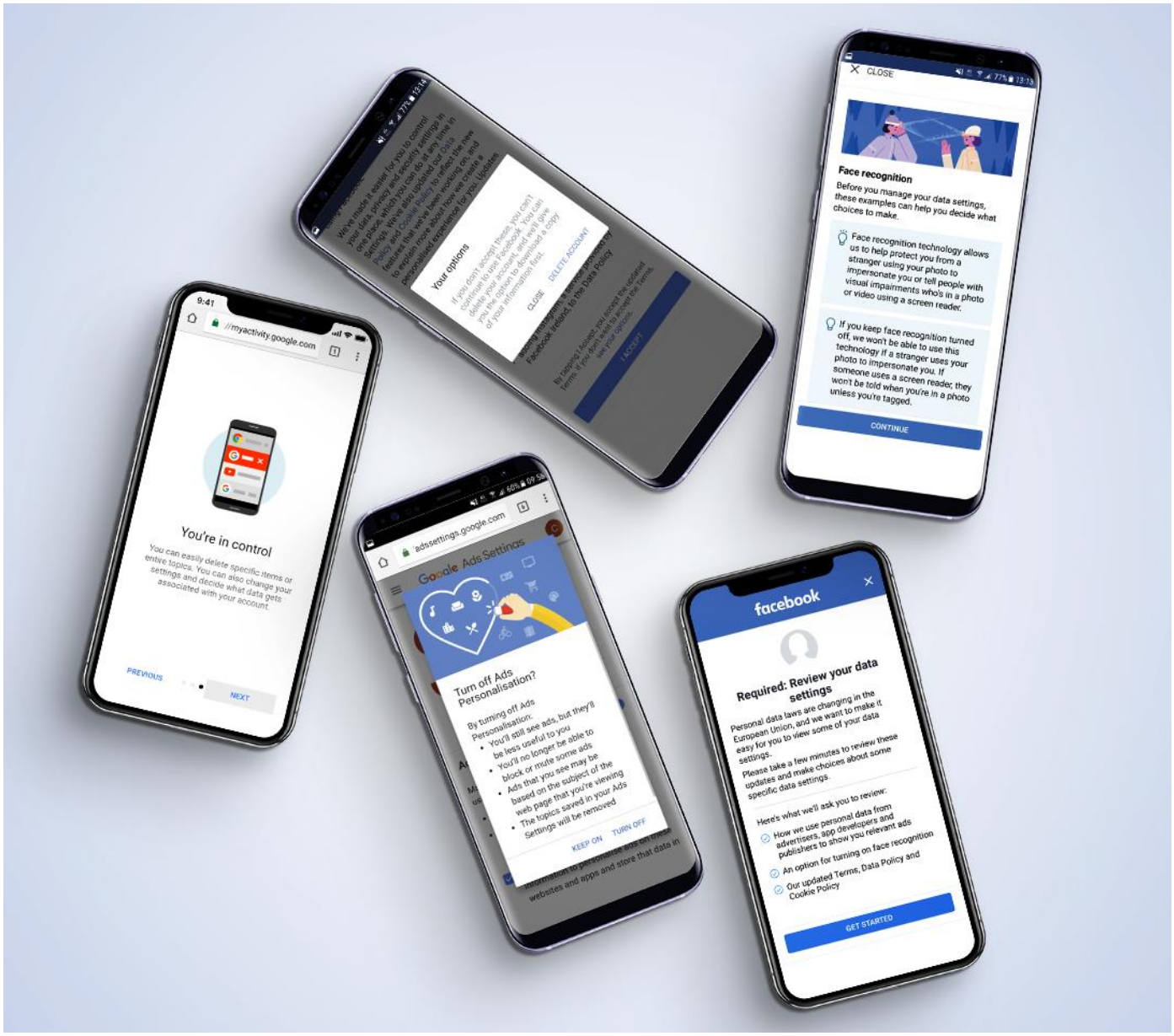


DECEIVED BY DESIGN

How tech companies use dark patterns to discourage us from exercising our rights to privacy

27.06.2018

FORBRUKERRÅDET

Table of contents

1 Summary

In this report, we analyze a sample of settings in Facebook, Google and Windows 10, and show how default settings and dark patterns, techniques and features of interface design meant to manipulate users, are used to nudge users towards privacy intrusive options. The findings include privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users.

Facebook and Google have privacy intrusive defaults, where users who want the privacy friendly option have to go through a significantly longer process. They even obscure some of these settings so that the user cannot know that the more privacy intrusive option was preselected.

The popups from Facebook, Google and Windows 10 have design, symbols and wording that nudge users away from the privacy friendly choices. Choices are worded to compel users to make certain choices, while key information is omitted or downplayed. None of them lets the user freely postpone decisions. Also, Facebook and Google threaten users with loss of functionality or deletion of the user account if the user does not choose the privacy intrusive option.

The GDPR settings from Facebook, Google and Windows 10 provide users with granular choices regarding the collection and use of personal data. At the same time, we find that the service providers employ numerous tactics in order to nudge or push consumers toward sharing as much data as possible.

	Facebook	Google	Windows	Chapter
No privacy intrusive default settings in popups	✗	✗	✓	4.1
Equal ease (number of clicks) for privacy friendly options in popups	✗	✗	✓	4.2
Design (colours and symbols) does not lead toward privacy intrusive option in popups	✗	✗	✗	4.2
Language does not lead toward privacy intrusive option in popups	✗	✗	✗	4.3
Privacy friendly options in popups come without “warnings”	✗	✗	✓	4.4
Users can clearly postpone the decision while accessing the service in the meantime	✗	✗	✗	4.5

To complement the analysis, we use two examples of how users are given an illusion of control through privacy settings. Firstly, Facebook gives the user an impression of control over use of third party data to show ads, while it turns out that the control is much more limited than it initially appears. Secondly, Google’s privacy dashboard promises to let the user easily delete user data, but the dashboard turns out to be difficult to navigate, more resembling a maze than a tool for user control.

The findings in this report are based on several user tests taking place in April and May 2018. The results represent the observations based on these tests, and may therefore vary somewhat between users of the services and geographic regions.

The combination of privacy intrusive defaults and the use of dark patterns, nudge users of Facebook and Google, and to a lesser degree Windows 10, toward the least privacy friendly options to a degree that we consider unethical. We question whether this is in accordance with the principles of data protection by default and data protection by design, and if consent given under these circumstances can be said to be explicit, informed and freely given.

2 Introduction

The Norwegian Consumer Council is an interest organisation for consumers funded by the Norwegian government. Part of our work is to promote consumer rights such as privacy, security and balanced contracts in digital products and services. We have published reports on how mobile apps[1] fail to respect consumer rights, and how connected devices such as toys lack basic security and privacy-protective measures.[2]

This report is part of our work on consumer privacy and the right to make informed choices.

In this report, we look at user settings updates in three digital services that relate to the new General Data Protection Regulation (GDPR). In May 2018, European service providers confronted consumers with a wide array of GDPR updates. Amongst these services, users of Facebook, Google's services, and Windows 10 had to click through and approve update messages as part of the companies' attempt to comply with the GDPR. These popups contained references to new user terms, and presented a number of user settings related to the ways that the companies may collect, process, and use personal data.

Facebook, Google, and Microsoft were chosen as examples, as they are some of the world's largest digital service-providers. Although the examples used in this report are probably not unique to these three service-providers, they serve to illustrate the problematic aspects that consumers face when using digital services.

As we argue below, providers of digital services use a vast array of user design techniques in order to nudge users toward clicking and choosing certain options. This is not in itself a problem, but the use of exploitative design choices, or "dark patterns", is arguably an unethical attempt to push consumers toward choices that benefit the service provider. We find that the use of these

[1] "Threats to Consumers in Mobile Apps" **https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/**

[2] "Internet of Things" **https://www.forbrukerradet.no/internet-of-things/**

techniques could in some cases be deceptive and manipulative and we find it relevant to raise questions whether this is in accordance with important data protection principles in the GDPR, such as data protection by design and data protection by default.

Creating seamless and enjoyable user experiences is central to user-centered design, but this does not excuse the use of exploitative nudging. Excessive nudging toward privacy intrusive options, use of dark patterns and privacy intrusive default settings, should in our view not be regarded as freely given or explicit consent.

Instead, digital service providers should trust their users to make independent choices about what data they wish to share, and how their personal data is used. After all, trust is the basis of any good customer relationship, and deceit and manipulation leads to the erosion of trust.

When digital services employ dark patterns to nudge users toward sharing more personal data, the financial incentive has taken precedence over respecting users' right to choose. The practice of misleading consumers into making certain choices, which may put their privacy at risk, is unethical and exploitative.

This report was written with funding from the Norwegian Research Council and the Norwegian ministry for Children and Equality and with input from academics from the ALerT research project,[3] BEUC, and Privacy International.

3 Background

In the digital world, the main revenue of free digital services is often the accumulation, use and analysis of user data, in many cases personal data.[4] These services rely on users sharing as much data as possible about themselves, both to personalize services, and then to sell individualized/targeted advertising. Under this business model, users are often considered to be paying for the service with their personal data, although this trade-off is subject to some controversy.

While many digital services monetize data by serving advertising, highly personal information such as political views, sexual preferences, and health data can also be used for other purposes. There are examples of personal data

[3] "ALerT - Awareness Learning Tools for Data Sharing Everywhere" https://www.nr.no/en/projects/alert-awareness-learning-tools-data-sharing-everywhere

[4] "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" GDPR Art.4 (1)

being used to exclude or discriminate based on race or ethnicity,[5] health information such as HIV status being shared with third parties,[6] and detailed personal profiles being used to manipulate voters in attempts to swing elections.[7]

Because many digital service providers make their money from the accumulation of data, they have a strong incentive to make users share as much information as possible. On the other hand, users may not have knowledge about how their personal data is used, and what consequences this data collection could have over time. If a service-provider wants to collect as much personal data as possible, and the user cannot see the consequences of this data collection, there is an information asymmetry, in which the service-provider holds considerable power over the user.

This information asymmetry puts the consumer at a disadvantage, because they are poised to share personal data without having any viable way to know how this personal data could be used to their detriment. The use of manipulative user design further widens the information gap.[8]

3.1 From nudging to exploitation through dark patterns

In user-centered design,[9] the designer will create an interface based on what users are likely to look for, trying to predict how to best accommodate their wants and needs.[10]

The concept of nudging comes from the fields of behavioural economy and psychology, and describes how users can be lead toward making certain choices by appealing to psychological biases. Rather than making decisions based on rationality, individuals have a tendency to be influenced by a variety of cognitive biases, often without being aware of it.[11] For example, individuals have a tendency to choose smaller short-term rewards, rather than larger long-term

[5] https://www.propublica.org/article/what-algorithmic-injustice-looks-like-in-real-life

[6] https://www.forbrukerradet.no/side/filing-complaint-against-grindrs-sharing-users-hiv-status-and-sexual-preferences/

[7] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[8] Similar practices in the financial services industry, where consumers are nudged toward choosing expensive currency conversion options in ATMs through graphic design choices, have also been criticized by consumer groups. http://www.beuc.eu/publications/beuc-x-2017-118_dynamic_currency_conversion_position_paper.pdf page 8.

[9] Throughout this report, we use "user-centered design" and "design" interchangeably. For simplicity's sake, we avoid similar terms such as user experience design, (UX design) and experience design.

[10] https://www.usability.gov/what-and-why/user-centered-design.html

[11] "Privacy's Blueprint: The Battle to Control the Design of New Technologies", page 36 https://books.google.no/books?id=YERMDwAAQBAJ&lpg=PA35&dq=nudging%20away%20from%20privacy&hl=no&pg=PA36#v=onepage&q=nudging%20away%20from%20privacy&f=false

gains (hyberbolic discounting), and prefer choices and information that confirm our pre-existing beliefs (confirmation bias).

Interface designers who are aware of these biases can use this knowledge to effectively nudge users into making particular choices. For example, making the healthy alternatives in a restaurant menu more prominent can nudge consumers toward making healthier eating choices. In digital services, design of user interfaces is in many ways even more important than the words used.

The psychology behind nudging can also be used exploitatively, to direct the user to actions that benefit the service provider, but which may not be in the user's interests. This can be done in various ways, such as by obscuring the full price of a product, using confusing language, or by switching the placement of certain functions contrary to user expectations. Deliberately misleading users through exploitative nudging is also called "dark patterns".[12]

Dark patterns can be described as "…features of interface design crafted to trick users into doing things that they might not want to do, but which benefit the business in question.", or in short, nudges that may be against the user's own interest.[13] This encompasses aspects of design such as the placement and colour of interfaces, how text is worded, and more direct interventions such as putting pressure on users by stating that the product or service they are looking at is about to be sold out.

