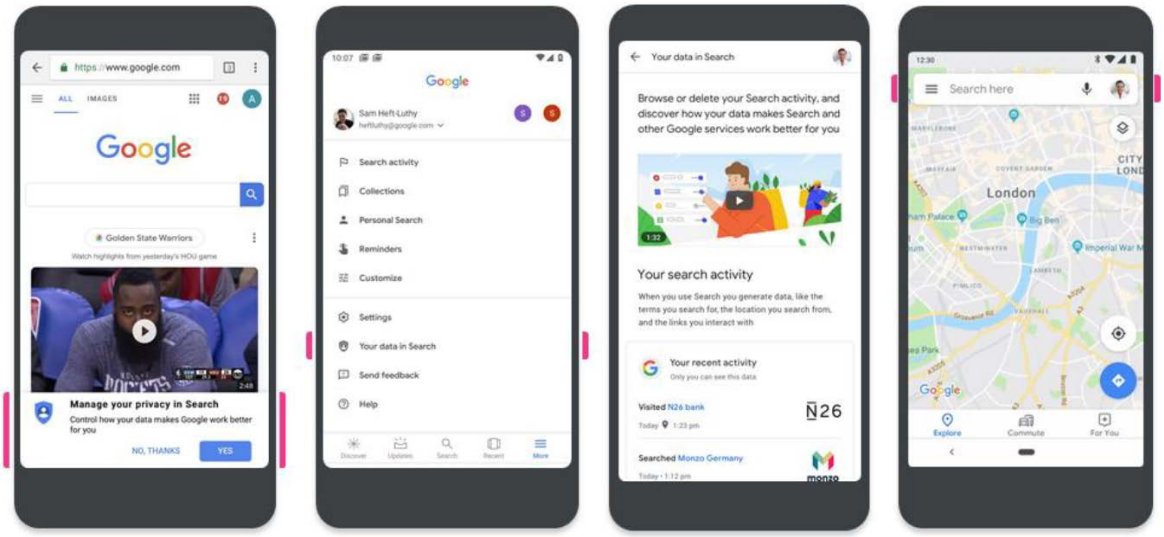
66. Clickwrap agreements, including that used by Microsoft, tend to bundle consent functionally, linking consent to data processing with agreement to use the service and the acceptance of cookies. Signing up to an account with Google or Microsoft also involves aggregating of consents across a number of services. Both companies confirm in their privacy policies that they combine data across their services and products. All-encompassing privacy agreements that underpin bundled accounts necessarily become lengthy or vaguely generic, and as consumers adopt further products from the same company with no separate sign-up, they may not take time to consider information privacy at each occasion.

How easy is it to exercise choice?

67. Google told us that it: frequently promotes user tools and controls in prominent places, including the homepage. Moreover, when a user opens a new Google account, they receive an email reminder 'inviting them to discover all the privacy controls available to them.'[27] As we set out in chapter 4, the proportion of UK users visiting Google's privacy page is relatively low.

68. Figure K.11 is a Google-provided image highlighting some of the points at which a consumer might interact with their privacy tools.

Figure K.11: Google-provided images highlighting its privacy tools



Source: Submitted by Google in response to our consultation on the Statement of Scope

[27] Google's Response to the CMA's consultation on the Statement of Scope, page 15.

69. The nature of the settings that are provided to consumers varies according to their function and the extent of control provided. Settings may allow consumers to control the collection of data, restrict its uses, or manage it through deletion, correction or update.

70. In Figure K.12, below we provide an illustration of the path that a logged-in consumer might take to adjust their advertising settings on Google. In the example, a consumer might:

- Begin at the 'Privacy Checkup' screen and scroll down to select 'Make Ads more relevant to you'. Here they can click on 'Manage your ad setting'.
- At the subsequent 'Ad personalization' screen they have options to:
  - Turn Ad personalisation on/off.
  - Control ad personalisation on other websites & apps that use Google ad services. If consumers select this option, they are directed to the 'Your Online Choices'[28] website via a weblink.
  - Learn more about how ads are personalised for them and update the personal information that they have added to their Google account which is used for this purpose.
  - Visit the Your Online Choices site via a further link where Google states that they can 'control ads from other ad networks.'
  - Select a link to learn how to install browser/ad-blocking extension plugins.

[28] Your Online Choices website.

Figure K.12: An illustration of the journey to control Ad settings

Source: CMA analysis of the consumer journey to access Google's ad settings (based on Google's website as it appeared on 15 June 2020).

Terms and conditions

71. The terms and conditions, privacy and data policies and statements of the search engines that we examined are, with the exception of DuckDuckGo, extremely lengthy. We noted some use of different approaches by the platforms to communicate this information, including animations, summarised and layered presentation and periodic reminders to consumers.

72. The word count comparison below is indicative of the main elements in each site. The figures do not count the additional text available through embedded links.

Figure K.13: Comparative length of search platforms' terms and policies

Terms / Policies	Search Platform		
	Google	**Bing**	**DuckDuckGo**
Accessible from front page?	Yes	Yes	No[29]
Approximate Length in Words	**8,100**[30] (3,400 Terms of Service 4,700 Privacy Policy)	**19,200**[31]	**2,200**[32]
Flesch reading ease score[33]	**44.1** ('Difficult to read')	**41.8** ('Difficult to read')	**58.6** ('Fairly difficult to read)
Clickwrap	No[34]	Yes	N/A

Source: CMA analysis of the terms and conditions documents of these platforms

73. In terms of readability, we were told by the Behavioural Insights Team (in its response to our Statement of Scope) that the characteristics of terms and conditions exacerbate asymmetries between platforms and their users.[35] Work they had done on consumer understanding of terms and privacy policies indicated that even when participants were incentivised to absorb information they correctly recalled just 40-60% of key terms. A recent interactive article in the New York Times graphically demonstrates most online privacy policies require a reading ability far above average.[36] Some sites use 'layered' techniques which they describe as intending to make the material more manageable and to allow consumers to drill down into areas of interest. However, these tend to remain lengthy and of similar complexity.

[29] This is located behind a pop-up encouraging the download of DuckDuckGo to Chrome.
[30] Google updated its Terms of Service on 31 March 2020. Google includes 4 x short videos in its Privacy Policy and an alternative pdf page.
[31] Bing figure is the total for the Microsoft Services Agreement and Microsoft Privacy Statement which applies to a range of Microsoft products in addition to Bing.
[32] DuckDuckGo figure is not comparable to others - the 2,100 words are in its 'Privacy' statement but much of the statement amounts to DuckDuckGo's commentary on how Search works and how they don't collect information that others do.
[33] In the Flesch reading-ease test, higher scores indicate material that is easier to read; lower scores indicate material that is more difficult to read. The scale ranges from 0.0 to 100.00 and is divided into seven bands of between 10 to 30, each assigned a (US educational system equivalent) level of education that is required to understand the material with a score in that band. For example, material scoring 90.00 to 100.00 is described as 'very easy to read' and easily understandable by an average 5th grade (11-year-old school pupil), whilst material scoring 0.0 to 30.0 is described as 'very difficult to read' and most likely to be understandable only by university graduates. We calculated the Flesch reading-ease scores for each of the platforms' policies by importing their text into Microsoft Word and applying the 'Readability Statistics' tool to this.
[34] The Google signup process breaks out permissions beyond a single 'accept and use' approach.
[35] The Behavioural Insights Team's response to the CMA's consultation on the Statement of Scope.
[36] 'We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.' The New York Times, 12 June 2019.

Deletion

74. Both Google and Microsoft have procedures for consumers to delete their accounts and download their data, although they differ slightly in their approaches.

75. Figure K.14 shows the comparative number of 'clicks' a consumer has to make in order to: (i) reach the account deletion page; and (ii) activate the deletion process once they have reached this page.

Figure K.14: Comparative number of consumer 'clicks' required to delete search engine account[37]

'Clicks' required to delete account	Search Platform		
	Google	**Bing**	**DuckDuckGo**
Minimum number of clicks required to reach account deletion webpage from platform homepage	5	7	N/A
Clicks required on account deletion page to delete account	3 (2 tick box acknowledgements, confirm account deletion button)	13 (10 tick box acknowledgements, drop down menu and closure reason selection and confirm account deletion button)	N/A

Source: CMA analysis of Google and Microsoft account deletion processes

Google

76. Google enables consumers to delete some individual services from their account, for example to delete YouTube and video they have uploaded, without closing their entire account. If consumers elect to delete their entire account its data is also deleted, although steps are available to download the information. Deleting an account will impact on consumers that use Android or Chromebook devices. Google warns that Android users will no longer be able to use some apps and services, that they won't be able to get or update apps from the Play Store and they will lose music bought elsewhere and added to

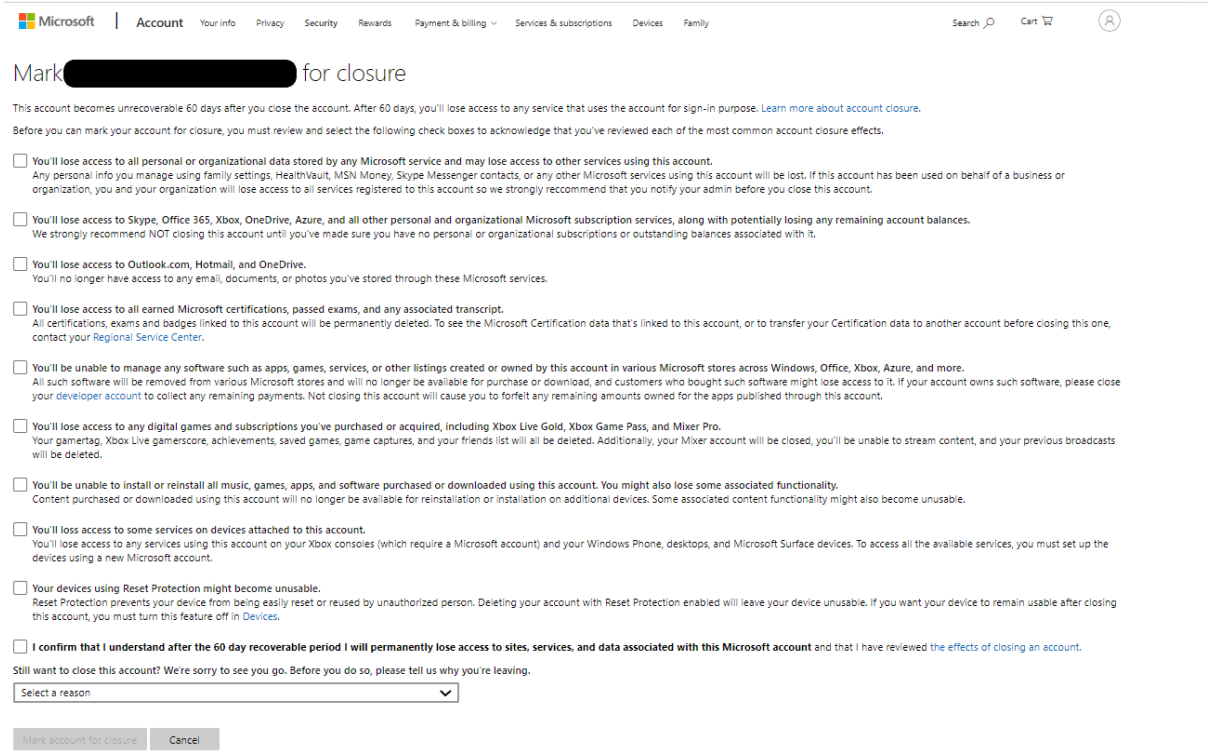
[37] The methodology we used to assess this was based on what we believed would be a typical consumer's journey to reach the account deletion page (and to subsequently delete their account) from a starting point of the platform's homepage. We understand that it may be possible for consumers to access the platforms' account deletion screens more quickly via alternative means, if they have sufficient knowledge of how to do so. For example, consumers may be able to access the platforms' account deletion screens by entering appropriate terms into a search engine and then clicking on a relevant link provided by the search engine if provided.

Google Play. Chromebook users are not be able to use Chrome apps or extensions for the deleted account.

Microsoft

77. Microsoft's account closure process involves closing and deleting all the services associated with it, including: OneDrive files, games data, Skype ID and contacts and email. Microsoft states 'You can't delete just one of these services and keep the others'. Once deletion has been selected, Microsoft waits 60 days before permanently deleting the account, after which time it cannot be recovered. An example deletion screen viewed in our review involved the user having to select 10 tick boxes and a drop-down reason for account closure as shown in Figure K.15.

Figure K.15: Microsoft deletion screen



Source: Screenshot of Microsoft's account deletion screen

Can consumers take their data with them?

78. Google's 'Takeout' process for consumers to download their data before account deletion can also be used at any time to download data. Google told us that 'in 2017 this facility had approximately 21 million unique visitors, who

had exported in total more than one Exabyte of data since launch. That is the equivalent of 50,000 years' worth of DVD quality video.'[38]

79. Consumers access the Takeout function via their account and are presented with a range of Google products from which they can download data. All of the options, of which there are over 40, are preselected to be included.

80. Microsoft's processes for consumers to download their data is divided between data that appears on their Activity history page and personal content from services like email, calendar, and photos which can be exported from within those products.

Consumer experience when signing up to and using social media platforms

81. Social media platforms provide a range of services which allow consumers to communicate and share personal content with their family, friends and acquaintances. Some alert consumers to content from third party providers, such as news websites, and are a means of accessing this content.