Dark patterns are considered ethically problematic, because they mislead users into making choices that are not in their interest, and deprive them of their agency.[14] This is particularly problematic given the power imbalances and information asymmetries that already exist between many service providers and their users. Additionally, if users trust the service provider, many will assume that the service provider knows what is best for the user. This, or a suspicion that tampering with default settings might remove important functionality, may affect the tendency to leave default settings alone.[15]

For example, the information asymmetry in many digital services becomes particularly large because most users cannot accurately ascertain the risks of exposing their privacy. If a user is asked to trade their personal data for a short-term financial benefit, such as a discount, the actual cost of the trade-off is difficult to grasp. In this case, the short-term gain (discount) is tangible and immediate, while the potential loss (privacy) long term.

---

[12] The term "dark patterns" was coined by user experience researcher Harry Brignull **https://darkpatterns.org/**

[13] "How Dark Patterns Trick You Online" **https://www.youtube.com/watch?v=kxkrdLI6e6M**

[14] "Dark Patterns and the Ethics of Design" **https://medium.com/adventures-in-ux-design/dark-patterns-and-the-ethics-of-design-31853436176b**

[15] "Do users change their settings?" **https://www.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/**

3.2 European data protection legislation

This report focuses on how design can be used to manipulate consumers to share personal information about themselves, and illustrates this with examples. The processing of personal data is regulated, and hence a brief background outlining of the European data protection legislative scheme follows below.

The right to privacy is enshrined in the European Convention on Human Rights,[16] and protected through European data protection legislation. This means that privacy and data protection are fundamental, inalienable, rights for individuals.[17] The essence of data protection is that organisations have an obligation to process and store the personal data of individuals responsibly, and amongst other things to limit the amount of personal data they collect and use.

The European General Data Protection Regulation (GDPR) came into effect in all EU states on May 25th 2018, and will also enter into effect in EEA countries (including Norway) in 2018. The regulation builds upon existing European data protection legislation, but strengthens existing consumer rights while adding a number of new rights and obligations. The regulation applies for all service providers who provide services for individuals who are in EU and EEA territory.[18]

Processing personal data requires legal grounds and fulfilment of the data protection principles. One of the principles is the principle of purpose limitation, which entails that personal data should be collected for a clear purpose, and should not be used for other incompatible purposes, and must be deleted when it is no longer necessary to process personal data for these purposes. Another important principle is the principle of data minimisation, which states that organisations should collect the minimum amount of personal data necessary to perform a task. Furthermore, the principle of transparency means that individuals should receive an explanation, in a clear and understandable manner, of what personal data is collected, and for what purposes.[19]

The GDPR also requires that services should be developed according to the principles of data protection by design and data protection by default.[20] Data protection by design means that services should be designed to ensure that data minimisation, purpose limitation, and transparency are safeguarded.[21] In

[16] European Convention on Human Rights, Article 8
[17] For the purpose of this report, «individual», «consumer», «user», and «data subject» are used interchangeably.
[18] The Regulation "applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law." (GDPR Article 3).
[19] GDPR Article 5
[20] GDPR Article 25
[21] The principles of data protection by design and default are used to designate the obligations placed on organisations under the GDPR. Privacy by design and default are broader concepts, encompassing an ethical dimension consistent with the right to privacy enshrined in the EU Charter of Fundamental Rights. See EDPS "Preliminary

addition to limiting the data collected, appropriate and effective measures to ensure the integrity and confidentiality of the data should also be implemented.

Data protection by default requires that consumers should receive a high level of data protection, even if they do not actively opt out of the collection and processing of personal data.[22] By default, services should only collect personal data that is necessary for the provision of each specific purpose of the service, trying to meet the expectation of the data subject. In practice, this also entails that boxes should be pre-checked for the most privacy friendly option, or the option that allows the collection of the least amount of personal data, and that it should be made clear to the user what personal data is being collected, and what it may be used for.[23]

Personal data must be processed lawfully.[24] For example, service-providers can process personal data in order to fulfil a contract with the user or where they can demonstrate that the processing is necessary for the purpose of their legitimate interest and provided it does not prejudice the rights and interests of individuals.[25] If personal data is processed for other purposes, consent from the data subject is necessary. Many digital services rely on consent from the user for processing personal data.

According to the GDPR, *Article 4(11)*;

> *«'consent' of the data subject means any **freely given**, **specific**, **informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her» (emphasis added)*

Previously, many services would ask for a blanket consent for most types of personal data processing. The GDPR requires that different uses of personal data require separate consent from the consumer. This can take the form of more granular types of consent, where users have choices to limit different forms of data collection and use. As services prepared for the implementation of the GDPR, in April and May 2018 consumers were faced with numerous new consent forms and privacy settings that they had to review and click through.

---

opinion on privacy by design", page 1
https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[22] "EDPS calls for workable technology which serves the interests of society"
https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-calls-workable-technology-which-serves_en

[23] "Preliminary opinion on privacy by design", page 7
https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[24] GDPR Article 6

[25] The reliance on legitimate interest, particularly for advertising and profiling purposes, is controversial. See "Why the GDPR 'legitimate interest' provision will not save you" https://pagefair.com/blog/2017/gdpr-legitimate-interest/

When dark patterns are employed, agency is taken away from users by nudging them toward making certain choices. In our opinion, this means that the idea of giving consumers better control of their personal data is circumvented. When service providers employ design tactics to nudge or manipulate consumers toward giving their consent to share personal data, in our opinion, this is at odds with the notion of consent being "freely given". The use of dark patterns to lead users toward less privacy-friendly options can also contravene the principle of data protection by default and design.

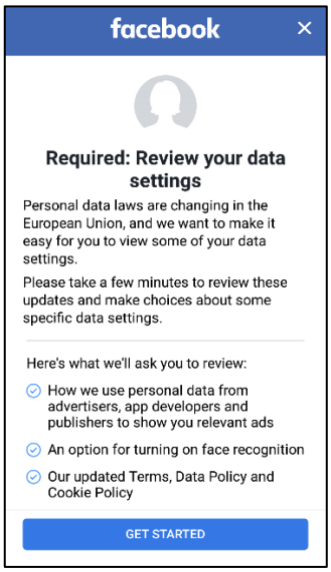
3.3 Methodology

The analysis was performed in May and June 2018.

Facebook, Google and Microsoft were chosen because of their dominant positions globally. All three presented users with new or revamped privacy settings in May 2018.

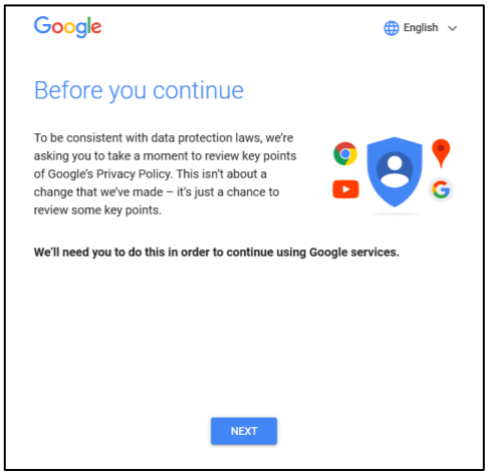
We have chosen to analyse the following updates and prompts:

- Facebook: "Review your data settings" popup received in service in May 2018. (henceforth referred to as "Facebook GDPR popup").



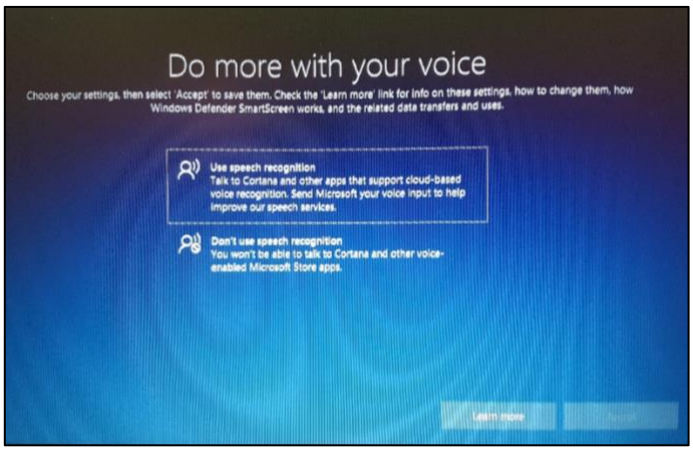
1 First page of the Facebook GDPR popup (mobile)

- Google: "A privacy reminder" popup from May 2018 (henceforth referred to as "Google GDPR popup"). This popup was presented to users who were or were not logged in on desktop versions of Google Services. Some of the settings that are presented in this popup leads users into Google's "privacy dashboard", a website with a vast array of settings. Changing settings in the dashboard required users to log in.



2 First page of the Google GDPR popup (desktop)

- Windows 10: Settings presented as part of a system update in May 2018 (henceforth referred to as "Windows Update").



3 First page of the Windows GDPR popup in the 10 update

It should be noted that Facebook and Google have somewhat different business models than Microsoft. Facebook and Google provide their services free of charge, and monetize user data. Microsoft's Windows 10 is not dependent on the same level of user data monetization. Therefore, we have chosen to have our main focus on Facebook and Google, but we still find it relevant to have examples from the Windows update.

We used dummy user accounts set up in April and May 2018, and checked our findings against our personal user accounts in the services. We only found minor differences between the updates on our personal accounts and the less used dummy accounts. The most significant difference was that the dummy account received one less option than the more used account on Facebook, regarding sensitive data. In this case we have gone forward with the dummy account results, since we assume this version might be more universal. The Windows update was only analysed on a desktop, while we looked at both desktop and mobile versions of the Facebook and Google popups. The

differences between mobile and desktop versions were mainly minor, but when they were significant, this is mentioned in the report.

The report includes an appendix including flowcharts showing the choice architecture of the popups that were analysed.

The scope of this report is limited to an analysis of user design and wording seen in the light of the principle of data protection by default in these updates. A full legal analysis, and an analysis of the terms of service or privacy policies of the services, are not within the scope of this report.

In addition to the tests in May 2018, a pilot analysis of privacy settings in the same services was performed in March/April 2018 to look at how the settings worked prior to the GDPR implementation. Screenshots were taken to document both processes.

In order to find examples of interface design that had been thoroughly and deliberately considered, we chose to look at the updates from three of the world's largest technology companies.

Since this is an analysis of digital settings and content that may be individualized or subject to change, we cannot say with certainty that all users of these services have been presented with identical settings and design patterns. Additionally, we limited the analysis to settings either in the actual GDPR updates, or websites that were linked to in the updates. Therefore, these findings should be considered samples based on the May 2018 updates.

Our opinion is that the findings are and will continue to be relevant even if the companies change their practices, because these examples illustrate the challenges consumers face in digital services at a given point in time. Because these examples are meant as an illustration of the outlined problematic practises in general, we have not found it necessary to present the results for the companies in question before publishing the report.

4 Dark patterns in prominent digital services

We have divided this chapter into categories of dark patterns, which have been taken from academic literature in the fields of behavioural psychology and user design.[26] The categories we have chosen to focus on are default settings, ease, framing, rewards and punishments, and forced action. These categories all overlap with each other to some degree, but together they form a comprehensive picture of dark patterns and exploitative nudges.

Note that none of these categories of nudging are inherently unethical, and can conceivably be used to achieve results that are in the users' best interests. However, we have chosen to focus on examples of how service providers use

[26] "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online" https://dl.acm.org/citation.cfm?id=3054926

dark patterns to nudge users, particularly when the consequences of data collection mainly benefits the service provider.

4.1 Default settings - Privacy by default?

Although many services that collect and process personal data provide users with privacy settings, the settings are presented in many different ways. Research has shown that most users will never look at, let alone change, the default settings.[27] In other words, default settings are often sticky, so they should be chosen carefully and responsibly. Following on the behavioural psychology of nudging, preselection of one option is a very efficient way of nudging users.[28] EU regulators have found this to be so efficient, that they have found it necessary to regulate defaults in the GDPR.

As mentioned in 3.2, the GDPR principle of data protection by default says that default settings should not allow for more data collection or use of personal data than is required to provide the service, and that the use of personal data for other purposes requires an explicit opt in consent.

Since most users do not change their settings, and many digital services are ad-driven, having users opt in to things such as personalized advertising could affect a company's bottom line. By contrast, when the default settings allow widespread collection and use of personal data, users are nudged toward giving away their data.

All three GDPR updates had settings relating to the use of personal data to serve tailored ads or experiences. From our point of view, we find it relevant to ask whether tailored ads are a part of the core functions of the services or not.[29] Personal data that is processed for purposes outside of the core functions of the service should not be mandatory or enabled by default. From an ethical point of view, we think that service providers should let users choose how personal data is used to serve tailored ads or experiences. Defaulting to the least privacy friendly option is therefore unethical in our opinion, regardless of what the service provider considers legitimate interest.