Nature of the relationship

82. Like search engines, most social media platforms offer their services to consumers for no monetary cost. This is because they can monetise consumers' attention, content and interactions with their platforms, through the sale of advertising.

83. The largest social media platforms do not draw consumers' attention specifically to this relationship between consumers' data and how they generate revenue during the sign-up process. This is when consumers are likely to have their first interaction with the platform and be most likely to engage with this information. For example, Facebook does not include this information on its home page nor does it specifically alert consumers to its business model during its sign-up process. However, Facebook does provide links to its terms of service and data policy which set out the legal bases for processing personal data. Consumers can also navigate to a page where they can 'Learn about Facebook ads'[39] via the 'Your ad preferences page', which contains some explanations of how Facebook makes use of consumers' data to show them ads.

[38] Google's Response to the CMA's consultation on the Statement of Scope.
[39] 'About Facebook Ads'.

84. On this page, Facebook explains how it uses data, the controls that consumers have regarding which adverts they are shown and the reasons why certain ads are displayed both on Facebook and on third party websites and applications. This contains short explanations of how consumers' activity can be used to show consumers ads.[40]

Experience when consumers are not signed up or logged-in

85. Overall, the functionality of the social media platforms we reviewed is limited for consumers who either do not have an account with the relevant platform or are not logged-in to this. For example, consumers who do not have a Facebook account or are not logged-in will only be able to access a very limited range of Facebook's webpages, eg those of businesses which have been made publicly viewable. However, some platforms do make use of a consumer's data even when that consumer does not have an account with the platform or is not logged-in to their account. In this section we have therefore focused on the experience of signed-in consumers. Where relevant we have referred to the activities of the platforms and third parties which make use of the data of consumers who are either not signed-up to that platform or signed-in to their account.

Experience when consumers sign up for an account

86. All the platforms we reviewed require consumers to provide certain pieces of personal information before they can sign-up to create an account with the platform. The specific pieces of information that it is mandatory a consumer provides differ by platform. These are summarised in Figure K.16.

[40] This activity includes consumers' interactions with: Facebook company products; other businesses; other websites and apps; and their location data.

Figure K.16: Information required from consumers for sign-up on social media platforms reviewed

	Social Media Platform					
Personal Information required for sign-up?	Facebook	Instagram	Snapchat	Twitter	Pinterest	TikTok
Full Name	✓	✓	✓	✗	✗	✗
Mobile Number or Email Address	✓	✓	✓	✓	✓	✓
Date of Birth	✓	✓	✗	✗	✗[41]	✓
Gender	✓[42]	✗	✗	✗	✗	✗

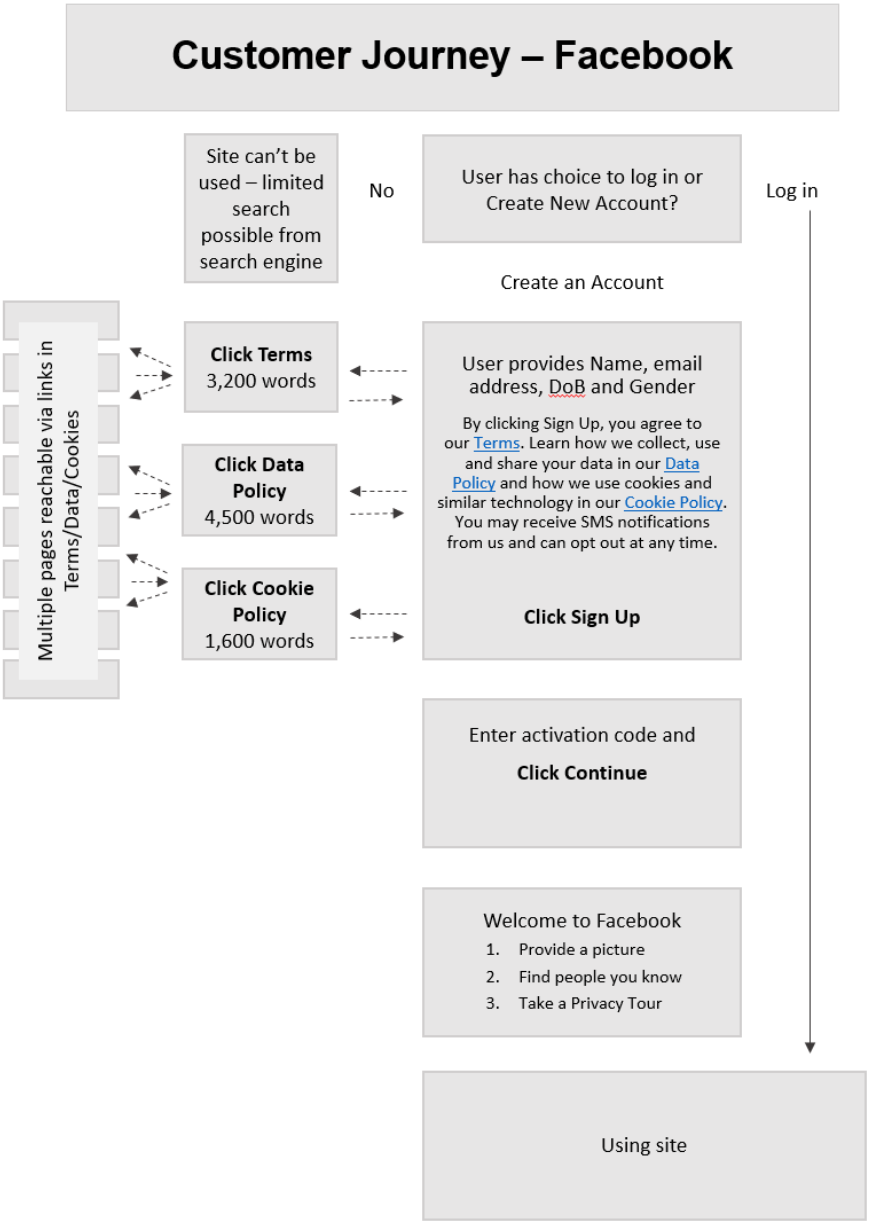
Source: CMA analysis of the information required by platforms for sign-up

Facebook

87. Facebook's sign up process can be completed quickly, with four pieces of information required from consumers on its Sign Up page (which takes the form of a pop-up from its main homepage). There is one subsequent step for consumers to complete before the account is created: entering an activation code which Facebook sends to either the consumer's email account or mobile phone (via SMS), depending on which piece of contact information they used to sign up with. The flowchart below illustrates the complete sign up process for Facebook.

[41] Pinterest does not require consumers to provide their date of birth specifically but does ask them to provide their age.
[42] Facebook asks the consumer to provide their gender during the sign-up process however it is optional to do so. Facebook does require consumers to specify the pronoun they would like to be used when statements are made on Facebook regarding their activity.

Figure K.17: Flowchart illustrating a consumer's journey through Facebook's Sign Up process



Source: CMA analysis of the sign-up process on Facebook.com

88. Facebook's homepage contains limited information about the service provided by the platform. Existing and prospective consumers are told that:

'Facebook helps you connect and share with the people in your life.'

89. No further information is provided on this page regarding the functionality or possible benefits of using the platform. It is made clear that consumers will need to either have an existing account or create a new account to gain access to Facebook's services.

90. Links to Facebook's Terms, Data Policy and Cookie Policy are all provided in the statement above the 'Sign Up' button in small font size text. Each of these

documents is found on a separate webpage(s) which the relevant links navigate to and each is a layered document. Each document is of significant length and Facebook's Privacy Policy alone has been found to take around 18 minutes to read.[43] Facebook told us that it cannot determine the proportion of consumers who accessed its Data Policy when first using its services. A cookie notice will also appear as a banner at the top of the screen, containing a link to the cookie policy, the first time a consumer visits the Facebook website.

91. Not only are Facebook's policy documents lengthy, they are also complex. The study conducted for the New York Times opinion piece indicated that the complexity of Facebook's privacy policy was similar to the type of texts that US college students needed to understand in order to be successful.[44]

92. The sign-up process when accessing Facebook on a mobile device is similar to that of the desktop website, the only difference being that new consumers are asked to provide each of the required pieces of information sequentially on separate pages. The same links to Facebook's Terms, Data Policy and Cookie Policy are provided in an identical statement to the desktop website's, above the Sign Up button on the final page of the process where new consumers are also required to choose a password. The cookie notice is also displayed the first time a consumer visits the website.

93. Other than the four pieces of information listed in Figure K.16, consumers are not required to provide any information to Facebook before signing up and using its service. Facebook stated that consumers are therefore able to choose what further information they share by simply not posting content. However, this does not fully reflect the extent of data collection that occurs once a consumer has created a Facebook account. For example, any interaction a consumer has with their friends' or other consumers' posts, advertising content or Facebook's search facility will result in Facebook collecting some data from this consumer. In addition, other consumers may choose to 'tag' a consumer in a post, photo, video or other content, which may again provide Facebook with further data relating to this consumer. Facebook told us that its policies make clear what information Facebook obtains from users.

[43] We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.' The New York Times, 12 June 2019.
[44] This was based on the Lexile Test, which is a means of measuring a text's complexity based on factors like sentence length and vocabulary difficulty.

94. When consumers have finished creating a new account, they are directed to a screen stating: 'Welcome to Facebook, [consumer's first name]'. They are then presented with prompts to complete the following actions:

- Upload a profile picture
- Find people you know
- Get to know your privacy settings (and, specifically, 'Take a Privacy Tour').

95. By placing these actions in this order, consumers are prompted to both upload a profile picture and find people they know, and therefore to share certain personal information required to complete these actions, before being prompted to familiarise themselves with their privacy settings.

96. If consumers choose to take a Privacy Tour, they are given a short walk-through of some of the basic aspects of how their information and content may be shared with other consumers and application, game and website operators. The privacy tour does not explain how consumers' data may be used by Facebook for the purposes of personalised advertising.

Instagram

97. Instagram is a Facebook product which enables consumers to take photos or videos, customise these with filters and other visual effects and share them with friends or followers on the platform in their 'photo feed,' or to send them directly to their friends. It is primarily designed for use on mobile devices, through its mobile app, but can also be accessed via both a desktop and mobile internet browser.

98. As a Facebook product, Instagram's sign-up process is similar to Facebook's and designed to be completed quickly. Consumers with an existing Facebook account can also use their Facebook account details to log-in to and begin using Instagram. For new consumers without a Facebook account, only three pieces of personal information are required to create an Instagram account: their mobile number or email address; full name; and their date of birth.[45] New consumers are asked to declare whether they are over or under 18 in a pop-up box which also states that consumers can still use Instagram if they are under 18 but that their 'age affects the resources we offer and the way we use your data for ads.' If the consumer selects that they are under 18, Instagram requires them to provide their birthdate. Instagram requires consumers to be

[45] On 4 December 2019 Instagram announced that it would henceforth require consumers to enter their date of birth when creating a new account. For consumers with a connected Facebook account, Instagram adds the date of birth given on their Facebook Profile to their Instagram account.

at least 13 years of age before they can create an account and all new consumers go through the same sign-up process. New consumers are also required to create a username and password.

99. The only subsequent step for new consumers to complete before the account is created is to enter an activation code (which Instagram sends to either the consumer's email account or mobile phone (via SMS), depending on which piece of contact information they provided at sign up).

100. The sign-up process when accessing Instagram on a mobile device is very similar to that of the desktop website, the only difference being that new consumers are asked to provide each of the required pieces of information sequentially on separate pages. The same links to the Terms, Data Policy and Cookie Policy for Instagram are provided and consumers are also implicitly deemed to have agreed to Instagram's terms when they have signed up, rather than explicitly being asked whether they agree to the terms.

101. Once a consumer has signed up to Instagram, they are prompted to find their friends, either via Facebook or their contacts on their mobile device, to add a profile photo, and to allow Instagram access to their photos, camera and microphone. Consumers are not prompted to review their privacy settings specifically during the sign-up process.

Snapchat

102. Snapchat, owned by Snap Inc. ('Snap'), is a multimedia messaging app designed for mobile devices, which is currently available for Android and iOS operating systems only.

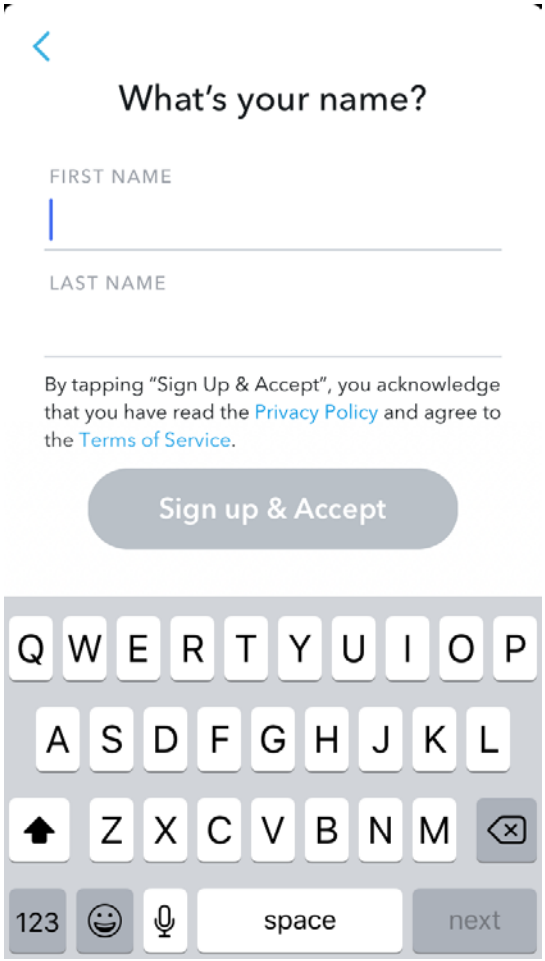
103. Snapchat's sign-up process is similar to Facebook and Instagram's when viewed on a mobile device and/or in their respective apps. However, Snapchat's is conducted within the Snapchat app, once this has been downloaded by a consumer onto their mobile device.

104. To sign-up to Snapchat, new consumers are required to provide the following mandatory pieces of information on separate, sequential pages: first and last name; birthday; and email address.

105. On the first page of Snapchat's sign-up process, text of a small font size is displayed below the spaces for consumers to enter their first and last names, which states that: 'By tapping 'Sign Up & Accept', you acknowledge that you have read the Privacy Policy and agree to the Terms of Service'. Snapchat's privacy policy and terms of service are accessible via hyperlinks embedded in the relevant words in this statement. Below this text, a prominent, large blue

button marked ‘Sign up & Accept’ is displayed, which a consumer must then click to progress to the next stage of the sign-up process.

Figure K.18: Snapchat’s sign-up screen



Source: Screenshot of Snapchat’s sign-up screen in the Snapchat App

Twitter

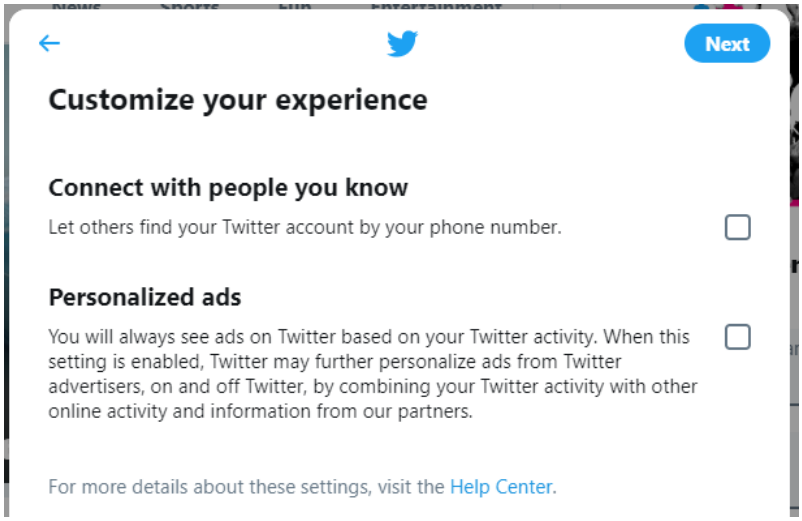
106. Twitter describes itself as a microblogging and social networking service on which consumers create posts and interact with each other, primarily with messages known as ‘tweets’. Twitter differs from most other social media platforms in that it allows consumers who are not signed-up or signed-in to Twitter significant access to consumer-posted content, for example by allowing them to view public tweets, replies and posts. However, to be able to post tweets, ‘follow’ and send direct messages to other consumers and like and retweet their tweets, a consumer must be signed-in.

107. Twitter’s sign-up process is similar to the other social media platforms’ and can be completed either via its website (on a mobile device, desktop or laptop computer), or via Twitter’s app. To sign-up to Twitter, new consumers are required to provide fewer mandatory pieces of information than the other platforms reviewed, with only a username and mobile telephone number

required on the initial sign-up page. Additional information can optionally be provided during the sign-up process, specifically a short 'bio' describing the consumer in up to 160 characters, and a profile picture.

108. On the first screen of Twitter's sign-up process, new consumers are asked to provide their name and either their mobile telephone number or email address. On the next screen, consumers are given options to 'Connect with people [they] know' and to turn on personalised ads, with short explanations of what enabling these options will mean. Both options are deselected by default and consumers can progress to the next stage of the sign-up process without enabling them.

Figure K.19: Screen during Twitter sign-up allowing consumers to opt-in to connecting with people they know and personalised ads



Source: Screenshot of Twitter's desktop website

109. On the next screen, text of a smaller font size is now displayed below the spaces for consumers to enter their name and telephone number or email address, which states that: 'By signing up, you agree to our Terms, Privacy Policy and Cookie Use. You also agree that you're over 13 years of age'. Twitter's terms, privacy policy and cookie use policy are accessible via hyperlinks embedded in the relevant words in this statement. Below this text, a prominent, large blue button marked 'Sign up' is displayed, which a consumer must click to progress to the next stage. This is another example of a clickwrap agreement, where acceptance of the platform's terms is implicit in the act of signing up.

Pinterest

110. Pinterest told us that it does not consider itself to be a social media platform as it is focused on helping its users find ideas and inspiration for their offline lives, rather than providing tools to connect them with other users online.

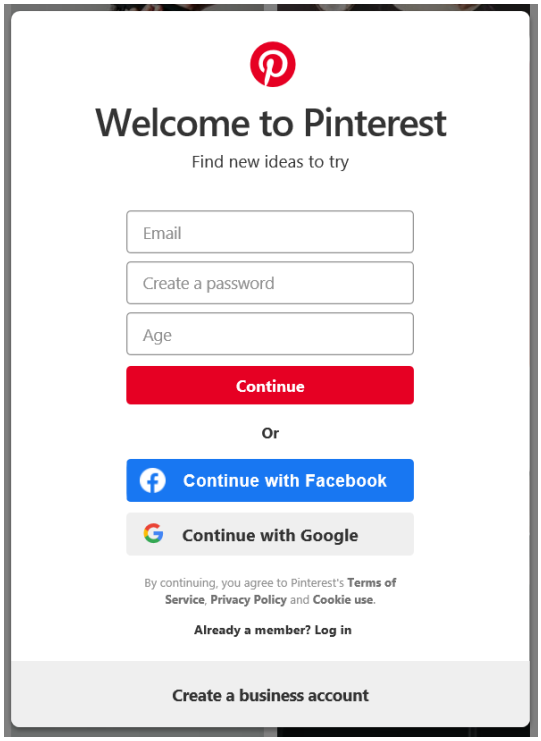
When a consumer has created a Pinterest account, Pinterest will show them visual recommendations (called 'Pins'), which are based on the consumer's interests. Consumers can then choose whether to save (and subsequently organise) these recommendations in collections, called 'Boards', which are centred around a specific topic or theme of interest.

111. There are aspects of the Pinterest platform which are similar to the other social media platforms we reviewed. For example, one of the primary functions it provides consumers is the ability to save images, GIFs and videos relevant to their areas of interest, which can then be found by other Consumers. Consumers are also able to 'follow' other consumers, which means their home 'feed' will automatically be updated with content provided or 'pinned' by these consumers.

112. Consumers can also communicate directly on the platform, by sending written messages, 'Pins', 'Boards' or 'Profiles' to each other. These aspects of the platform mean that we consider it relevant to consider Pinterest alongside the other social media platforms reviewed.

113. Pinterest's sign-up process is similar to the other social media platforms' and can be completed either via its website (on a mobile device, desktop or laptop computer), or via the Pinterest app. To sign-up to Pinterest, consumers are required to provide their email address and age if they wish to create a specific Pinterest account. Consumers may also use existing Facebook or Google account details to begin using the platform.

Figure K.20 Pinterest's sign-up screen



Source: Screenshot of Pinterest's desktop website

114. Text in a smaller font size is displayed some distance below the ‘Continue’, ‘Continue with Facebook’ and ‘Continue with Google’ buttons (all given prominence through contrasting colours) which states that: ‘By continuing, you agree to Pinterest’s Terms of Service, Privacy Policy and Cookie Use.’ Pinterest’s terms, privacy policy and cookie use policy are accessible via hyperlinks embedded in the relevant words in this statement. This is another example of a clickwrap agreement.

115. Before using the platform, consumers are then asked to state which gender they identify as (Female, Male or non-binary) and to choose a minimum of five areas of interest from a pre-determined list.

TikTok

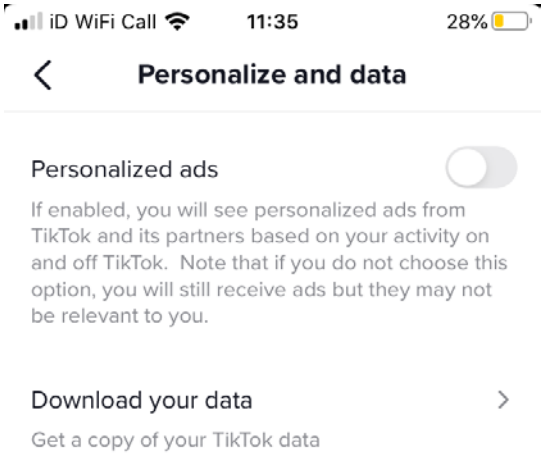
116. TikTok Inc (TikTok) is the provider of the TikTok app in the UK. TikTok is part of the ByteDance group of companies. The TikTok app is a platform for viewing, creating and sharing short videos on mobile devices. TikTok allows consumers to create and upload videos directly from their smartphones, enabling users to add filters, stickers, effects and music to their videos.

117. Consumers can view videos recommended for them through a personalised ‘For You’ feed or they can search specific types of videos via a search bar. TikTok’s services are predominantly accessed via the TikTok app although TikTok also operates a website which provides information about TikTok and content that is ‘trending’ on the platform.

118. Unlike the majority of the other social media platforms reviewed, TikTok allows consumers to watch videos and scroll through content without opening an account or directly providing any personal information. However, TikTok states in its privacy policy that it will still collect information about a consumer if they download the app and interact with TikTok’s platform, even if they do not create an account.

119. When a consumer first opens the TikTok app, a notice is displayed on the first screen, prompting them to review TikTok’s privacy and cookies policies. Below this message is an option for the consumer to ‘Manage settings’. If this is selected, the consumer is taken to the ‘Personalize and data’ settings page, where they can choose to turn on personalised ads.

Figure K.21: TikTok's 'Personalize and data' page



Source: Screenshot of the TikTok app

120. To access or use some of TikTok's services, a consumer must create a TikTok account. If a consumer chooses to create an account, they are required to provide their date of birth and their telephone number or email address, and to set a password on successive screens. They are then able to proceed using the app as a logged-in user. On each screen of the sign-up process, consumers are told that by continuing, they confirm that they agree to TikTok's terms of use and have read and understood its privacy policy. This is another example of a clickwrap agreement.

Terms and conditions

121. The social media platforms we reviewed all had lengthy terms and conditions, privacy and data policies or statements. These would all take an average consumer significant time to read and comprehend before deciding whether to create an account with the platform.

122. Some, such as Facebook, set out documents in a 'layered' format, which are intended to make this material more accessible and easier to navigate, allowing consumers to more quickly focus on a specific area of the document if it is of interest to them.

123. However, even layered documents remain lengthy overall and do not always highlight important information for consumers' attention, such as how their data is used for advertising. Instead, the platforms reviewed provide links to the text on certain subject headings within the documents. The word count comparison below focuses on each of the platforms' primary policies, for example their terms of service/use, and their privacy/data and cookie policies. The figures do not count the additional text of further documents, often made available by the platforms through embedded links within their primary

policies. As shown in Figure K.22, the platforms' terms of service and key policies are all over 8,000 words in length and spread over multiple documents.

Figure K.22: Comparative length of social media platforms' terms and policies

Terms / Policies	Social Media Platform					
	Facebook	**Instagram**	**Snapchat**	**Twitter**	**Pinterest**	**TikTok**
Accessible from front page and sign-up page?	Yes	Yes	Yes	Yes	Yes	Yes
Approximate length in Words	**10,100** in 3 parts (4,000 Terms of Service, 4,500 Data Policy 1,600 Cookie Policy)	**9,100** in 3 parts[46] (2,400 Terms of Service, 4,500 Data Policy, 2,200 Platform Policy)	**8,200** in 2 parts (4,400 Terms of Service, 3,800 Privacy Policy)	**11,300** in 2 parts[47] (5,700 Terms of Service, 5,600 Privacy Policy)	**8,500** in 3 parts (3,100 Terms of Service 4,400 Privacy Policy 1,000 Cookie Policy)	**11,500** in 3 parts (6,200 Terms of Service 3,500 Privacy Policy 1,800 Cookie Policy)
Clickwrap agreement used?	Yes	Yes	Yes	Yes	Yes	Yes
Flesch reading ease score	**44.1** ('Difficult to read')	**41.6** ('Difficult to read')	**48.7** ('Difficult to read')	**38.7** ('Difficult to read')	**48.3** ('Difficult to read')	**42.5** ('Difficult to read')

Source: CMA analysis of the terms and conditions documents of these platforms (based on the published documents available on 1 June 2020.)

124. For platforms accessed via a mobile device, difficulties consumers face in understanding the implications of these documents may be exacerbated when reading them on the small display screens of such devices. Consumers attempting to view such documents on their mobile devices will have to scroll through numerous screens to read them in their entirety. They may also find it more difficult to navigate to specific sections of the documents that may be of interest to them and may be more quickly fatigued when reading the documents than when doing so on a desktop or laptop computer.

[46] Instagram shares Facebook's Data Policy but has its own Terms of Service and Platform Policy
[47] Twitter's 'User Agreement' also includes the 'Twitter Rules and Policies' which set out the conduct permitted by consumers when using Twitter's services. The length of this document has not been included in the assessment above.