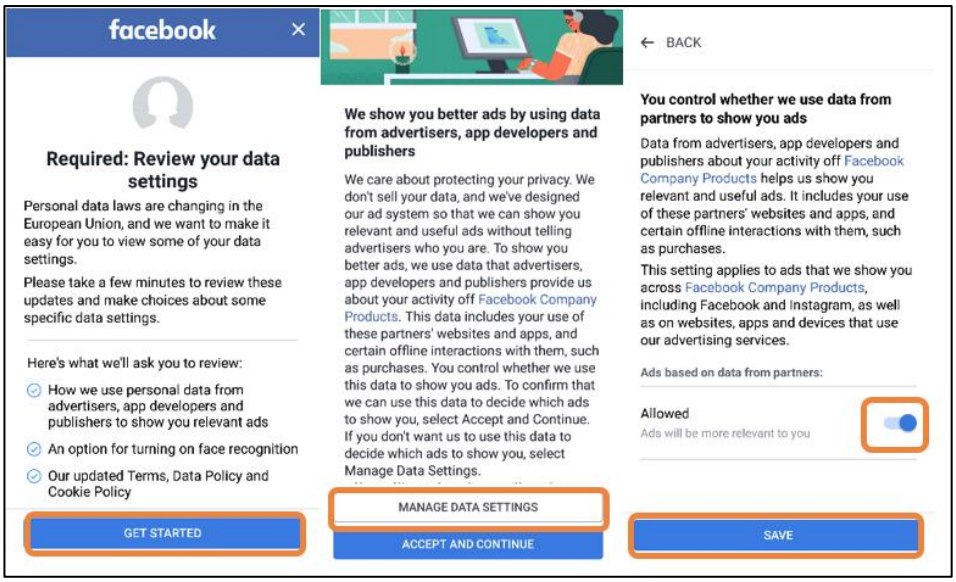
---

[27] "Do users change their settings?" https://www.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/

[28] As an example, studies have shown how organ donor policies that make citizens organ donors by default (meaning they must to opt out rather than opt in), sharply increased the number of organ donors. See "Do Defaults Save Lives?" http://www.dangoldstein.com/papers/DefaultsScience.pdf

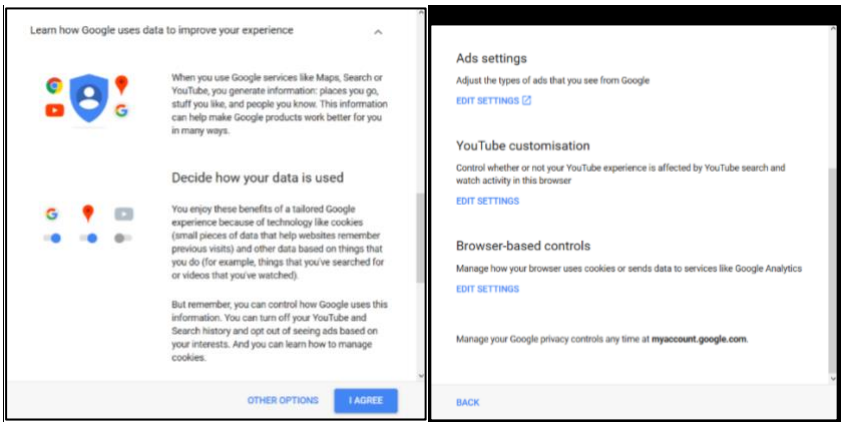
[29] Our comprehension/understanding is that the core function of Facebook is to provide users with a social network. Windows 10 is an operating system. Similarly, the core function of Google Search is being a search engine, Gmail is a mail service, Google Maps is a map/navigation service, etc. Targeted advertising is not a direct part of the functionality for the users. Thus, from this point of view it is relevant to ask whether they should rely on separate and explicit opt in consent for the collection and use of personal data for targeted advertising.

As the screenshots below illustrate, the Facebook GDPR popup requires users to go into “Manage data settings” to turn off ads based on data from third parties. If the user simply clicks “Accept and continue”, the setting is automatically turned on. This is not privacy by default.

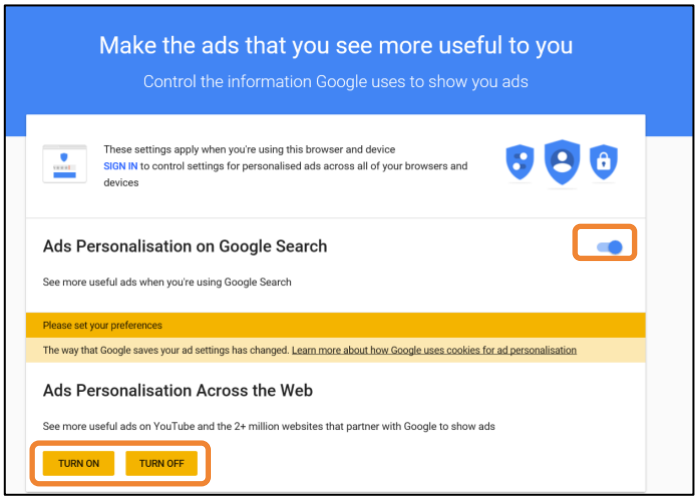


4 Facebook data settings (mobile)

Similarly, Google’s settings for ads personalisation and for sharing web & app activity requires the user to actively go into the privacy dashboard in order to disable them. On the other hand, the settings to store Location History, Device Information, and Voice & Audio Activity are turned off until the user actively enables them.



5 Google other options and ad settings (desktop)



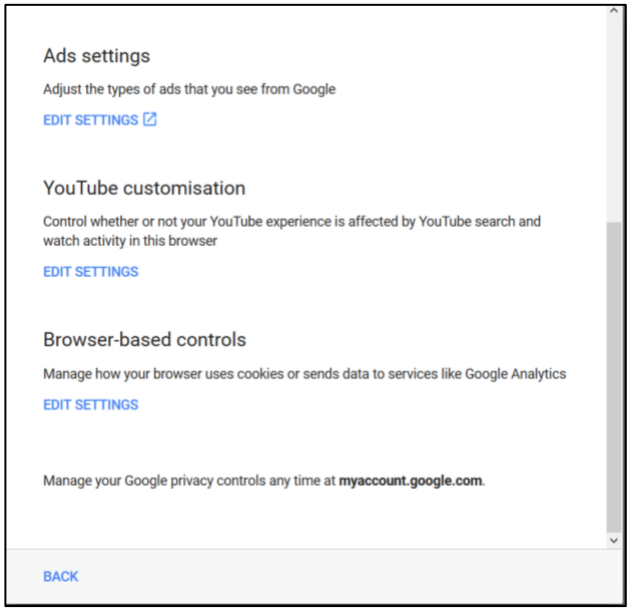
6 Google ad settings (desktop)

Facebook and Google both have default settings preselected to the least privacy friendly options.

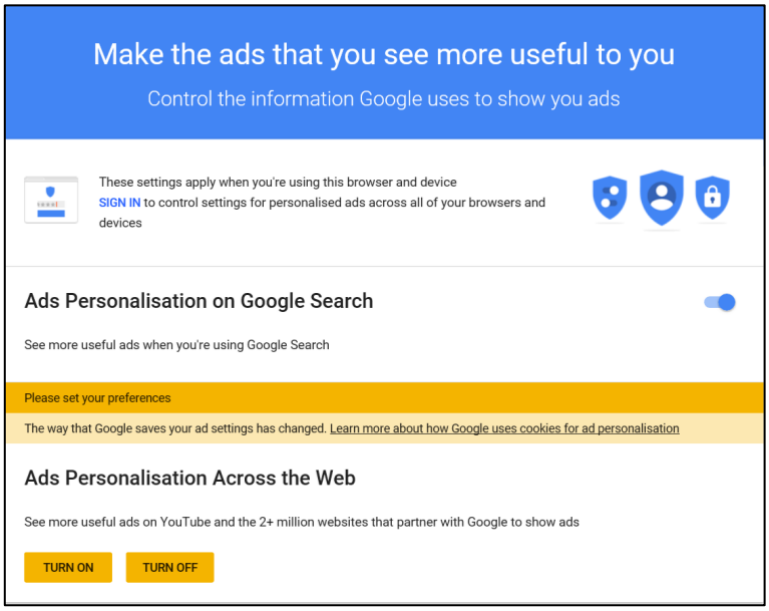
Additionally, both services hide away or obscure preselected settings so that users who simply click through the “Agree” or “Accept”-buttons will never see the settings, and it is hard to know what is preselected. We have chosen to call this “hidden defaults”. An example from Google’s ads settings and Facebook’s face recognition settings illustrate this.

In the introduction page of Google’s GDPR-popup, the user must scroll through some screens of text. Among other things, it is noted there that users can “opt out of seeing ads based on your interests”. The user can choose to “agree” or click the “edit settings” button after scrolling. If the user chooses to edit their settings, the next page introduces the actual ads settings. Here, the only text introducing the ad settings choice is “Adjust the types of ads you see on Google”. The user must remember the note on ad settings from the introduction page to know that ads personalization is turned on by default. This is a somewhat hidden default, where the least privacy friendly option is turned on by default. Note that the desktop version of the Ad Settings is somewhat different from the mobile version. The option for “Ads Personalisation on Google Search” is on by default also in the desktop version. The desktop version, however, has two buttons to ”turn on” or “turn off” “Ads Personalisation Across the Web”, and since neither of the two buttons are preselected, it is not clear which option would be turned on if the user did not visit the Ad Settings.

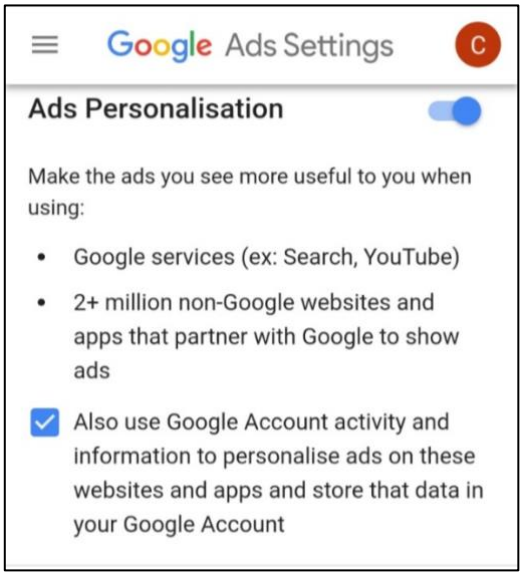
On the mobile version, both options are controlled by one button, which is on by default.



7 The Google GDPR popup leads users into the privacy dashboard (desktop)



8 In the desktop version of Google's ads settings, it is impossible to tell if "Ads Personalisation Across the Web" is turned on or off by default.

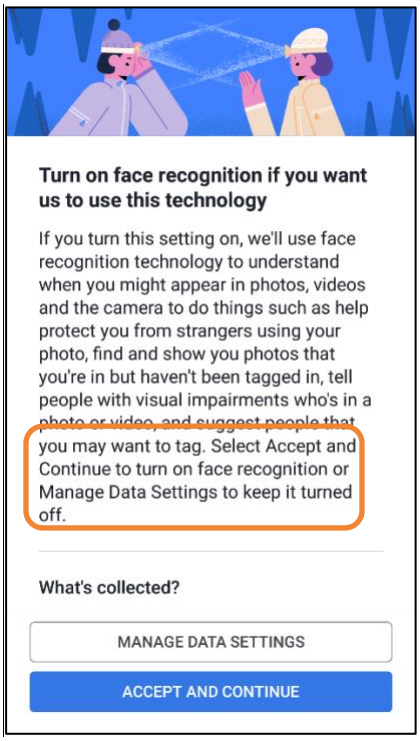


9 In the mobile version of Google's Ad Settings, all personalised ads are turned on by default.

Regarding using third party data for ads personalisation, Facebook explains the content of the setting in the introductory page: "We show you better ads by using data from advertisers, app developers and publishers". Therefore, they are not obscuring this particular default setting.

In the example of face recognition, however, Facebook effectively hides privacy-intrusive default settings from the user. Despite the headline "Turn on face recognition if you want us to use this technology", users who want to change the setting and turn on face recognition, do not have to do anything except click "Accept and continue".