Clickwrap agreements

125. Facebook, Instagram, Snapchat, Twitter, Pinterest and TikTok all use clickwrap agreements to obtain consumer acceptance of their terms of service and other policies. With these clickwrap agreements, new consumers are deemed to have accepted the platforms' terms and policies if they complete the relevant sign-up process.

How do consumers find out about their terms and make changes?

126. The social media platforms we reviewed profess to provide consumers with easy access to their terms of service, privacy and data policies and settings to control these. However, we found that it is not always obvious how to access these documents on the platforms and the settings themselves may only be visible after navigating through multiple menus. This may discourage consumers from engaging with the settings available to them and encourage inertia to the default settings.

Facebook

127. Facebook's Data Policy is accessible via links on Facebook.com and in the Facebook and Messenger apps. Facebook has also introduced a series of 'interactive tools' to explain how consumers' data is shared and displayed. However, Facebook's settings webpage can only be reached via a menu whose location is not prominently displayed on the Facebook website.

128. As is the case with most other pages on the Facebook desktop website, there are multiple (10) links displayed to other areas of the website at the bottom of its settings page. These include a link also entitled 'Privacy' which, when clicked, directs consumers to Facebook's Data Policy.

Instagram

129. Consumers can access Instagram's Terms of Use and the Facebook Data Policy, via links which appear at the bottom of most pages on the Instagram website or app. However, these are not prominently displayed and appear alongside multiple other links to additional information about the platform.

130. To adjust their privacy settings, consumers must navigate to the 'Privacy and Security' page of their Instagram account settings. On neither the desktop website or the mobile or app versions of Instagram are these settings clearly or prominently displayed. On the desktop website, these settings are found on the consumer's profile page and accessed by clicking on a 'cog' icon next to an Edit Profile button.

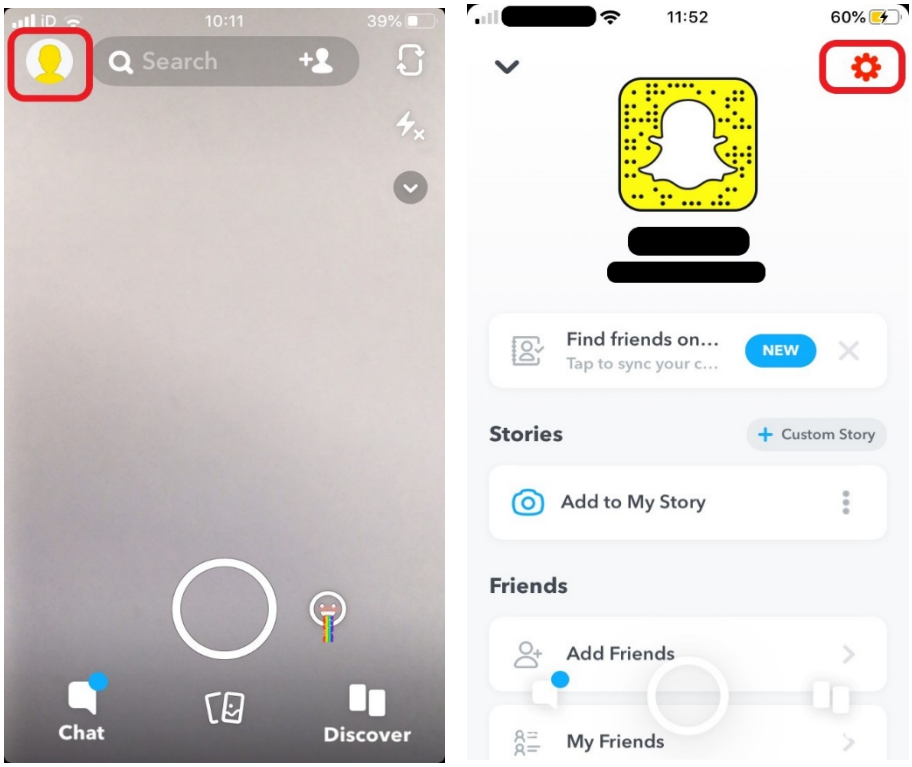
131. Without knowing this navigational path, there is no clear and prominent indication to consumers that this series of screens must be navigated in order to change their privacy settings. By default, consumers' 'Activity Status' will be shown to other consumers who choose to follow or message them.

132. On the mobile app, the privacy settings are found by swiping upwards, selecting settings, then selecting the 'Privacy' option. The consumer is then presented with a series of options classified under this category. Again, there is no clear and prominent indication to consumers that this series of screens must be navigated in order to change their privacy settings on the mobile app.

Snapchat

133. Snapchat is only available to consumers via its mobile app. Consumers who want to access Snapchat's terms of service, privacy policy, and information on its advertising must navigate to these via Snapchat's 'Settings' menu. As shown in Figure K.23, to reach the settings menu consumers must navigate to their profile page from Snapchat's opening page. This is the current image seen by the camera of a consumer's mobile device, overlaid with several buttons. Clicking on the button in the top left of the homepage, illustrated with a silhouette of a person's head and shoulders, takes consumers to their profile page. The button to reach Snapchat's settings menu is then quite prominently displayed on the profile page as a red cog.

Figure K.23: Snapchat app Opening Page (L) and example Snapchat User Profile Page (R)



Source: Screenshot captured on the Snapchat app.

134. The options in Snapchat's Settings are relatively numerous and it may not be obvious to consumers where certain controls are located. For example, controls relating to consumers' preferences regarding advertising are located via the 'Manage' button in the Additional Services section of the Settings menu. Other links and controls relating to consumers' privacy, such as the links to Snapchat's terms of service and privacy policy and the link for them to download their data, are located towards the bottom of the list of options, with consumers having to scroll through the equivalent of two to three screens of options to reach these.

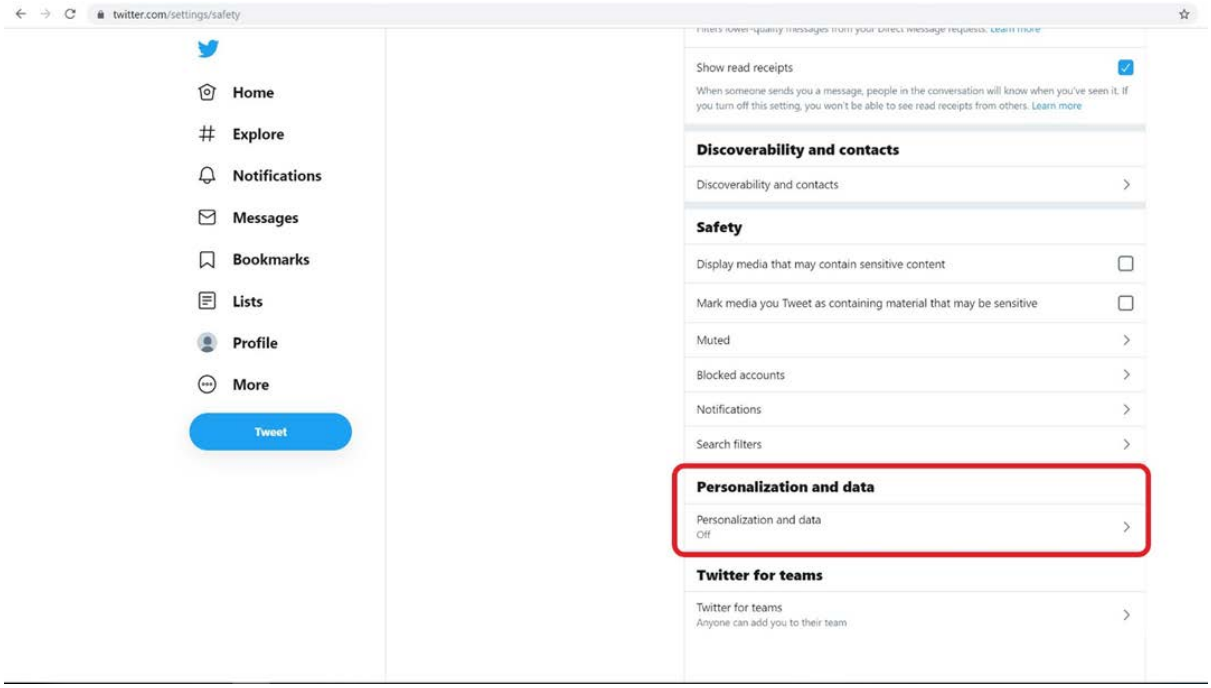
135. Controls relating to which of consumers' personal information and content other consumers using Snapchat can see are more prominently displayed on the second screen of the Settings menu. These are located under the heading 'Who can…'

Twitter

136. Consumers can access Twitter's terms of service, privacy and cookies policies, and information on how its advertising works via links on their Twitter homepage. However, these are not prominently displayed, and indeed not initially visible as they appear at the bottom of the right-hand side of the homepage, in un-bolded text. To access and adjust their privacy settings, consumers must click on the 'More' button on the left-hand side of the page, where they are then presented with a link to reach options regarding their 'Settings and privacy'.

137. When consumers click on this link, they are taken to their 'Settings' page, which includes 'Privacy and safety' options under the second category of settings. In this category of settings, options regarding 'Personalization and data' can be accessed 'below the fold' of the webpage, if consumers scroll down.

Figure K.24: Screenshot showing the location of Twitter's Personalization and Data settings



Source: Screenshot of Twitter's settings page

138. When this link is clicked, consumers are then presented with some options regarding the use of their data for the personalisation of ads. The display of these options on the mobile version of Twitter's website is very similar to that of the desktop website, with the primary difference being that the 'More' button on the homepage is represented only by an ellipsis symbol.

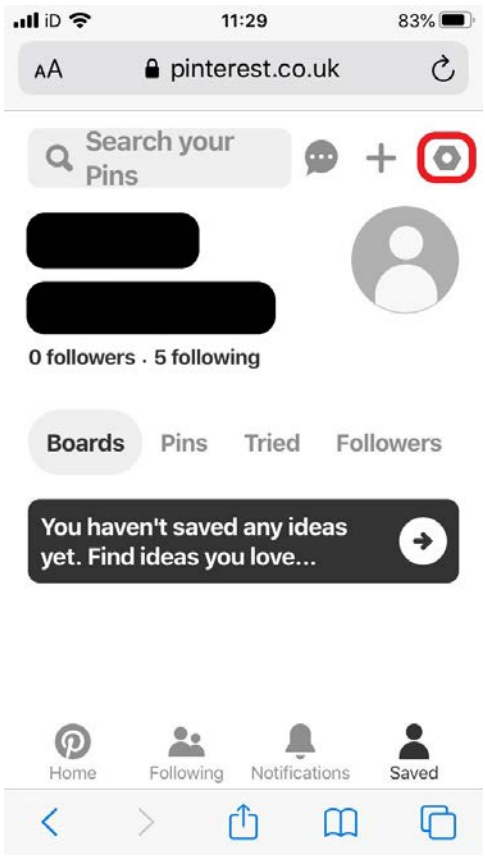
139. On neither the desktop or mobile versions of Twitter's website are there clear and prominent indications to consumers that this series of screens must be navigated in order to change their settings regarding their privacy and the use of their data for personalised advertising.

Pinterest

140. Consumers can access Pinterest's terms of service, privacy and cookies policies, and information on how its advertising works via a link in the 'Settings' menu on the consumer's homepage. This menu is accessed via a small ellipsis symbol located in the top right corner of the homepage.

141. The location of these settings is less prominent on the mobile version of the Pinterest website. On a consumer's home page, displayed when they first access the site, consumers must first navigate to the page entitled 'Saved' via a location bar at the bottom of the page. The settings are then found via a hexagon shaped button in the top right of the screen. This navigational path may not be obvious to a consumer using the app for the first time.

Figure K.25: Screenshot showing the location of Pinterest's settings (on a mobile device)



Source: Screenshot of Pinterest's (mobile) website

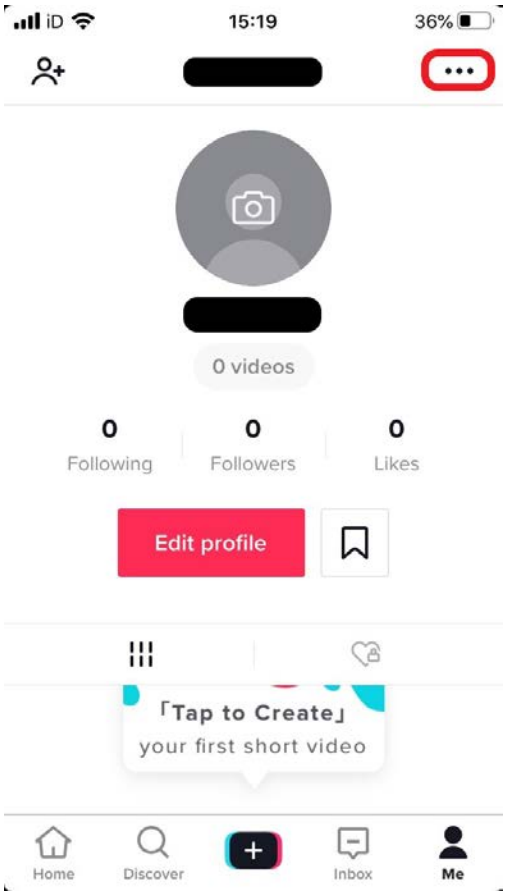
142. In its privacy policy, Pinterest also states that consumers may object to Pinterest processing their information, including using this information to send consumers marketing emails or push notifications. However, Pinterest does not state here how this should be done or what outcome consumers can expect if they do make an objection.

TikTok

143. TikTok's services are primarily accessed via its mobile app. As described, consumers are prompted to read TikTok's privacy and cookie policies when they first use the app and, if they choose to create an account, will also be prompted to read its terms of use.

144. If consumers want to access TikTok's policies or privacy settings at other times, they must navigate to their profile via a link labelled 'Me' in the bottom right of each page. They must then navigate the 'Settings and privacy' menu, via a small ellipsis located in the top right of this page. Links to TikTok's terms of use and privacy policy are near the bottom of this menu. Links to consumers' privacy and safety settings are available at the top of this menu.

Figure K.26 TikTok's profile page showing the location of the settings and privacy menu



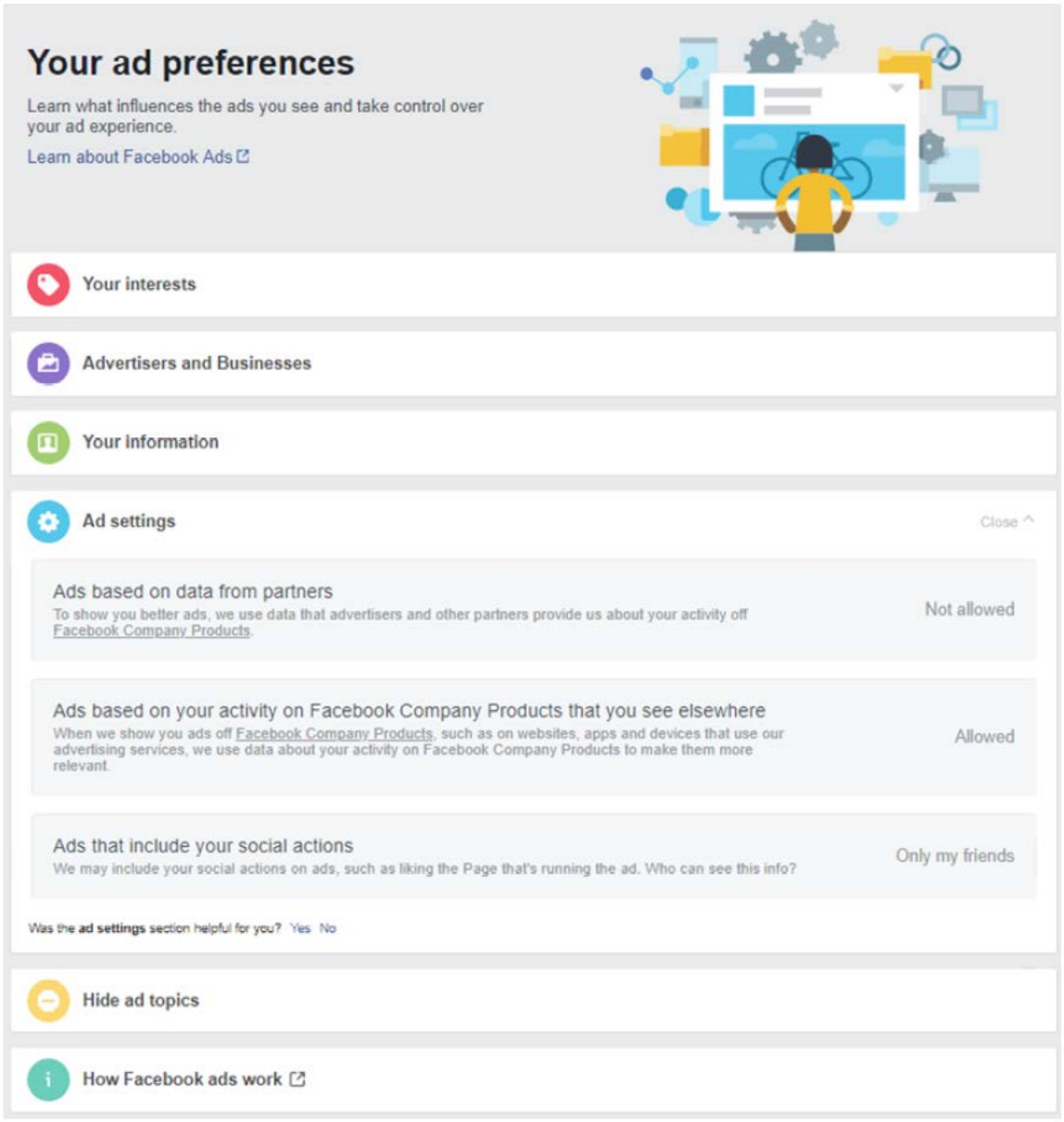
Source: Screenshot of the TikTok app

Advertising settings and personalised ads

Facebook

145. Facebook states on its website that consumers can prevent certain types of data from being used for ad personalisation. For example, this message is conveyed in the 'Ad Settings' on Facebook's 'Your Ad Preferences Page', as shown in Figure K.27.

Figure K.27: Screenshot of Facebook's 'Your ad preferences' page



Source: Screenshot of Facebook's 'Your ad preferences' page

146. Facebook's ad preferences are also accessed via one of the 20 links on the left-hand side of the Settings page. Consumers have some control over the pieces of their personal information Facebook can use to determine whether to show certain ads to them. However, it is not possible for consumers to disable the personalisation of ads completely. It is also not possible for consumers to prevent the sharing of their data for any underlying analysis which Facebook undertakes to determine which personalised adverts might be deemed appropriate to be shown to them.

Instagram

147. Instagram provides consumers with minimal control over what ads they see, what personal data is shared with advertisers and how this data is used on the Instagram platform itself.

148. Consumers using Instagram must visit the 'Your ad preferences' area of Facebook to exercise controls on how Facebook uses information from partners to show them ads on Instagram. In the section of Instagram's Help Centre entitled 'Ads on Instagram', Instagram states: 'if we can determine you've made a choice on other Facebook Company accounts that you use, we'll apply your ads preferences to them as well.'

Snapchat

149. Snapchat allows consumers to prevent advertisers from showing them ads based on information about them collected on third party websites and services by Snapchat. In the 'Advert Preferences' section of a consumer's settings on Snapchat, consumers can opt out of:

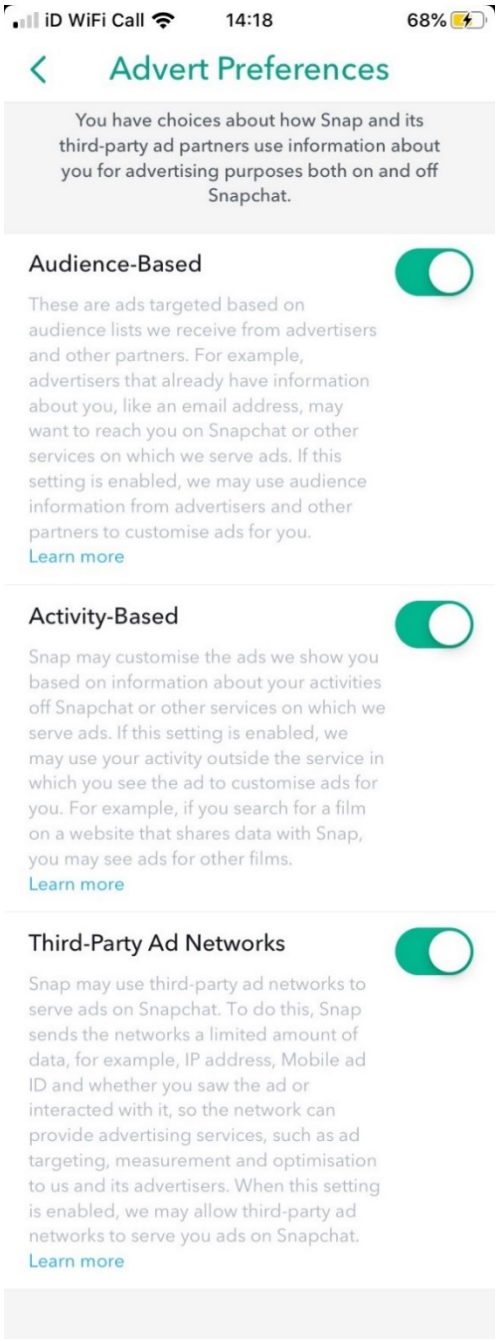
(a) 'Audience-Based Ads', which are based on audience lists Snapchat receives from advertisers and its other commercial partners;

(b) 'Activity-Based Ads', which are based on information about consumers' activities away from Snapchat or other services on which Snapchat serves ads; and

(c) 'Third-Party Ad Networks', whereby Snapchat sends data to a third-party ad network so that they can provide ad targeting, measurement and optimisation to Snapchat and other advertisers.

150. By default, all these types of ads will be shown to consumers who have not updated their settings on Snapchat. The screenshots below show the options selected on the 'Advert Preferences' screen, accessible via the 'Manage' button on Snapchat's Settings.

Figure K.28: Default 'Advert Preferences' on Snapchat



Source: Screenshots of 'Advert Preferences' page on the Snapchat app

151. Consumers may also opt out of being shown some types of personalised advertising by enabling specific features on their mobile devices.

152. Despite consumers having the ability to opt out of being served certain personalised ads, they will still see ads when using Snapchat and other Snap Inc. services regardless. These ads may also still be based on consumers' information, gathered by Snap when they are using Snapchat's services. For example, consumers may still see ads based on their activity on Snapchat and other Snapchat services, even if they have opted out of the three types of personalised advertising described above.

Twitter

153. Twitter provides some degree of control to consumers with regards to personalised ads. However, this again does not amount to an 'opt-out'. Twitter states in its 'Personalization and data' settings, that it will always use information it gathers from consumers' activity on the platform, including information regarding consumers' devices, where they signed up and their current location, to personalise both the ads consumers see and their experience when using the platform.

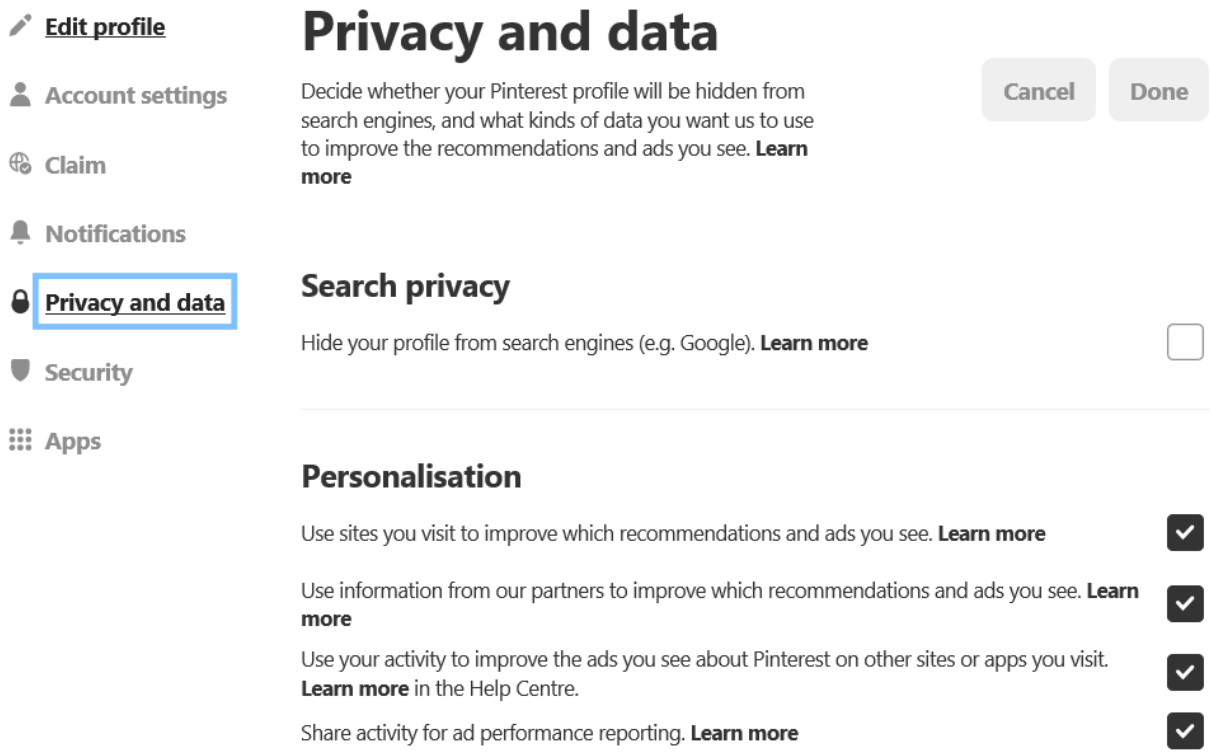
154. Twitter only allows consumers to prevent Twitter from further personalising the ads they see and their experience on the platform. Consumers are able to prevent or allow Twitter from: combining their on-platform activity with personal information and information on their online activity which Twitter has obtained from its partner organisations; making inferences about consumers' identities based on devices and browsers they haven't used to log-in to Twitter; personalising ads and content based on locations a consumer has visited in addition to their sign-up and current locations.

155. Twitter allows consumers to prevent it from sharing non-public data, such as the content they've viewed or their interests with certain of Twitter's business partners for the purposes of personalised advertising and brand marketing.

Pinterest

156. Pinterest provides consumers with the ability to turn off personalised advertising. In its privacy policy, it states that only 'if [a consumer's] settings permit', will it allow certain service providers to collect and use information on Pinterest to create personalised ads. Pinterest also states that consumers can choose whether it uses information to customise its service by visiting their Pinterest account settings. Here, consumers can prevent Pinterest from using information about their activity, gathered both on Pinterest and from its partners to 'improve the recommendations and ads [they] see'.