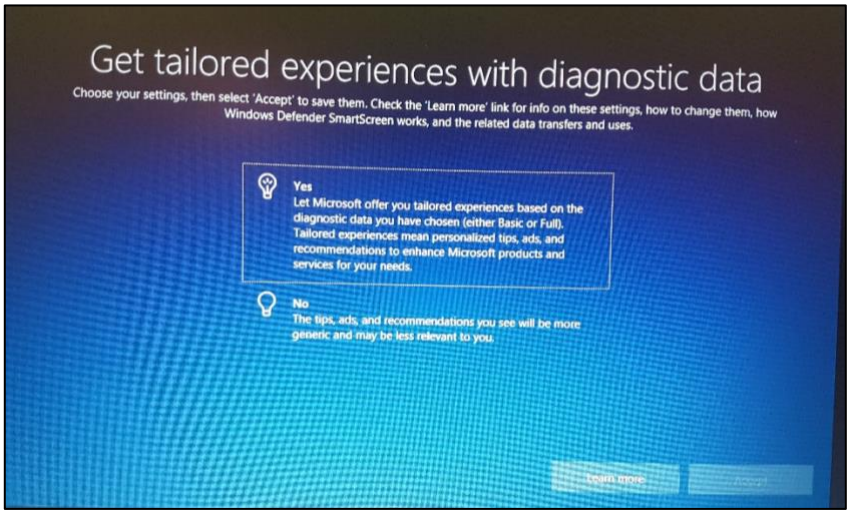
Users that want to keep face recognition turned off, have to go into the settings and *actively select* off. For the many who do not click manage data settings, the least privacy friendly choice is in fact preselected. Note that choosing the most privacy friendly option requires four more clicks than the least privacy friendly option. That neither option is preselected once one have clicked through form "Manage data settings", only sugar-coats the fact that the least privacy friendly option in fact is preselected through the design.



10 Facebook Face recognition settings (mobile)

Taken together, Facebook's combination of privacy intrusive hidden settings, and confusing wording obscuring what the "Accept"-button actually does, constitutes a dark pattern. Users that do not wish to accept more data collection should not have to search for the default settings in order to turn them off.

The Windows 10 update requires users to actively click on the choice they prefer for every step. There are no preselected choices, so in order to progress the user must make an affirmative selection. The use of design and wording is elaborated upon in 4.3, but the choice architecture is an example of giving users an explicit choice, rather preselecting an option that is preferred from the service provider's side.



11 Windows Update diagnostic data option

By requiring users actively to opt in to data collection, Microsoft and the Windows 10 update is the only one of the three services to respect user agency through not preselecting a default option.

Hiding and obscuring the preselected defaults is a step beyond having privacy-intrusive defaults. In our view, the question could be raised whether the default settings in the Facebook and Google popups are contrary to privacy by default and informed consent.

4.2 Ease - Making the privacy option more cumbersome

If the aim is to lead users in a certain direction, making the process toward the alternatives a long and arduous process can be an effective dark pattern. This relates to the issue of defaults, since the default setting clearly is the easiest option for the user. It is however also easier to see and act on some designs or colours than others, and making some buttons or options more salient may also affect our choices. For example, Google once famously tested 41 different shades of blue to measure user responses, illustrating that for some companies, a lot of effort is put into effective design. [30]

In Facebook's GDPR-popup, the interface was designed with a bright blue button enticing the users to "Agree and continue". Taking the easy path by clicking this button, took the user to a new screen about face recognition, with equivalent similar button to accept and continue[31].

On the other hand, users who wanted to limit the data Facebook collects and how they use it, had to first click a grey box labelled "Manage data settings",

[30] "Putting a Bolder Face on Google"
https://www.nytimes.com/2009/03/01/business/01marissa.html
[31] To see choice architecture of the Facebook popup illustrated in a flowchart, see appendix 1

where they were led through a long series of clicks in order to turn off "Ads based on data from partners" and the use of face recognition technologies. This path was, in other words, considerably longer.

The contrast of blue buttons for accepting, and dull grey to adjust settings away from the default, is an example of design intended to nudge users by making the "intended" choice more salient.[32] In other words, the option that the service provider wants users to choose was deliberately made more eye-catching. In addition, the user cannot know what awaits under the "manage data settings" button – there might be many settings and difficult issues to handle, and the user probably opened the service because she wanted to use it, not to work through a variety of settings. The easiest way to return to using the service is to accept and continue.

12 Facebook GDPR popup (mobile)

Users that were in a rush to use Facebook were inclined to simply click the blue button and be done with the process, which results in the maximum amount of data collection and use. This "easy road" consisted of four clicks to get through the process, which entailed accepting personalised ads from third parties and the use of face recognition.[33] In contrast, users who wanted to limit data collection and use had to go through 13 clicks. By making it simpler and more streamlined to allow the collection of the largest amount of data, in comparison to limiting data sharing, Facebook were nudging users toward the former.[34]

The Google GDPR popup was similarly designed, with a blue button to accept and continue using the service, and the alternative requiring clicking through a number of different submenus, some of which required the user to leave the popup and move into Google's privacy dashboard[35].

13 Google GDPR popup (desktop)

[32] "A flaw-by-flaw guide to Facebook's new GDPR privacy changes" https://techcrunch.com/2018/04/17/facebook-gdpr-changes/

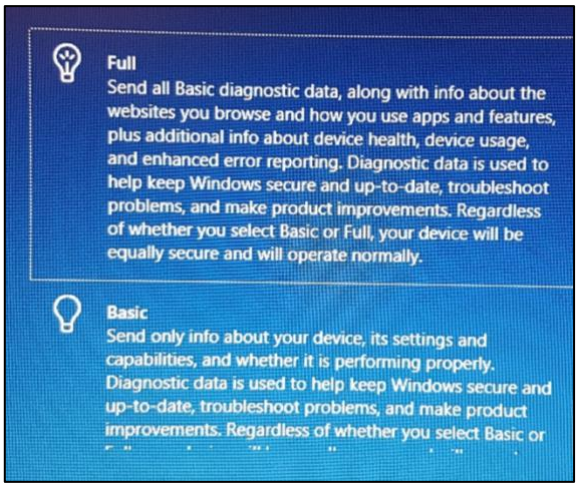
[33] An additional set of options were presented to some users regarding processing and sharing data with special protections. Not all users were presented with these options, and we have therefore not chosen to focus on this.

[34] "Facebook Is Steering Users Away From Privacy Protections" https://www.wired.com/story/facebook-is-steering-users-away-from-privacy-protections/

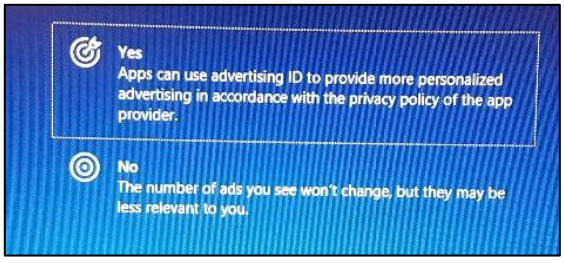
[35] To see the choice architecture of the Google popup illustrated in a flowchart, see appendix 2.

In Microsoft's Windows 10 update, the number of clicks for "no" equalled the number of clicks towards "yes". This illustrates that it is possible to design choice architecture that lets users choose to easily limit data collection[36].

Even so, the visual cues and symbols in the Windows update were loaded toward affirming data sharing. For example, if the user wanted to opt out of "tailored experiences with diagnostic data", they had to click a dimmed lightbulb, while the symbol for opting in was a brightly shining bulb. For the choice to let apps use an Advertising ID, the "Yes" choice was accompanied by an arrow hitting its target, while the "No" choice had an empty target. The opt-in choice was also always placed at the top. These are nudges towards clicking yes. However, these nudges can be considered softer, or at least more discreet, than forcing the user to click through extra settings pages in order to choose the more privacy friendly option.[37]



14 Windows Update



15 Windows Update

[36] To see the Windows update choice architecture illustrated in a flowchart, see appendix 3.

[37] Microsoft and Windows 10 has faced criticism for their data collection and use. However, these practices were not particularly apparent in the Windows 10 update that was analysed in this report. "EFF blasts Microsoft over Windows 10 privacy concerns" **https://www.theverge.com/2016/8/22/12582622/eff-microsoft-windows-10-privacy-concerns**

All of the services nudge users toward accepting data collection through a combination of positioning and visual cues. However, Facebook and Google go further by requiring a significant larger amount of steps in order to limit data collection.

4.3 Framing – Positive and negative wording

In order to nudge users toward making certain choices, the way that the different options are framed is an effective motivating factor. Focusing on the positive aspects of one choice, while glossing over any potentially negative aspects, will incline many users to comply with the service provider's wishes. This is another example of a dark pattern.

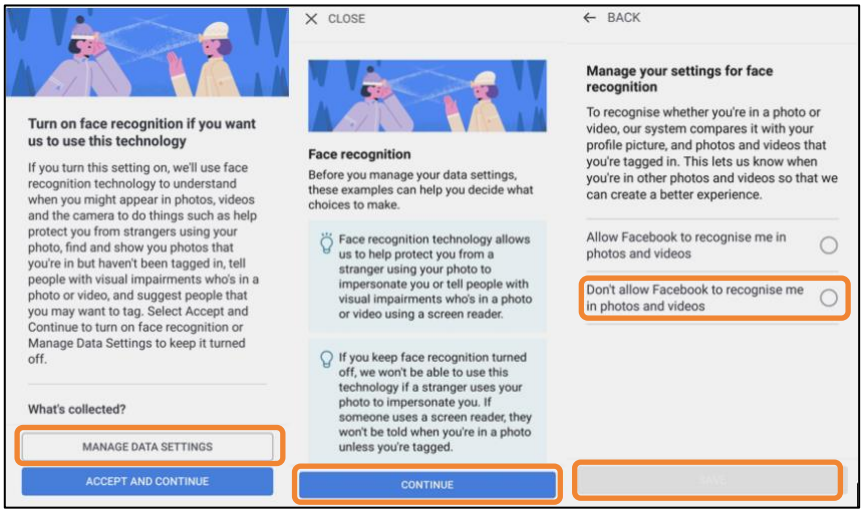
For example, Facebook's face recognition technology was stopped in Europe in 2012, due to data protection issues.[38] The feature was rolled out in Europe again as a part of the GDPR popup. Rather than addressing or attempting to alleviate such concerns, Facebook focus on the positive sides of data sharing.

Face recognition entails processing biometric data, which is considered a special category of personal data under the GDPR, and requires a separate and explicit consent in order to be processed. Upon clicking through the Facebook GDPR popup, users were asked whether they consent to the use of facial recognition technologies. The technology is, according to the popup, used for purposes *"such as help protect you from strangers using your photo"* and *"tell people with visual impairments who's in a photo or video"*.

The next screen informed the user *"if you keep face recognition turned off, we won't be able to use this technology if a stranger uses your photo to impersonate you. If someone uses a screen reader, they won't be told when you're in a photo unless you're tagged"*. This framing and wording nudged users towards a choice by presenting the alternative as ethically questionable or risky.[39]

[38] "Facebook Turns Off Facial Recognition In The EU, Gets The All-Clear On Several Points From Ireland's Data Protection Commissioner On Its Review" https://techcrunch.com/2012/09/21/facebook-turns-off-facial-recognition-in-the-eu-gets-the-all-clear-from-irelands-data-protection-commissioner-on-its-review/

[39] This practice is also known as "Confirmshaming" https://darkpatterns.org/types-of-dark-pattern/confirmshaming



16 Facebook face recognition settings (mobile)

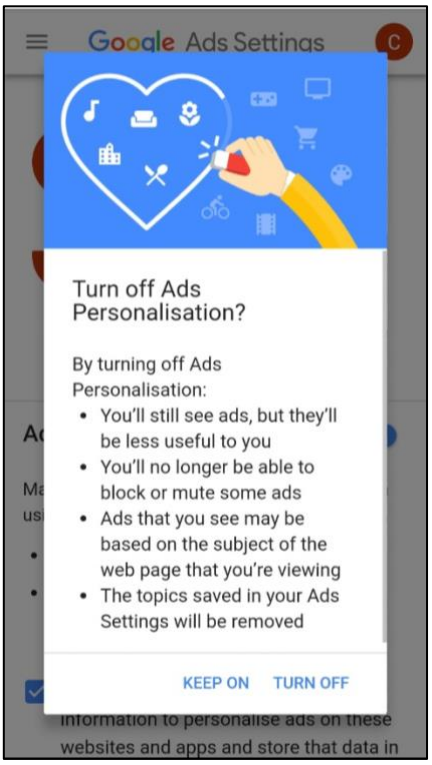
As the example above demonstrates, Facebook made a convincing argument for turning on the face recognition feature. However, users were not informed about the complete scope of how Facebook may use this data. A selective use of examples was employed to convince the user that letting Facebook use the user's biometric data would both help the user stay secure, and assist the visually impaired.

In the popup, the user was informed that face recognition "lets us know when you're in other photos or videos so that we can create a better experience". It was not mentioned what limitations are in place on how Facebook may use this information. For example, the use of face recognition could be used for targeted advertising based on emotional states,[40] or to identify users in situations where they would prefer to remain anonymous.