Figure K.29 Privacy and data options on Pinterest, showing the default settings



Source: Screenshot of Pinterest's website.

157. In its privacy policy, Pinterest states that consumers can prevent it from using their activity outside of Pinterest to personalise their experience by changing the settings on their browser's 'Do not track' feature, in addition to turning off personalisation in their Pinterest account settings.

TikTok

158. TikTok provides users with a binary choice of either being served personalised ads or not. TikTok told us that data is collected for the purpose of optimising personalised advertising but is only used to serve personalised advertising on a consumer if the consumer switches this on.

What happens when changes are made?

Facebook

159. When changes are made to Facebook's Data Policy, Facebook prompts consumers to review the updated policy, for example it will publish a series of posts in the 'Newsroom' area of its website explaining the changes. Prior to

the GDPR coming into effect, Facebook told us that all its UK consumers were required to complete a 'User Engagement Flow' in order to continue using Facebook's services. This also prompted consumers to review Facebook's updated Data Policy. Where Facebook has the email address of signed-up consumers, an email notification was sent informing them of updates to its Data Policy, and where it has consumers' mobile telephone numbers, a similar SMS notification was sent.

160. Any UK consumers that did not complete the GDPR related User Engagement Flow by 25 May 2018 could not continue to access their Facebook profiles but were permitted to download or delete their data if they did not want to continue using Facebook's services. Facebook told us that, unlike its Terms of Service, as its Data Policy is a privacy notice and relies on a number of legal bases under the GDPR to process user data, and as the privacy policy is also not a contract, Facebook is not required to obtain consent from consumers to this policy, either on creation of an account or following any changes to the policy once they had created an account.

Instagram

161. Facebook's Data Policy also applies to consumers using Instagram and a link to this is located at the bottom of most webpages on the Instagram website.

162. Facebook told us that prior to its roll-out of new terms of use and data policy for Instagram on 19 April 2018, its European consumers were shown a promotion at the top of their Instagram feed indicating that the Instagram Terms of Use and Data Policy were changing. Until 24 May 2018, consumers had the option to engage with the promotion, at which point they were presented with a screen notifying them that 'if [they] agree to our new Terms and continue using Instagram, Facebook Ireland will be the official corporate entity responsible for [their] data'. The screen also notified them about the new Data Policy, which addressed processing for Instagram. The next screen advised the consumer that Instagram 'need[s] you to agree to [the Terms of Use] before continuing to use Instagram' and the consumer had to click 'Agree to the Terms' to proceed to use Instagram.

163. Facebook stated that any consumer who did not voluntarily engage with the promotion before 24 April 2018 was sent an activity notification in the app and, if a consumer had added an email address, an email with the relevant information. Consumers who did not engage with the User Engagement Flow or agree to the Instagram Terms of Use through the email notification were blocked from accessing their profile until they agreed to the Terms of Use.

Snapchat and Twitter

164. Snap told us that when a 'material change' is made to its Privacy Policy, it will provide a pop-up notice to consumers when they open the Snapchat app. This contains a disclosure that the Privacy Policy has been updated, which includes a general statement about the update and a link to the revised policy.

165. Snap said that 'non-material changes' to the Privacy Policy are communicated by a change in the date of the Privacy Policy at the top of the policy and may sometimes be communicated via an in-app pop-up.

166. Twitter told us that when 'material changes' are made to its privacy policy, Twitter will notify its account holders of the change, either via an email or in-application notification. These notifications will include a link to Twitter's updated privacy policy.

Pinterest

167. In its privacy policy, Pinterest states that any changes will be posted on the webpage containing the policy and that if consumers continue to use Pinterest after the changes come into effect, they indicate their agreement to the new policy. Pinterest also states that if the changes are significant, it may provide a more prominent notice or get consumers' consent, as required by law.

168. Pinterest told us that when there is a substantive or material change to the Privacy Policy, Pinterest sends an email to all email addresses associated with its European consumers explaining the changes that have been made and when the new version of the Privacy Policy will apply.

TikTok

169. TikTok told us that when there is a change in its privacy policy, consumers will receive a notification when they open the TikTok app.

170. TikTok told us that it will also provide consumers with a pop-up notification and a hyperlink to its new privacy policy, when this is rolled out.

Are settings changed when terms are updated?

Facebook and Instagram

171. Facebook told us that when it updates its Data Policy for its Ad-Supported Services (which include Instagram), consumer settings are 'generally retained'. This approach has remained consistent since the implementation of

the GDPR. When Facebook revised its Data Policy in April 2018, it did not change any existing consumer settings or reset these to a default position.

Snapchat

172. Snap told us that it does not 'reset' user privacy settings, and that it provides notice of material updates to its Privacy Policy through a pop-up notice at app-open. Snap said that this notice explains the material aspects of the update and links to the Privacy Policy, enabling users to review the changes, and if Snap were offering a new setting, make an active choice regarding the setting.

Twitter

173. Twitter told us that when its privacy policy is updated, its account holders can follow a hyperlink to their settings from the policy and make any changes there. This suggests that Twitter may make changes to consumers' settings when its policies are updated.

Pinterest

174. Pinterest told us that when it updates its privacy policies, users' preferences are retained.

TikTok

175. TikTok told us that when it updates its privacy policy, a consumer's original preferences are retained.

Tracking and collection of data from consumers with a social media account off-platform, including by third parties

Facebook and Instagram

176. Facebook's Data Policy states that third party websites and apps may choose to integrate certain Facebook services into their website. An example is 'Facebook Login' which allows consumers to log into these websites/apps using their Facebook account details.[48] When consumers log-in to third party websites in this way, certain data is sent to Facebook. This includes data from the browser or mobile software development kit (SDK), including the

[48] Facebook's Data Policy.

consumer's IP address, browser type and version. A cookie file is also sent to Facebook which contains data associated with the browser. Facebook states that this information is used for authentication and security purposes, among other uses.[49]

177. When a consumer has logged into a website or app via Facebook Login, these websites/apps may also choose to send Facebook additional data about the consumer's activities on that site or app, eg whether the consumer made a purchase on this website/app.

178. The terms and conditions for Facebook Business Tools require third parties to gather consent from consumers regarding the use of their personal information, when they are active on these third parties' websites.[50] Facebook's Data Policy states they never sell data to third parties, but data is used within the group of Facebook products.

Snapchat

179. In its privacy policy, Snap states that it may collect information about consumers from the following: other consumers; Snap's affiliates; and other third parties.[51] Examples of how this data collection may occur, which Snap provides in its privacy policy are:

- If a consumer links their Snapchat account to another service (like Bitmoji or a third-party app), Snap may receive information from the other service, like how the consumer uses that service.
- Advertisers, app developers, publishers, and other third parties may share information with Snap as well. Snap may use this information, among other ways, to help target or measure the performance of ads.
- If another consumer uploads their contact list, Snap may combine information from that consumer's contact list with other information it has collected about the consumer.

180. In Snapchat's terms of service, Snap also states that If consumers use a service, feature, or functionality that is operated by a third party and made available through its services (including services jointly offered by Snap with the third party), each party's terms will govern the respective party's

---

[49] These uses are described at length in Facebook's Data Policy under the headings: To provide, personalise and improve our Products; To provide measurement, analytics and other business services; To promote safety, integrity and security; To communicate with users; and To research and innovate for social good.
[50] Facebook Business Tools Terms.
[51] Snapchat's Privacy Policy.

relationship with the consumer.[52] Snap states that it is not responsible or liable for a third party's terms or actions taken under the third party's terms.

181. In Snapchat's privacy policy,[53] Snap states that its services may contain third-party content and 'integrations', and that through these, consumers may be providing information to the third party as well as to Snap. Snap states that it is not responsible for how those third parties collect or use consumers' information and that it encourages consumers to review the privacy policies of every third-party service that they visit or use.

Twitter

182. Twitter told us that its ad partners and affiliates share information with Twitter regarding consumers. This includes consumers' browser cookie IDs, mobile device IDs, hashed email addresses, demographic or interest data, and content viewed, or actions taken on a website or app. Twitter said that this information is used for digital advertising.

183. Twitter's privacy policy states that some of its ad partners, particularly advertisers, allow Twitter to collect similar information directly from their websites or apps by integrating Twitter's advertising technology into their services.[54]

184. Twitter's privacy policy also states it may receive information about consumers from third parties who are not its ad partners, such as others on Twitter, partners who help Twitter evaluate the safety and quality of content on its platform, its corporate affiliates, and other services consumers link to their Twitter accounts.

185. The privacy policy states that consumers may choose to connect their Twitter account to accounts on third-party services, and that these services may send Twitter information about consumers' accounts on that service. Twitter states that it uses the information it receives to provide consumers with features like cross-posting or cross-service authentication, and to operate its services.

186. Twitter allows consumers to control some of the additional information that it receives from them, for example whether they are shown interest-based ads on and off Twitter and whether Twitter can keep track of websites where consumers will see Twitter content. Although consumers can opt out of being shown interest-based advertising via Twitter's 'personalization and data

---

[52] Snap Group Limited Terms of Service.
[53] Snap's Privacy Policy.
[54] Twitter's privacy policy.

settings' consumers cannot remove themselves from advertisers' audiences. Whilst consumers can review their demographic and interest data from Twitter's ads partners, consumers cannot control how these ad partners derive this data.[55]

187. In its privacy policy,[56] Twitter states that if a consumer shares information such as their direct messages or protected Tweets with someone else who accesses Twitter through a third-party service, then that information may be shared with the third-party service. Twitter does not provide notice to an individual consumer when such information sharing has occurred.

188. Twitter also states in its privacy policy that it uses a variety of third-party services to help operate its services, such as hosting its blogs and wikis and for web analytics. Twitter states that it may share consumers' private personal data with such service providers subject to obligations consistent with its privacy policy and any other 'appropriate confidentiality and security measures', on the condition that the third parties use this private personal data only on Twitter's behalf and pursuant to its instructions.

Pinterest

189. In its privacy policy, Pinterest states that it may infer information about consumers' education or professional experience based on their activity when they link their accounts to accounts they have with third parties such as Facebook and Google.

190. Pinterest states that it obtains information about consumers' activity outside Pinterest from its affiliates, advertisers, partners and other third parties. For example, some websites or apps use Pinterest features such as its 'Save' button, which can also be installed by consumers on their browsers. If so, Pinterest will collect log data from these sites or apps.

191. Pinterest also states that online advertisers or third parties share information with it to measure, report on or improve the performance of ads on Pinterest, or to work out what kinds of ads to show consumers on or off Pinterest. This includes information about consumers' visits to an advertiser's site or purchases they have made from them and information about consumers' interests from a third-party service. Such information may also be used by Pinterest to determine which ads to show consumers.

---

[55] On the webpage 'Interests from Twitter partners', there is no indication that consumers can prevent Twitter's ad partners from determining what their interests are.
[56] Twitter's Privacy Policy.

TikTok

192. In its privacy policy, TikTok states that whilst consumers may choose to share certain data from third parties with TikTok, it may collect some such data automatically. For example if a consumer registers for a TikTok account using another social media account (eg Facebook, Google, Instagram or Twitter), they will provide TikTok with their username and public profile.

193. TikTok also states that it will share consumers' device ID with measurement companies, so that it can link consumers' activity on TikTok with their activity on other websites. TikTok states it will then use this information to show consumers adverts which may be of interest to them.

Tracking and collection of data from consumers without an account

Facebook and Instagram

194. Facebook told us that it does not track or create profiles for consumers who do not use Facebook products. However, Facebook does receive information from such consumers when they visit a publicly open Facebook page or third-party website which has chosen to integrate Facebook Pixel or Facebook's social plugins. Facebook's servers will automatically log the fact that a particular browser visited the third-party website. If the consumer does not have cookie-blocking technology enabled on their browser, information regarding their browser, including the IP address, browser type and version will be shared with Facebook via Facebook Pixel. A cookie file containing data associated with the browser and additional data relating to the cookie's functionality will also be shared with Facebook.

195. Facebook told us that this data would be for security, website and product integrity purposes, and to allow third-party website operators to obtain insights into consumers' use of their websites. Facebook said that this data would not be used to show consumers who do not use Facebook products personalised advertising.

196. The level of data collection and sharing which occurs when visiting websites/apps which have chosen to integrate Facebook's services and the purposes to which this data is put are not therefore materially different for consumers who do use Facebook products and those who do not.

Snapchat

197. Snapchat's terms of service and privacy policy indicate that Snap does not track or collect data from consumers who do not have a Snapchat account.

Consumers cannot use Snapchat, without first signing-up and logging-in to the app.

Twitter

198. Twitter allows consumers without a Twitter account to access significantly more posted content than other social media platforms. Twitter does track and collect data from such consumers who do not have a Twitter account. Twitter's privacy policy states that it provides consumers who do not have an account with a version of Twitter's 'personalization and data settings' and 'Your Twitter data' to allow them to see the data and settings for a logged-out browser or device that they have used to access Twitter.[57] This is separate from any Twitter account that uses that browser or device.

Pinterest

199. Consumers cannot use Pinterest, without first signing-up and logging-in to their account. Pinterest's terms of service and privacy policy indicate that Pinterest does not track or collect personal data from consumers who do not have a Pinterest account.

TikTok

200. TikTok states in its privacy policy that it will still collect information about a consumer, if they download the app and interact with TikTok's platform, even if they do not create an account.

201. TikTok states that this includes: how consumers engage with its platform and interact with content they are shown, the ads they view, videos they watch and problems encountered; content they like and/or save; and the users they follow. TikTok infers consumers' preferences, including their interests, gender and age for the purpose of personalising content. TikTok also processes information about consumers' followers, the likes they receive and responses to content they upload, to promote their content to other consumers.

Data retention policies

Facebook and Instagram

202. Facebook told us that it stores consumer-identifiable data until either it is no longer required for the provision of its services and products, or until a

[57] From page 7 of Twitter's Privacy Policy.

consumer's account (or content) is deleted by the consumer. Facebook said the length of time data is retained is determined on a case-by-case basis, depending on the nature of the data, the purpose for which it is collected and processed, and relevant operational (eg service integrity and security) or legal retention needs.

Snapchat

203. In the 'How Long We Keep Your Information' section of Snapchat's privacy policy, Snap explains that most messages sent in Snapchat will be automatically deleted by default from its servers after it detects they've been opened by all their recipients or expired.[58] Snapchat contains a link to the 'Snapchat Support' page of its website where further information on when it deletes 'Snaps and Chats' is provided.[59] Snap also states that it stores other information for longer periods of time. For example, Snapchat stores consumers' basic account information (eg their name, phone number, email address and friends list) until consumers request that Snap deletes them.

204. Snap states that it stores location information for different lengths of time based on how precise it is and which services consumers use. For example, for consumers using the 'Map', Snap stores information about their favourite places for up to 40 days.

205. Snap also states that it is constantly collecting and updating information about consumers' likes and dislikes but does not indicate how long such information is retained for.

Twitter

206. Twitter did not specify how long it retains consumers' data. Twitter told us only that its retention/deletion policies for a given category of data depend on a variety of factors including but not limited to, for example, the legal basis for the data collection and its business need for continued use of the data. Twitter told us it maintains the same retention and deletion policies for UK consumers as it does for international consumers.

Pinterest

207. In the 'How Long We Keep Your Information' section of Pinterest's privacy policy, Pinterest states only that it will keep consumers' information for as long as it needs it to provide Pinterest to them and fulfil the purposes described in

---

[58] Snap's Privacy Policy.
[59] Snapchat Support – 'When does Snapchat delete Snaps and Chats'.

its privacy policy. Pinterest states that this is also the case for anyone that it shares consumers' information with and who carries out services on its behalf. Pinterest states that when it no longer needs to use consumers' information and there is no need for it to keep it to comply with its legal or regulatory obligations, it will either remove it from its systems or depersonalise it so that it cannot identify the consumer it has come from.

208. Pinterest does not state specifically in its privacy policy how long it will retain any of the information it collects from consumers.

TikTok

209. In its privacy policy, TikTok is not specific about the length of time it will keep hold of consumers' information. TikTok states only that it will retain consumers' information for as long as it is necessary to fulfil its contractual and legal obligations, its legitimate business purposes and to conduct a defence in relation to potential disputes.

Deletion

210. All of the social media platforms reviewed allowed consumers to delete their accounts with the platform and download their data, although there are slight variations in their approaches.

211. Figure K.30 shows the comparative number of 'clicks' a consumer has to make in order to: (i) reach the account deletion page; and (ii) activate the deletion process once they have reached this page.

Figure K.30 Comparative number of consumer 'clicks' required to delete social media account[60]

'Clicks' required to delete account	Social Media Platform					
	Facebook	**Instagram**	**Snapchat**	**Twitter**	**Pinterest**	**TikTok**
Minimum number of clicks required to reach account deletion webpage from platform's homepage	6	6 (account deletion must be carried out via Facebook)	6 (deletion webpage can only be accessed via Snapchat website not app)	3 (for account 'deactivation' rather than deletion)	7	5
Clicks required on account deletion page to delete account	1 (confirm account deletion button)	1 (nb account deletion must be carried out via Facebook)	1 (consumer's password must also be entered to confirm account deletion)	1 (for account 'deactivation' rather than deletion)	1 (final confirmation of account deletion is completed via button in confirmation email	2 (delete and confirm account deletion buttons)

Source: CMA analysis of social media platforms' account deletion processes

Facebook and Instagram

212. For Facebook and Instagram, upon receipt of a deletion request a consumer's account will be immediately deactivated and no longer visible to other consumers. The process of deleting the consumer's data will not begin until 30 days after this request, in order to provide consumers with a period to change their mind and cancel the deletion request. Following this 'cooling off' period, deletion of the consumer's account will be permanent and irreversible.

213. If a user opts to delete their account, Facebook said that normally it takes up to 90 days for the deletion process to complete, but that the consumer's information would not be visible to other Facebook users during this time. Data may also be held in backup storage for up to 90 days for disaster recovery purposes. Upon completion of the deletion process, consumers' personal data is deleted or de-identified from Facebook's servers and is not accessible to Facebook, except for: the user ID of the deleted account; time and date of account deletion; private messages sent by the consumer to other consumers (in the recipient consumer's inbox); correspondence between the

[60] The methodology we used to assess this was based on what we believed would be a typical consumer's journey to reach the account deletion page (and to subsequently delete their account) from a starting point of the platform's homepage. We understand that it may be possible for consumers to access the platforms' account deletion screens more quickly via alternative means, if they have sufficient knowledge of how to do so. For example, consumers may be able to access the platforms' account deletion screens by entering appropriate terms into a search engine and then clicking on a relevant link provided by the search engine if provided.

consumer and Facebook; information on payments made by the consumer on Facebook (as long as required by law); and other data subject to a legal hold to comply with an applicable law or regulation.

214. Facebook said that 'Log Data', highly technical data recorded by reference to time, is 'stored until no longer necessary' as determined on a case-by-case basis. Any such data stored for longer than 90 days is subject to a pseudonymisation process.

215. Social plugin impression logs are retained for up to 90 days, but not linked to an account or identifiable information, except when an active security investigation in ongoing. Pixel logs are retained for up to two years which Facebook said was necessary to enable measuring and reporting of advertising effectiveness across annual seasons.

Snapchat

216. Snapchat allows consumers to delete their accounts through the Snapchat Support website rather than directly through its app. This may not be evident to consumers, given that all their activity on the platform occurs within the Snapchat app on their mobile device. If a consumer searches for Snapchat Support via Google, a direct link to the 'Delete My Account' option will appear under the Snapchat Support search result.

217. Firstly, Snapchat explains its deletion process to consumers before directing them to the account portal. On the account portal, consumers are asked for their Snapchat credentials and are then required to complete a CAPTCHA. The consumer will be asked for their username and password again, before the account is deactivated and ultimately deleted 30 days later.

218. In the Snapchat Support centre, Snap explains that deletion after the 30-day period where a consumer's account is deactivated will be permanent, meaning a consumer's account, account settings, friends, Snaps, Chats, Story, device data, and location data in Snapchat's main consumer database will all be deleted.[61] Snap states that it may retain some personal data for certain legal, security, and business needs. For example, it will retain information about purchases a consumer has made through Snapchat. Snap also retains the date when a consumer accepted its Terms of Service and Privacy Policy.

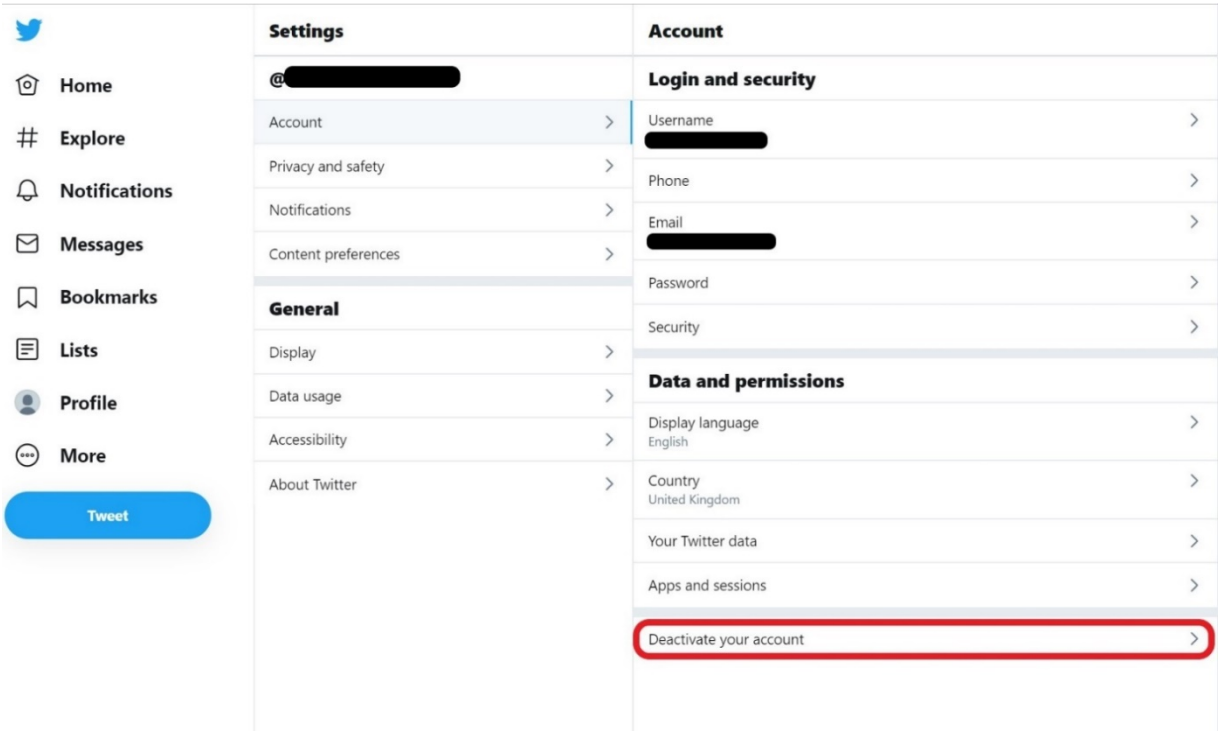
[61] Snapchat Support – 'Delete My Account'.

Twitter

219. Twitter allows consumers to 'deactivate' their Twitter account via a link in its settings page.

220. In its privacy policy, Twitter states that, when deactivated, a consumer's Twitter account, including their display name, username, and public profile, will no longer be viewable on Twitter.com or its iOS and Android apps. For up to 30 days after deactivation a consumer's account may be restored if it was accidentally or wrongfully deactivated. Search engines and other third parties may still retain copies of a consumer's public information, like their profile information and public Tweets, even after a consumer has deleted the information from Twitter's services or deactivated their account.

Figure K.31: Location of link to deactivate a consumer's account on Twitter



Source: Screenshot of Twitter's settings page

221. In its privacy policy Twitter states that it keeps consumers' 'Log Data', which is information it receives when consumers view content on or otherwise interact with Twitter's services, for a maximum of 18 months.

Pinterest

222. Pinterest allows consumers to either deactivate or close their Pinterest accounts. If a consumer deactivates their account, their profile and boards will no longer be visible on Pinterest. The deactivation will be reversed if a consumer subsequently logs in to their account.

223. If a consumer chooses to close their Pinterest account, this will be permanent and Pinterest will delete their data, including their Pins and boards.

224. When consumers close their account, whilst their public profile is deactivated immediately, it takes 14 days for their account to be permanently closed. If consumers change their mind before the end of these 14 days, they will be able to reactivate their accounts by logging-in and requesting a reactivation link from Pinterest.

TikTok

225. TikTok allows those consumers who have created an account, to delete this. The 'delete account' page is found within TikTok's 'Manage my account' menu in its app. Once a consumer has navigated to this page, TikTok explains some of the consequences, should a consumer decide to proceed with deleting their account. It also states that after a consumer makes the deletion request, their account will be 'deactivated' for 30 days, during which time it will not be publicly visible.

226. In its terms of service TikTok states that consumers may contact TikTok via email in order to receive further assistance and guidance on the account deletion process. TikTok states that once the deletion process is complete, consumers will not be able to reactivate their account or retrieve any content or information they have added. Information not stored in the consumer's account, such as chat they have sent, may still be visible to others.

227. In its privacy policy TikTok states that after a consumer has terminated their use of its platform, it will store their information in an aggregated and anonymised format.

Can consumers take their data with them?

Facebook and Instagram

228. Facebook provides consumers with tools to access and download their Facebook and Instagram information. Facebook's Access Your Information Tool (AYI Tool) allows consumers to see what categories of personal data Facebook holds about them and view such information directly. Facebook defines these categories as:

- 'Your information', which is information the consumer has uploaded and shared, such as profile, posts and comments; and

- ‘Information about you’, which is information associated with the consumer, for example, devices the consumer has used.

229. Facebook’s AYI Tool also notifies consumers that there is a separate tool for downloading this information. Facebook’s Download Your Information Tool (DYI Tool) allows consumers to download a copy of their information from Facebook in a machine-readable format,[62] which can be shared with third parties. Facebook is also participating in the Data Transfer Project.[63]

230. Instagram’s ‘View Account Data’ tool allows consumers to view their former account info (eg email addresses), connections and activity (eg logins). It also allows consumers to see what interests Instagram has identified as possibly relevant to them. As a Facebook product, Instagram also allows consumers to download their data, via a ‘Data Download’ option in the Privacy and Security area of their profile.

Snapchat

231. Snapchat allows consumers to obtain a copy of their information that isn’t available in its apps in a portable format, via its ‘Download My Data’ tool.[64] Snapchat’s privacy policy states that consumers are then able to move this data or store it ‘wherever they want’.[65]

232. Snapchat requires consumers to verify their identity or provide additional information before they can access or update their personal information. Snapchat states that it may also reject consumers’ requests to access or update their personal information for several reasons, including, for example, if the request risks the privacy of other consumers or is unlawful.