By framing the use of face recognition in a solely positive manner, deliberately leaving out any possible negative consequences, Facebook nudged users toward enabling the option without fully informing them. In fact, an appeal to helping the user stay more secure, and to assist visually impaired users, is used to collect highly sensitive personal data. This obfuscated important factors that should have been presented to the user in order to make an informed choice.

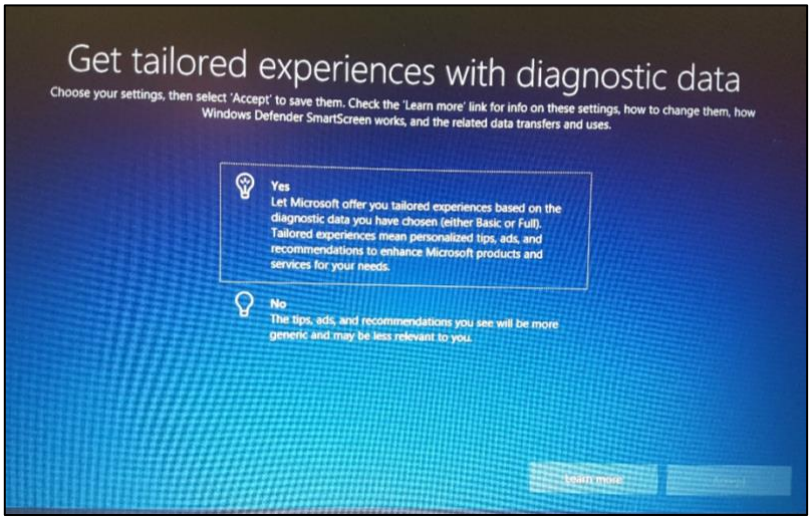
[40] "Inside The Orwellian World Of Ad-Funded Face-Recognition Technology" http://www.businessinsider.com/advertisers-using-facial-recognition-technology-2013-5?r=US&IR=T&IR=T

The way that Google presents the option of receiving personalised ads is also rose-tinted. After the GDPR popup led the user to the privacy dashboard, the setting was presented as “Make ads more relevant to you”. If the user tried to turn the setting off, a popup window appeared explaining what happens if Ads personalisation is turned off, and asked users to reaffirm their choice. There was no explanation about the possible benefits of turning off Ads Personalisation, or negative sides of leaving it turned on. Instead, the user was informed that “You’ll still see ads, but they’ll be less useful to you”.



17 Google Ads Personalisation settings (mobile)

The Windows 10 update used similarly loaded language in the same way as Google and Facebook. When asking users to choose whether Microsoft can allow apps to use the users’ Advertising ID to personalise ads, users were only told that denying this permission would result in less relevant ads. Additionally, every setting in the process was framed as a statement, such as “Improve inking and typing recognition” and “Get tailored experiences with diagnostic data”. Allowing data sharing was always framed as a positive “Yes”, while restricting sharing and collection was a negative “No”.



18 Windows Update

All three companies presented the settings that maximise data collection as the positive option. Dark patterns such as skewed wording, focus on positives such as “improve services”, glossing over potential negative consequences, and not

explaining the full extent of the choices, all serve to nudge users toward allowing wider data collection and use.

4.4 Rewards and punishment

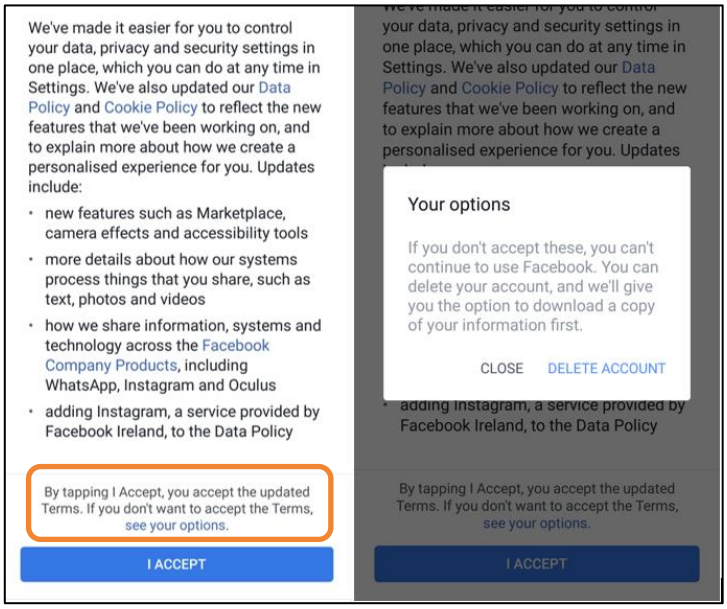
In order to entice users to make certain choices, a common nudging strategy is to use incentives to reward the "correct" choice, and punish choices that the service provider deems undesirable.[41] The reward could be extra functionality or a better service, while the punishment might be the opposite. This is particularly problematic if the reward and punishment is not directly related to the choice that is being presented.[42]

On the last page of Facebook's GDPR-popup, users were presented with an apparent choice regarding the new user terms. Hidden above the big blue "I accept"-button, the clickable text said "see your options". Clicking the text lead the user to another choice, between going back and accepting the terms, or deleting their account. Since users potentially have years' worth of information stored on their profiles, along with their network of friends and associates, this does not seem like much of a choice. Although users will get the option to download their data, the threat of deletion will probably be punishment enough to deter most users, leading them to accepting the terms. This use of ultimatum is sometimes referred to as a "take it or leave it" situation. [43]

[41] "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online", page 22 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2859227

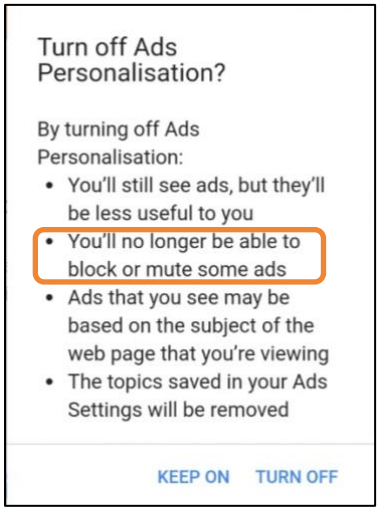
[42] For example, it makes sense that users who do not consent to the use of location data will not be able to see their current location in a map service. If users are blocked from accessing the map at all, however, this is not proportional nor directly related to the choice.

[43] This take it or leave it choice is one of the main points of a complaint against Facebook to the Austrian data protection authority. The NGO NOYB claims that this sort of "take it or leave it" ultimatum is not in accordance with the GDPR. See "COMPLAINT UNDER ARTICLE 77(1) GDPR" https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf



19 Facebook GDPR popup "see your options" (mobile)

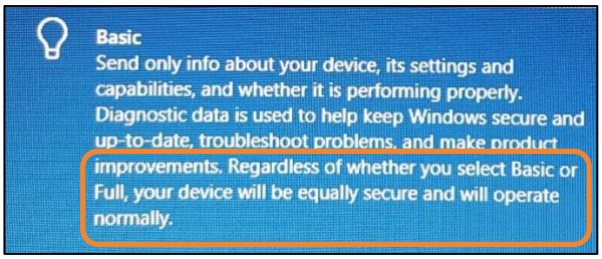
When attempting to opt out of personalized advertising through Google's GDPR Popup, and being sent to the privacy dashboard, users were, among other things, told that they will lose the ability to block or mute some ads. Note that there was no explanation of what "mute ads" entails.[44] For example, this could mean the lack of ability to turn off the sound in ads (e.g. on YouTube), or to disable certain kind of ads. When it is not clear what 'mute ads' actually means, some users could worry about choosing this option, since for example noisy ads in a work environment would be very problematic.



20 Google Ads Personalisation warning (mobile)

By contrast, at one point of the Windows 10 update, users were presented with a choice between sending "basic" or "full" diagnostic data to Microsoft. Both options included a disclaimer that "regardless of whether you select Basic or Full, your device will be equally secure and operate normally". This assures users that they will not be denied any functionality if they choose not to share more data than necessary. In short, this illustrates how it is possible to present choices about data sharing without enticing or nudging users by promising rewards or threatening with punishment.

[44] According to Google Support, The "Mute This Ad" feature provides users with the ability to control the ads they see and signal which ads aren't interesting to them" https://support.google.com/adxbuyer/answer/2695260?hl=en



21 Windows Update diagnostic data options

Many users may need such reassurance in order to select the no or turn off option, since their main concern is that they want their service to function, and might fear having to return to the settings that took away important functionality.

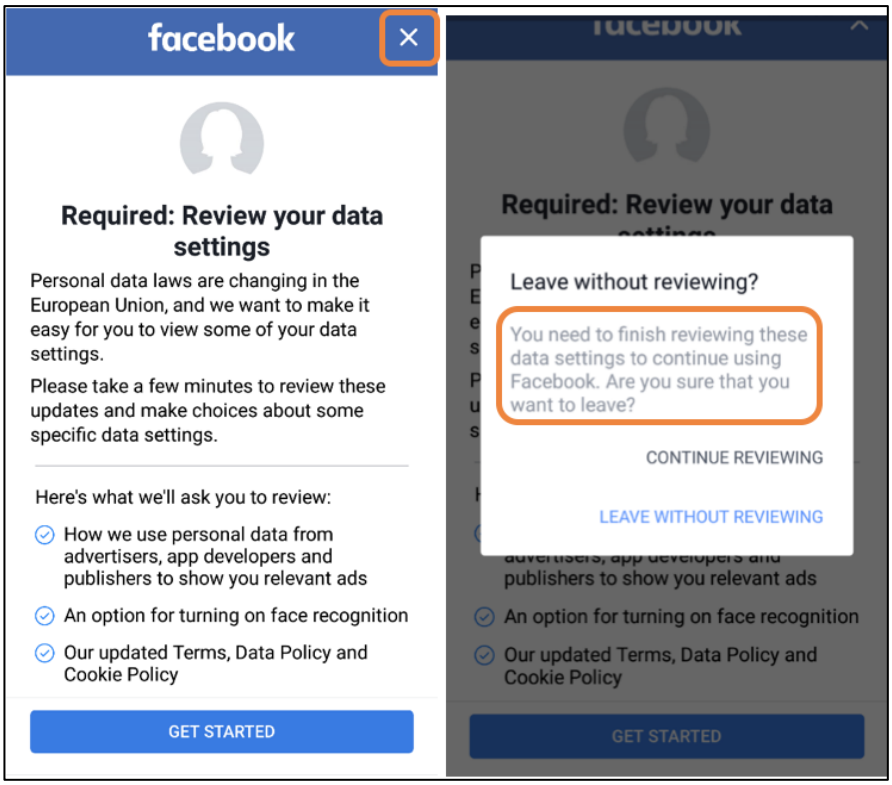
Through warning users with account deletion or the loss of functionality if they decline or opt out, Facebook and Google are nudging users towards accepting.

4.5 Forced action and timing

Consumers are often using digital services on their phones while on the go. Forcing users to choose between actions on the spot is therefore a particularly strong nudge.

Both Facebook and Google's popups showed up when the user attempted to use the service. Windows' update was an integrated part of the Windows 10 update.

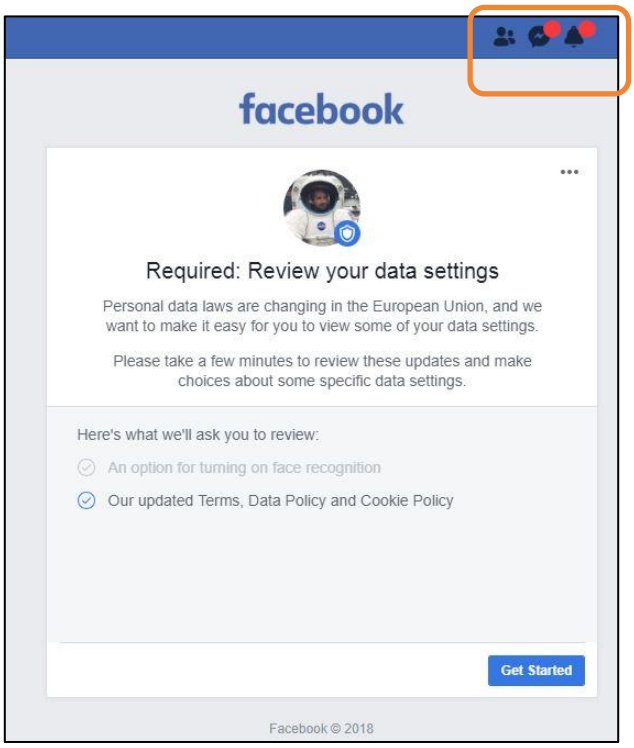
When users first received the Facebook GDPR popup, they had two options. Either they could click "Get started", or they could click the X in the corner to close the popup. Doing the latter resulted in another popup that stated, "You need to finish reviewing these settings to continue using Facebook". This gives the impression that the user will be blocked from using Facebook until the settings have been reviewed. This turned out to be false. Users could effectively postpone their choices by exiting the prompt. One can assume that the user opening their Facebook app was interested in accessing Facebook as soon as possible. Therefore, the only choice appeared to be clicking "get started".



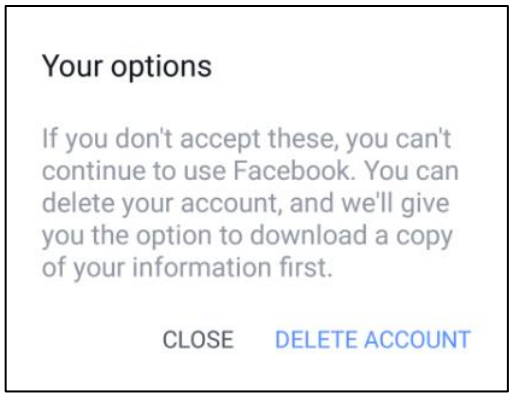
22 Facebook GDPR popup cancellation options (mobile)

On the desktop version of the app, the Facebook GDPR popup could, according to the information available, not be circumvented without going through the process. Red dots signifying message notifications were the only part of the regular Facebook interface that was visible during the process, leading the user to think that there were messages waiting. These dots were displayed even if the user did not have any unread messages. This placed further pressure on the user to go through the process quickly, and not delete the account, so that these apparent messages could be read.[45] If this was in fact a deliberate design from Facebook, this is a very clear example of use of dark patterns to manipulate users.

[45] "COMPLAINT UNDER ARTICLE 77(1) GDPR", page 6 https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf



23 Facebook GDPR popup (desktop)



24 Facebook GDPR popup (mobile)

Once the user had gone through the process, the final screen asked the user to accept Facebook's terms & conditions and privacy policy. There was also a clickable text that stated, "If you don't want to accept the Terms, see your options". Clicking this text another window popped up titled "Your options". The window read, "If you don't accept these, you can't continue to use Facebook. You can delete your account, and we'll give you the option to download a copy of your information first". There were two further options to click, "Close" and "Delete account".

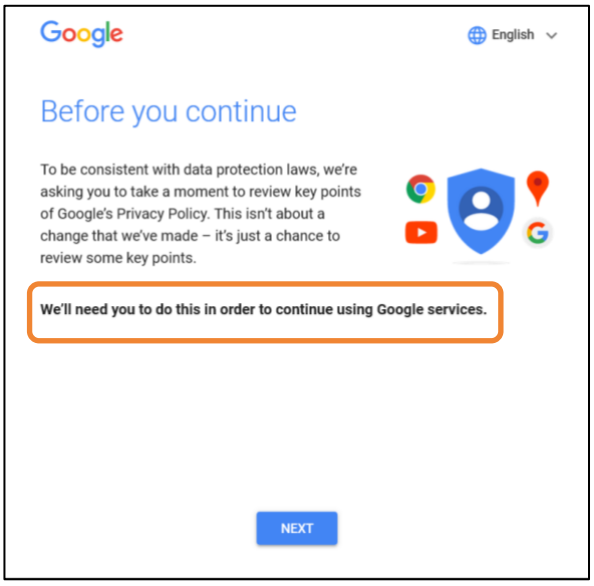
In other words, in order to access their account, the user had to implicitly read and agree to the terms (21 pages of text).[46] Otherwise, their only option was to delete their account. Assuming that deleting their account entirely is not a viable option for most users, this forces the user to accept the new terms immediately. By using this technique, Facebook was practically forcing the user to accept a very long set of legal documents in order to access their profile, or leave the service.

[46] For the Facebook Terms of Service, Cookie Policy, and Data Policy, as of 15.06.2016.

When the user is trying to access their account, a popup that leaves no choice but to agree or leave is a powerful nudge toward the quick and easy solution. For example, if the popup appeared just when the user is trying to read a message, or access information on an event they are about to attend, the immediacy of the task can reduce the likelihood that the users take the time to read through what they are actually agreeing to.

With Facebook's popup, any attempt to leave the popup without agreeing resulted in a note saying that the account would be inaccessible. A clear option to postpone the decision would have alleviated this problem, by letting the users look at their options at a time that is convenient for them.

Google's GDPR popup also stated that the user must review the settings before continuing use of the service. Users had to scroll through a short summary of Google's privacy policy, and according to the text, reviewing the popup seems to be a prerequisite for continued use of Google's services.



25 Google GDPR popup (desktop)

The Windows settings came directly following a major system update. The actual update was possible to postpone, but the privacy settings were mandatory, and directly followed the update. Upon device start-up, the user had to go through the process of choosing privacy preferences. There was no way to access the operating system until the process has been finished. This introduced an unnecessary urgency to the process.

Users that are in a hurry to access their computer, will be unlikely to take the time to actually reflect on the choices provided, although the lack of a default setting means that they are forced into making active choices. If these options had been presented before proceeding with the installation, users who were in a hurry would also have had the option to postpone their choices to a more convenient time.

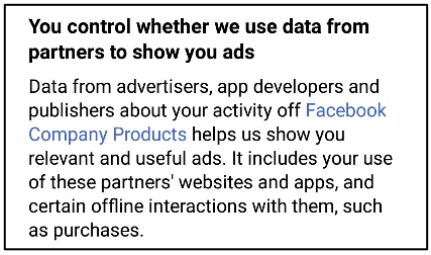
From a service provider point of view, one can argue that there is never a good time for prompting users to consider new terms of service or new settings. Users simply want to use the service. It is however clear that timing can be used, in combination with other techniques, to nudge users into acceptance or to make certain choices.

All three services put pressure on the user to complete the settings review at a time determined by the service provider, without a clear option to postpone the process.

5 Illusion of control

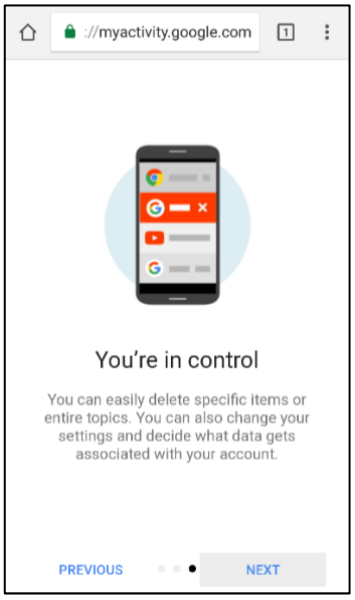
Through their GDPR popups and privacy dashboard, both Facebook and Google emphasise that they are giving users control of their data (screenshots 26 and 27).

Studies have indicated that users who perceive that they are given more control, are also susceptible to take more risks when disclosing sensitive information. This is called the control paradox.[47] This makes it particularly important that the controls are actually effective, and that they do what users expect. If users are only given an illusion of control, this can be considered a dark pattern used to manipulate users.



26 Facebook GDPR popup, ads settings (mobile)

[47] "Gone in 15 Seconds: The Limits of Privacy Transparency and Control" https://www.computer.org/csdl/mags/sp/2013/04/msp2013040072.html



27 Google My Account splash page (mobile)

Here, we consider whether users are given the illusion of control through the use of two examples. First, we analyse the controls we are given in Facebook's GDPR popup: 'You control whether we use data from partners to show you ads' (see screenshot above). Are users given substantial control, and what do the settings actually control?

Thereafter we look at the privacy dashboard that Google leads users into through their GDPR popup, and consider whether it is possible for the user to "easily delete specific items or entire topics" as promised in the splash screen for the My Activity-page, which is part of the privacy dashboard (screenshot 27).

5.1 Facebook: "You control whether we use data from partners to show you ads"

We have seen that the choices that users are provided are not always clear cut. Facebook has drawn criticism for extolling the virtues of putting users in control, despite giving very few options to limit the amount of data that Facebook themselves can actually collect and/or use.[48]

As noted, the Facebook GDPR popup universally provided three perceived options. First, the option to opt out of ads using data from third parties. Second, to accept or turn off face recognition. Finally, the user can accept the terms, or delete their account.

[48] "No, Mark Zuckerberg, we're not really in control of our data" https://www.washingtonpost.com/news/the-switch/wp/2018/04/12/no-mark-zuckerberg-were-not-really-in-control-of-our-data/?utm_term=.ba39a38680fc

The setting about allowing Facebook to display ads using data from third parties warrants a closer look (screenshot 28).

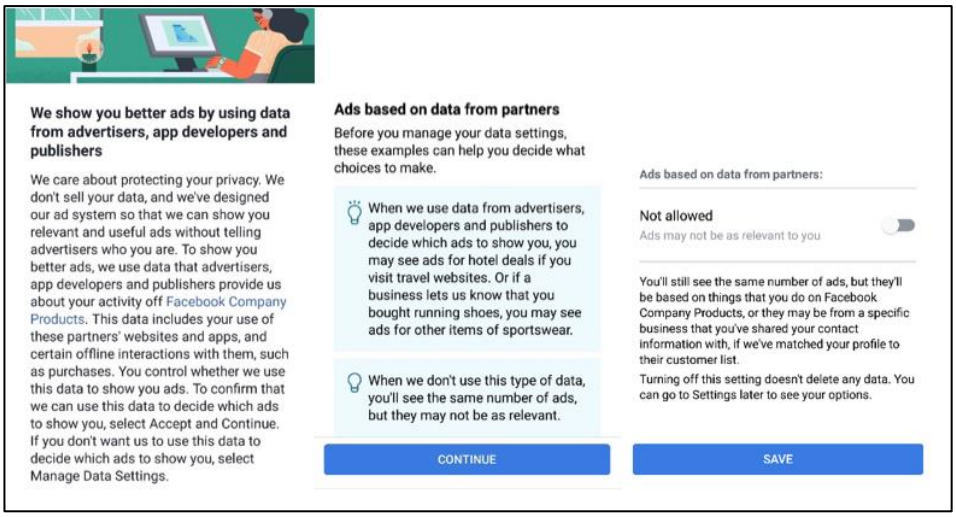
From reading the headline "You control whether we *use data from partners* to show you ads", it is clear that it is not a question of controlling data collection, but it is a setting about what ads the user will see. We argue that this is a quite limited scope of control.

Since many are not aware of how their data can be used, this setting could still be misunderstood by users as giving them more control of data use than what it really entails. In fact, this setting, and the GPDR popup in general, gives users no control over other uses of data than ads personalisation and face recognition. For example, control of how Facebook shares user data with third parties is not included in the scope in the GDPR popup.[49]

That the setting only lets you control how *data from partners* is used to show ads, imposes another limitation to what the user actually controls. Facebook is an enormous ecosystem for collecting and processing data about the user. Therefore, the option to stop only the use of data from third parties for personalised ads is a far cry from switching off personalisation of ads.

If the user chooses to turn off use of data from partners to show ads, another limitation is presented to the user: A disclaimer states that turning off the setting means that ads "will be based on things that you do on Facebook Company Products, *or they may be from a specific business that you've shared your contact information with, if we've matched your profile to their customer list*" (see screenshot below). In practice, this seems to say that even if users turn off the option to show "ads based on third party data", they will still be shown data from certain third parties that "you've shared your contact information with". What kind of data, and what third parties that the user has actually opted out of, is not clear.

[49] For examples of how third parties have been able to use data from Facebook, see the Cambridge Analytica scandal. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
Facebook have also drawn criticism for allowing device makers to access user data. "Facebook Back on the Defensive, Now Over Data Deals With Device Makers" https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships-criticized.html



28 Facebook GDPR popup, Ads settings (mobile)

In effect, users can only choose to limit advertising based on an unspecified subset of third party data. At the same time users may feel that they are in control – which may compel them to share more. Additionally, users are not presented any actual choices about what data Facebook *collects* from third parties.[50]

If Facebook intended to give users real control over how their data is collected and used, they should have given users choices that are more impactful as part of their GDPR-popup.

In the end, we conclude that users seem to not have been given a substantial choice, even after going through the extra effort of changing their settings with the intention of using their data protection rights.

5.2 Google: «Easily delete specific items or entire topics"

Both Google and Facebook offer a lot of settings and options through their respective privacy dashboards.

As mentioned, Google are known for their meticulousness when it comes to user interaction design. Therefore, it stands to reason that these design patterns are carefully tested and considered.

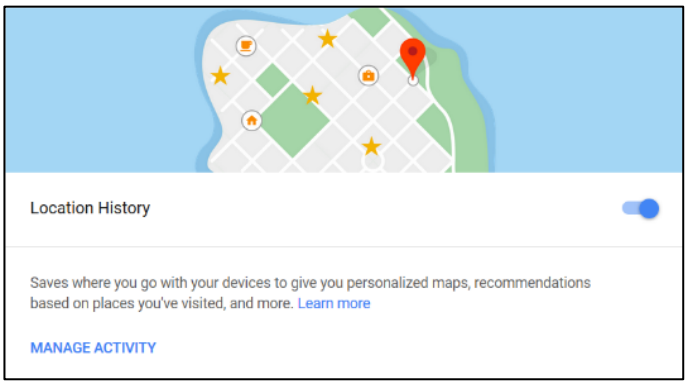
We wanted to check Googles claim that their controls can be used to "easily delete specific items or entire topics" (screenshot 27).