Twitter

233. Twitter told us that it provides consumers with a number of ways to access or retrieve information they have shared on Twitter. In Twitter’s privacy policy, it states that consumers can download ‘certain account information’, including their Tweets.

---

[62] Eg JSON or HTML.
[63] This is a cross-platform, open-source project seeking to allow consumers to transfer their data into and out of online multiple online services.
[64] Snap’s ‘Download My Data’ tool.
[65] Snap’s Privacy Center – ‘Control Over Your Information’.

234. In the ‘Your Twitter data’ section of the Twitter website, consumers can view information that Twitter has collected from them including on their apps, devices, account activity and interests and ad data.

Pinterest

235. Pinterest allows consumers to request access to the information it collects and holds about them, via its Help Centre. In its privacy policy, Pinterest states that it will ‘usually share this with [consumers] within 30 days of [a consumer] asking for it.’[66]

236. Pinterest states that it will also allow consumers to have their information sent to another organisation, where Pinterest holds this, with the consumer’s consent or for the performance of a contract with the consumer, and: ‘where it's technically feasible for [Pinterest] to do so.’

237. Consumers can also request more details about the information Pinterest collects and how and why it is used and shared by Pinterest.

TikTok

238. Within the ‘Personalization and data’ section of TikTok’s settings, TikTok allows consumers to request a copy of their data. TikTok states that it takes up to 30 days to process such requests. The information which can be downloaded relates to the consumer’s profile, their activity and app settings.

Browser- and operating system-level controls

239. In this section we set out and explain some of the data controls available to consumers within their internet browsers and operating systems (OS). A more detailed and technical discussion of the controls available to consumers at the browser and OS level, with a particular focus on the role of tracking in personalised advertising, in contained in Appendix G.

Browsers

240. In addition to platform level controls, consumers can also adapt the privacy settings in their browser to control the collection and use of their data for the purposes of personalised advertising. We set out the controls available to consumers on the most commonly-used browsers below.

---

[66] Pinterest’s Privacy Policy.

Safari

241. Safari is a web browser developed by Apple and used as the default browser on iOS devices. Consequently, it is widely used on mobile devices but is less prevalent as a desktop browser.

242. Safari offers consumers a range of features which consumers can use to control the collection and use of their data for the purposes of personalised advertising. Some of these focus on blocking or deleting cookies in order to prevent platforms, websites, apps and third parties from collecting browsing data for the purposes of personalised advertising. Others allow consumers to control the collection of data by their browser.

- Prevent cross-site tracking – Companies are able to collect consumers' browsing data across multiple websites, whether by cookies placed on the consumers' browsers when they access content or by other means, eg social media buttons on websites. That browsing data can be used to provide targeted advertising or create consumer profiles and may be shared with third parties, such as data brokers and advertising networks. When a consumer activates 'Prevent cross-site tracking', Safari will periodically delete tracking data from the consumer's device, preventing advertisers from collecting browsing data to target their advertising.[67]

- Block cookies – By default, Safari accepts cookies and website data from sites that a consumer visits. When a consumer opts to 'Block all cookies' in Safari, all existing cookies stored on the device are deleted and future cookies blocked.[68] This prevents advertisers from collecting browsing data for the purposes of serving consumers personalised advertising. However, blocking (or disabling) cookies will affect the functionality of many websites (eg consumers may be prevented from accessing content without cookies enabled).

- Clearing stored cookies – Consumers can also opt to delete stored cookies from a device by deleting website data, such as cookies and login details, or by clearing their Safari browsing history, which includes browsing data such as cookies.

[67] This feature replaced another control ('Ask Websites Not To Track Me') by which consumers instructed Safari to send requests to websites, asking them not to track usage; however, the requests were often ignored and consumers' activity tracked regardless. The feature was therefore retired.
[68] Activating this option also automatically enables the 'Prevent cross-site tracking' feature, as blocking cookies also prevents tracking across websites.

- Private browsing – When a consumer activates private browsing, Safari doesn't remember the websites visited by the consumer and will also ask sites and third parties, including advertisers, not to track the consumer.

- Location data – consumers can decide whether or not to allow Safari to give their location data to websites or apps while these are in use, via pop-up permission requests when they first access the site, or via the privacy settings in Safari. Consumers who deny permission will not be served personalised advertising based on location, as advertisers will be unable to collect that data, but may find that the website or app will not function properly without access. A further privacy option is for consumers to deny websites and apps access to the camera and microphone on their device, again preventing companies from accessing that data for in order to target advertising to the consumer.

- Change default search engine – Consumers can decide which search engine to set as their default in Safari. The available options include DuckDuckGo, which does not store consumer information or serve personalised ads based on search history.

Chrome

243. Chrome is a web browser developed by Google. It is usually installed as the default browser on Android devices[69] and is the most widely-used web browser, accounting for more than half of all web traffic.[70] The privacy settings offered by Google are set out in the 'Platforms' section, above.

Mozilla Firefox

244. Firefox has built a strong reputation as a privacy-focused browser; it offers a range of highly customisable features which allow consumers to control the collection and use of their data. These include:

- Change default search engine – Consumers can choose to change their default option (Google) to another search engine.

- Content Blocking – Consumers can opt to block a range of content that tracks the sites that they visit to facilitate profiling. Consumers can choose between 'Standard' content blocking (which allows some trackers so that websites function properly but blocks third party cookies and other forms of tracker such as cryptominers and fingerprinters), Strict (which brings up

[69] Consumers can opt to use a different browser eg by installing the relevant app.
[70] According to Statista, Chrome's had the largest global internet browser market share of 68.11% in March 2020.

a warning that it may cause some websites not to function), and Custom modes. There is the option to disable content blocking for specific trusted sites.

- Do Not Track – Firefox also has an option to request that websites do not track consumers, but many websites simply ignore these requests.

- Configuration settings – Aside from the general settings above, consumers can also make a number of different modifications in Firefox by changing their configuration settings. For example, consumers can opt to make Firefox more resistant to browser fingerprinting, or utilise enhanced controls over the blocking and deletion of cookies and the ability to disable geo-location tracking. However, making changes to the configuration settings requires significant technical knowledge on the part of the consumer, and accessing these settings brings up a warning that doing so may void the warranty for the application and that consumers should only proceed if they know what they are doing.

245. Firefox also offers a variety of privacy and security add-ons to the browser; however, it is unlikely that the average consumer would have the technical understanding or awareness to engage with these options.

Microsoft Edge

246. Microsoft Edge is a web browser developed by Microsoft and has overtaken the market share of Microsoft's earlier browser, Internet Explorer.[71] Microsoft now recommends that consumers use Edge as their default browser, rather than Internet Explorer.[72] Edge includes integration with Microsoft's 'Cortana' virtual assistant and offers consumers a range of privacy features, including over the collection of data by Cortana.

- Do Not Track – Consumers can opt to have Edge send 'Do Not Track' requests to websites; however, websites may still track browsing activity even when a Do Not Track request is sent.

- Private browsing – Microsoft Edge offers a private browsing mode in which browsing information like cookies, history, and temporary files will not be saved on the consumer's device after the browsing session has ended.

- Clear browsing data – Edge allows consumers to clear browsing information stored on their device; consumers can choose which types of

[71] According to Statista, Edge's global internet browser market share was 4.56% compared with 3.77% for Internet Explorer in March 2020.
[72] Microsoft, 'Lifecycle FAQ – Internet Explorer and Edge', June 2020.

data to clear (eg cookies, saved passwords) and can also instruct Edge to clear that type of data whenever a browsing session ends. In addition, consumers can clear the browsing data sent to Cortana; they can also opt to stop Microsoft Edge from collecting their browsing history for the purposes of personalising their Cortana virtual assistant.

- Block cookies – Consumers can stop Edge from collecting or storing their data by managing their cookie settings. They can either opt to block all cookies (which prevents any website saving cookies to their device) or to block only third-party cookies (which allows cookies from websites visited, but blocks cookies from external web services, such as from ads embedded on the sites visited).

AdChoices

247. Browsers can also help facilitate consumers' choices via the industry's self-regulation programme.[73] Via the European Interactive Digital Advertising Alliance (DAA) website,[74] consumers can see which of the DAA's participating partner businesses is currently using targeted adverts on their device. Consumers are able to record their choice to opt out of targeted advertising on a business-by-business basis: this results in 'opt-out cookies' being stored on their device browser.[75]

Operating systems

248. The majority of consumer devices use either the Apple iOS or the Android operating system. Both of these systems provide consumers with options to control the collection of their data and its use for the purposes of targeted advertising. Consumers adopting these controls will generally continue to see a similar number of adverts as previously, but these will no longer be targeted to their interests on the basis of data collected from them.

249. The privacy controls available at operating system-level form part of a suite of controls which consumers can adopt to limit the collection and use of their data for personalised advertising purposes.

[73] See Appendix A for further information on the self-regulation programme.
[74] See YourOnlineChoices website.
[75] As this 'opt-out' mechanism relies on the use of cookies, clearing cookies will nullify the consumer's choices.

Apple

250. Apple devices such as iPhones and iPads use the iOS system, which offers consumers the following controls.

- Limit ad tracking – this feature allows consumers to opt-out of having an Advertising Identifier, or IDFA,[76] associated with their device. When a consumer turns on 'Limit ad tracking', their Advertising Identifier appears blank when tracked. As a result, advertisers are unable to serve the consumer with targeted advertising, although the consumer might still see ads related to the content in an application or based on other non-personal information.[77]

- Reset Advertising Identifier – this option enables consumers to disassociate the data linked with their existing Advertising Identifier (which is used to serve targeted advertising to the consumer) and assigns a new, random Advertising Identifier in its place. However, a new data profile will begin to build which is associated with the newly Advertising Identifier and will then be used to target ads.

- Limit apps' access to information – Consumers can control which apps have access to information stored on their device, such as their contacts list (which a messaging app might use to find any friends already using the same app) or their photo library (from which a consumer might want to upload pictures to a social-networking app). Consumers can modify their privacy settings by selecting a type of data from the list to see which apps have asked for permission to use that data and adding or removing permission from any app that has asked for access to data.

- Opt out of location-based advertising – iOS gives consumers the option to turn off location-based advertising, preventing advertisers from utilising a device's location, as determined by iOS's Location Services. Ads seen in apps will no longer be customized on the basis of geographical location.

---

[76] An Advertising Identifier, or IDFA, is an anonymised, non-permanent device identifier. Unlike its predecessor, the Universal Device Identifier (UDID) which was previously used for advertising and consumer tracking in iOS, the IDFA does not contain any device information and cannot be linked to a specific iOS device (or, by extension, to its user).

[77] According to *28 days later: What happened to Limit Ad Tracking?*, a blog by Adjust (a global company specialising in mobile marketing, mobile measurement and fraud prevention), 16.52% of consumers in the UK had adopted the 'Limit Ad Tracking' feature within a month of its launch in September 2016, compared with a global average figure of around 18%.

- Opt out of collection of data relating to location[78] – Location Services allows apps and websites (including Maps, Camera, Weather, and other apps) to use information from various sources to determine the approximate location of a device. Some apps use location data only while the app is in use, while others access location data even when the app is not in use.[79] Consumers can individually control which apps and system services have access to Location Services data.[80] iOS devices also keep a list of consumers' frequent locations, ie places that a consumer visits regularly and how long the consumer stays there; consumers can opt to turn this feature off.

Android

251. Android devices offer consumers a similar range of options by which to control the collection of their data and exposure to targeted advertising.

- Opt out of personalised advertising – On Android devices, consumers can opt out of receiving personalised advertising by activating the 'Opt out of Ads Personalisation' feature. When activated, the consumer's Advertising ID will no longer be used by apps to build advertising profiles based on usage and apps will be prevented from displaying personalised advertising (although random ads will be shown instead).

- Reset your advertising ID – As with iOS, Android devices' advertising ID can be reset to a random number. Using this feature will remove the data that was already collected, based on app and internet usage; new data will then be collected using the new advertising ID but, depending on the frequency with which a consumer resets their ID, the amount of data linked to that consumer can be minimised.

- Limit apps' access to information – As with iOS, consumers can control which apps have access to information stored on their device and modify their privacy settings by selecting a type of data from the list to see which apps have asked for permission to use that data and by adding or removing permission from any app that has asked for access to data. Some apps, such as Google Maps, use location data from Android devices to determine the approximate location of a device. Consumers can

---

[78] Can also reset all location settings to the factory default, with the result that apps will stop using location data until granted permission.
[79] When Location Services is switched on, a GPS-enabled iOS device will also periodically send GPS locations and travel speed information to Apple to be used for building up Apple's crowd-sourced road-traffic database. The crowd-sourced location data gathered by Apple is anonymous and encrypted.
[80] Apple states that 'For safety purposes, your iPhone's location information may be used when you place an emergency call to aid response efforts regardless of whether you enable Location Services.'

individually control which apps and system services have access to location data in the same way as they can control access to any other data. Consumers can also delete stored location data.

- Turn off location data – Consumers can opt to switch off location data on their device, so preventing advertisers from serving targeted advertising based on location (or, at least, the location of their device).

- Clear data collected from Google apps – Chrome, Gmail, Google Calendar, and other apps created by Google are often included as pre-installed apps on Android devices. Pre-installed apps are usually non-removable, but consumers can still remove any personal information they may have accumulated.