In order to test Google's claim about the ease of deleting "specific items" or "entire topics", we attempted to delete all location data from a dummy Google

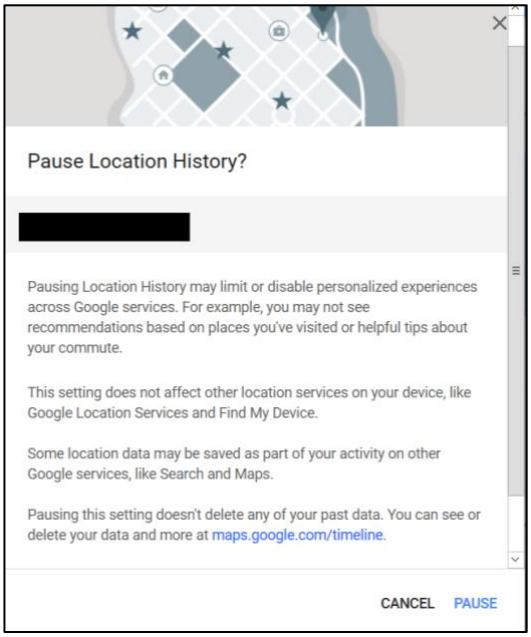
[50] Facebook has been criticised for tracking consumers across the web, also if the consumer does not have a Facebook account. "Facebook 'tracks all visitors, breaching EU law'" https://www.theguardian.com/technology/2015/mar/31/facebook-tracks-all-visitors-breaching-eu-law-report

account and two personal accounts. The user test was performed by clicking through to the privacy dashboard from the popup, and then attempting to follow the steps that a "normal" user might take if they wanted to delete their location data. The test was only performed on desktop.

The Google Privacy Dashboard offers a wide variety of options and settings.[51] The settings are spread out through many different pages. In the user test, both initial testers ended up going through between 30 and 40 different links in an attempt to locate the "delete all location data" option.



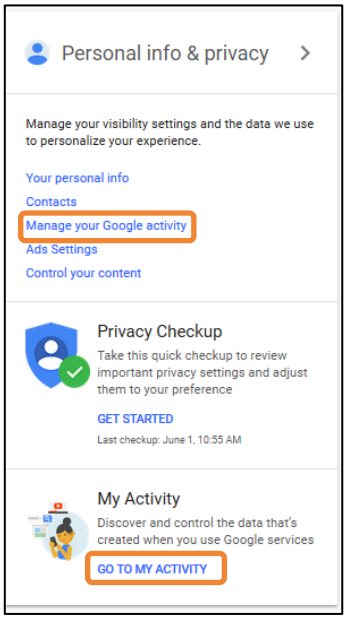
29 Google Location History, privacy dashboard (desktop)



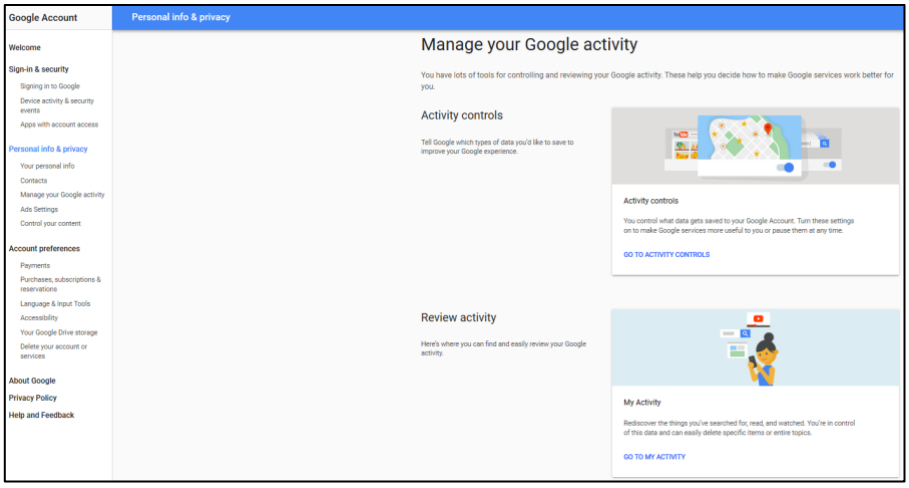
30 Google Location History settings, privacy dashboard (desktop)

In addition to "Manage your Google activity", there is also a completely different page confusingly named "My Activity", which allows bulk deletion of data.[52]

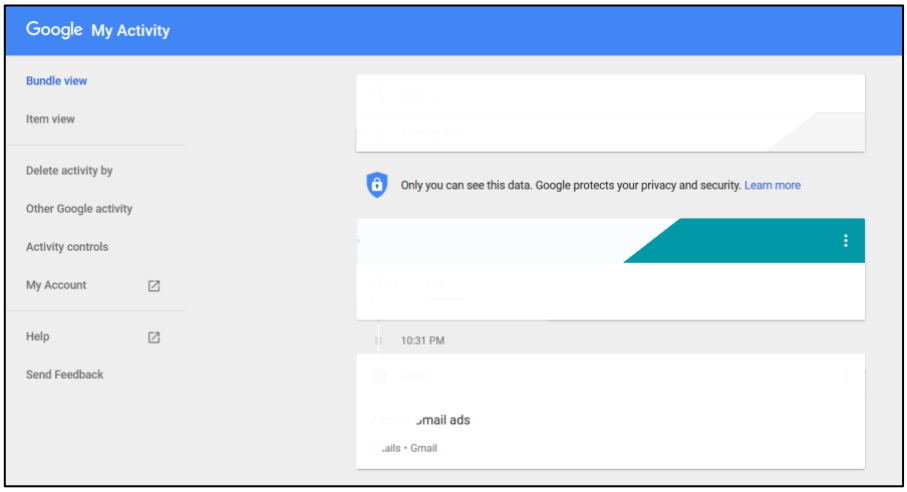
[51] https://myaccount.google.com/privacy
[52] https://myactivity.google.com/myactivity



31 Google privacy dashboard (desktop)



32 Google Manage your Google Activity (desktop)



33 Google My Activity (desktop)

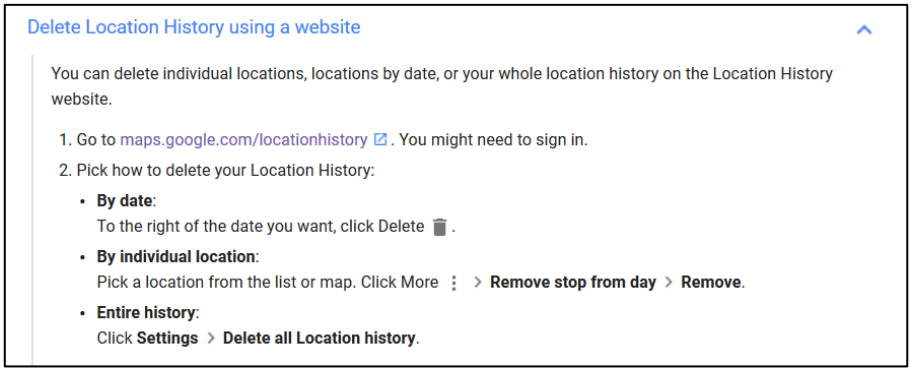
The ‘Manage Location History’ page (screenshot 35), only seemed to let users delete individual events or location points. The testers navigated back and forth through the same pages and variations of similar options several times, without being able to locate any options to delete all location history.

Some of the pages had arrows making it simple to navigate back and forth, but others did not, forcing the user to try to start over through selecting among formerly used tabs in the browser.

Another confusing factor is that the scope and form of what services the settings apply to, varies from setting to setting. In some cases the settings, such as the ads settings, automatically seem to apply to all Google services.[53] A second variant, applicable in the “delete individual events” settings, is that you can choose among any number of Google services freely from a drop down list. In the case of the option “delete all data”, one can choose all Google services or only one from a drop down list.

To delete all Google Maps data did not delete the testers’ location history, but presumably only removed all data gathered through the particular Google Maps service. In other words, Google Maps data and Google Location History have separate controls.

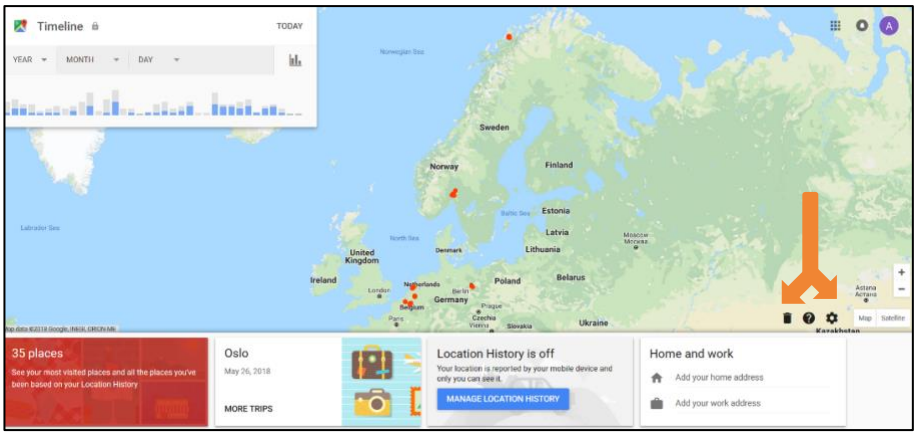
After both testers had given up finding the delete all location data option in the privacy dashboard, a Google search for “how do I delete Google location” was attempted. The search yielded a Google support site called “Manage or delete your Location History”.[54] On this page, the solution to how to delete “Entire history” was described.



34 Google support (desktop)

Screenshot 35 shows where to find the “Settings”-button, located on the Manage Location History page. As illustrated, this is not easy to find through navigating the privacy dashboard, and required a specific instruction for the initial testers.

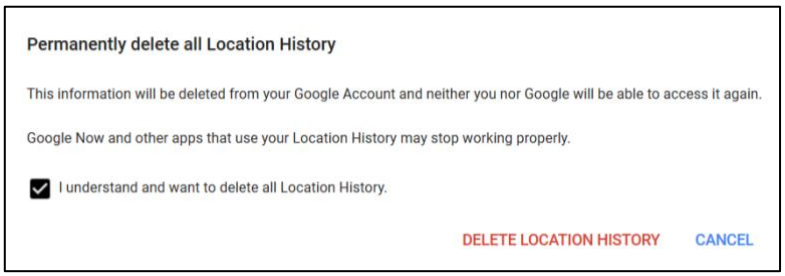
[53] Gmail, Youtube and several other services.
[54] https://support.google.com/accounts/answer/3118687?hl=en



35 Google Manage Location History (desktop)

If the user succeeds in finding the “delete all location history” option, they are met with a popup warning that deleting location history could mean that “other apps” “may stop functioning properly”, without any further explanation of what this entails.

After confirming one more time that they actually want to delete the data despite the warning, users have to click a red text placed on the left side, while the blue text placed on the right will cancel the action. The colour red is often associated with warnings of danger, while Google normally uses the blue colour for most buttons. Additionally, the cancel button was on the opposite side of its usual position in the dashboard, subverting the natural flow of clicks.



36 Google Manage Location History (desktop)

In the end, the only confirmation of the deletion of all the location data was a popup in the service. We were not offered or sent a confirmation or documentation of the deletion request and finalisation.

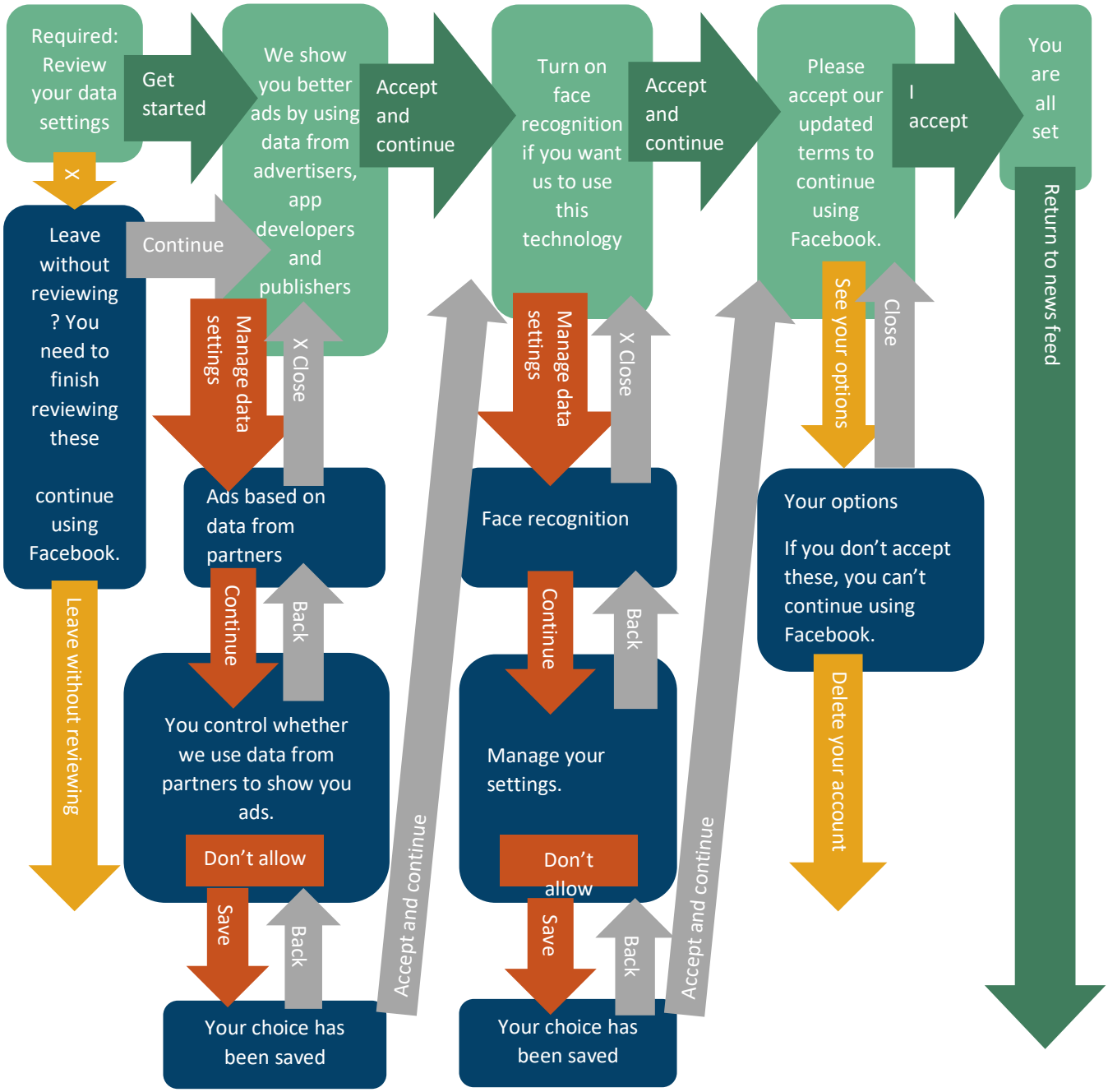
To control that the initial test was representative, several other testers with varying computer skills have performed the same test later. One tester easily came across a trashcan option in the Manage Location History, that turned out to lead to the possibility to delete all location data page (see screenshot 35). One tester got lost and another gave up after more than twenty clicks. Finally, two testers found the settings button after some rounds back and forth. This shows that it is in fact possible to delete the location history through the dashboard. However, we still conclude that most users attempting to navigate

through the Google privacy settings would likely give up before finding what they were looking for.

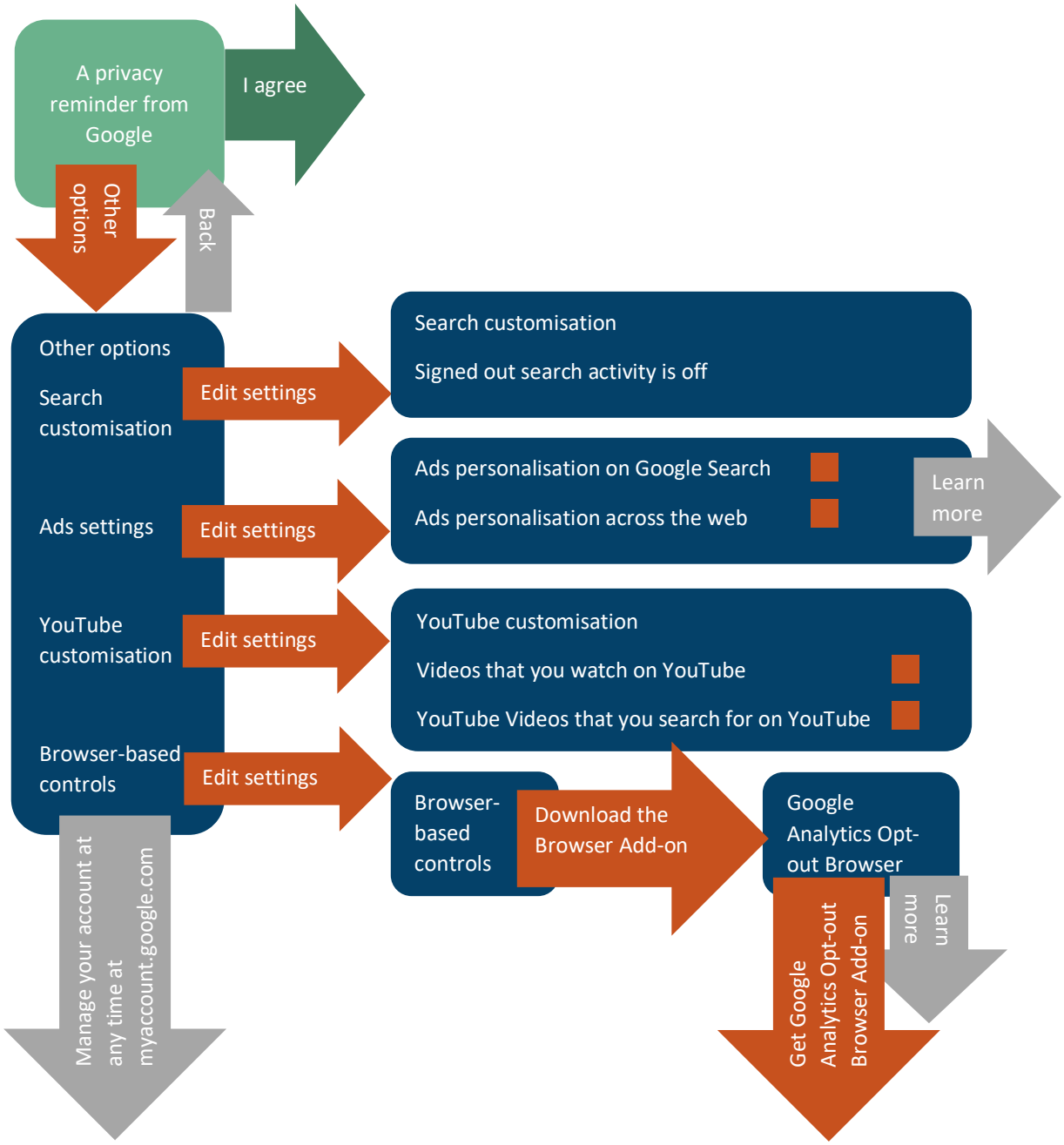
By giving users an overwhelming amount of granular choices to micromanage, Google has designed a privacy dashboard that, according to our analysis, actually discourages users from changing or taking control of the settings or delete bulks of data. Simultaneously, as noted above, the presence and claims of complete user control may incentivise users to share more personal data.

6 Appendix: Flowcharts

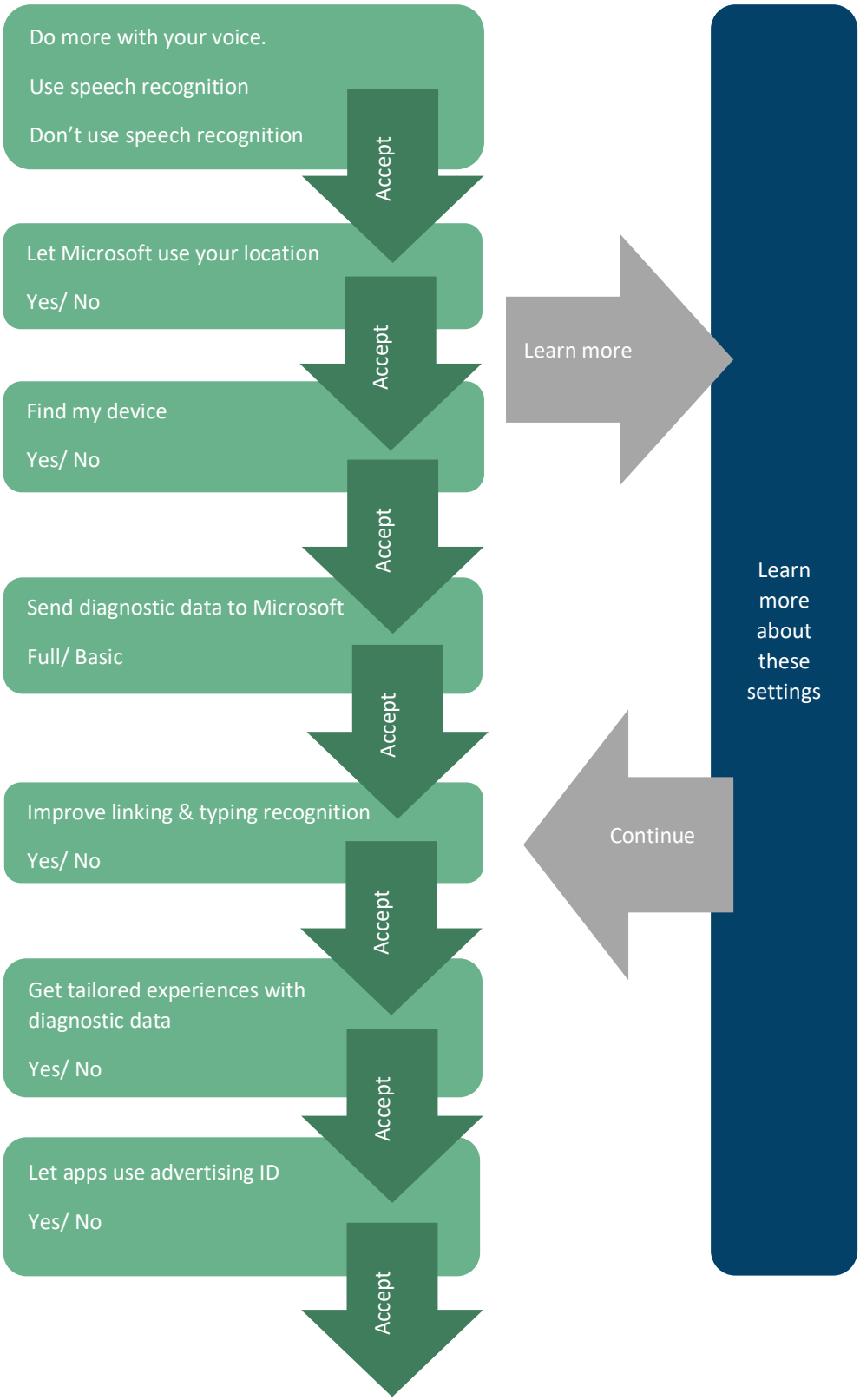
6.1 Facebook



6.2 Google


A privacy reminder from Google
I agree
Other options
Back
Other options
Search customisation
Edit settings
Search customisation
Signed out search activity is off
Ads settings
Edit settings
Ads personalisation on Google Search
Ads personalisation across the web
Learn more
YouTube customisation
Edit settings
YouTube customisation
Videos that you watch on YouTube
YouTube Videos that you search for on YouTube
Browser-based controls
Edit settings
Browser-based controls
Download the Browser Add-on
Google Analytics Opt-out Browser
Manage your account at any time at myaccount.google.com
Learn more
Get Google Analytics Opt-out Browser Add-on

6.3 Windows 10



The flowcharts explained

Green fields and arrows represent the easiest route toward returning to use the service counted in number of clicks (Facebook: 5 clicks, Google: 2 clicks, Windows: 7 clicks)

Red fields and arrows represent extra clicks when choosing to manage data settings (Facebook: 8 extra clicks, Google: 7 extra clicks, Windows: no extra clicks)

Orange arrows represent routes toward deletion of account while gray arrows represent the route back to the main route of the choice architecture. Blue fields represent extra screens met when not choosing ‘get started’, ‘accept and continue’ or ‘I accept’.

All the texts in the flowcharts are quotes from the choice architecture. While the texts in the arrows represent all texts in the choice buttons they represent, the texts in the squares in many cases only represent headlines. For full text, view screen shots.

Scrolling is not illustrated in the flow chart. The size of arrows and fields is adapted to the amount of text, and does not represent importance or design in the service. While all choice buttons that take the user to a new option page are represented by arrows, ordinary links are not included.