

DPIA on government Facebook Pages

Data protection impact assessment on the processing of
personal data on government Facebook Pages

Version 1

Date	16 November 2022
------	------------------

Status	public version
--------	----------------

Colophon

DPIA by

Ministry of the Interior and Kingdom Relations
Turfmarkt 147
2511 DP The Hague
PO Box 20011
2500 EA The Hague
www.rijksoverheid.nl/bzk

Contact

T Press department: +31 70 426 88 88

Project name

DPIA report on the processing of personal data on government Facebook Pages

Authors

Privacy Company
Sjoera Nas and Floor Terra, senior advisors
www.privacycompany.eu

Contents

Contents	1
Change log	5
Summary	6
Introduction	10
Part A. Description of the data processing	19
1. The processing of personal data.....	19
1.1 About Facebook/Meta.....	20
1.2 Processing of four categories of personal data	35
1.3 Processing for ranking and profiling	40
2. Personal data and data subjects.....	42
2.1 Definitions of personal data.....	42
2.2 Network traffic	46
2.3 Insights and Activity log of Page.....	46
2.4 Cookies and device identifiers	52
2.5 Results data subject access requests.....	62
2.6 Data subjects.....	75
3. Privacy controls	78
3.1 Privacy controls Page administrators	78
3.2 Privacy controls Facebook users	79
4. Purposes of the processing.....	81
4.1 Purposes Insights	81
4.2 Purposes observed and inferred personal data about Page interactions.....	81
5. Processor or (joint) controller	85
5.1 Definitions	85
5.2 Data processor	85
5.3 Data controller	86
5.4 Joint controllers.....	92
6. Interests in the data processing.....	95
6.1 Interests of Dutch government organisations	96
6.2 Interests of Facebook.....	96
7. Transfer of personal data outside of the EU	97
7.1 Facebook's factual transfers of personal data to the USA	97
7.2 GDPR rules for transfers of personal data	98
7.3 Legal obstacles data transfers to the USA	101
8. Techniques and methods of the data processing	103
8.1 Machine learning	104
8.2 Big Data Processing	105
9. Additional legal obligations: e-Privacy Directive	108
10. Retention periods.....	110
Part B. Lawfulness of the data processing.....	112

11.	Legal Grounds.....	112
11.1	Data observed and inferred from visits to a government Page.....	114
11.2	Facebook Insights	124
12.	Special categories of data	127
13.	Purpose limitation.....	128
14.	Necessity and proportionality	129
14.1	The principle of proportionality.....	129
14.2	Assessment of the proportionality	129
14.3	Assessment of the subsidiarity	133
15.	Data Subject Rights	134
Part C. Discussion and Assessment of the Risks		138
16.	Risks.....	138
16.1	Identification of data protection risks	138
16.2	Summary of risks	143
Part D. Description of risk mitigating measures.....		144
17.	Risk mitigating measures	144
17.1	Measures against the severe high and one low risk.....	144
Conclusions		146
Appendix 1		147
Response Meta to Dutch government DPIA on Facebook Pages		147
Response Privacy Company		148

FIGURES

Figure 1: Monthly active Facebook users in the Netherlands in June 2022	21
Figure 2: Facebook default ranking settings when following a Page	24
Figure 3: Posting from the Ministry of Privacy in the News Feed of test user C	25
Figure 4: Example of recommended post in the News Feed of test user B	25
Figure 5: Anti-government Covid posting in the News Feed	26
Figure 6: Another posting from the same source shown in the News Feed.	27
Figure 7: Facebook interfaces for posts and videos when clicking on the dots	27
Figure 8: Radical organisation 'suggested for you' in profile of test user B	28
Figure 9: Facebook recommendation to like 'De Hotspot' Page	29
Figure 10: Facebook activity log showing timestamps of likes	29
Figure 11: Related pages shown on the Page of the Ministry of the Interior	30
Figure 12: Suggested pages shown on the Page of the Ministry of the Education	30
Figure 13: Sponsored post in the News Feed of test user C for investment platform	31
Figure 14: Advertisement shown in the top right corner of the profile	31
Figure 15: Facebook explanation about this advertisement	32
Figure 16: Facebook generic explanation to users why ads are shown	32
Figure 17: Misleading content of ad shown to test user B	33
Figure 18: Other example of advertisement for cryptocurrency with explanation	34
Figure 19: Facebook banner with encouragement to log-in for non-users	40
Figure 20: Facebook description of four categories of "information"	44
Figure 21: Facebook Page performance results	47
Figure 22: Insights Current Audience	47
Figure 23: Insights potential audience for the government test Page	48
Figure 24: Facebook potential audience for the government test Page	49
Figure 25: Facebook analytics about interactions with the test Page	50
Figure 26: Hyperlink to Insights Addendum after creation of Page	51
Figure 27: Activity Log of the Ministry of Privacy test Page	52
Figure 28: Facebook cookie consent banner	53
Figure 29: Datr cookie set by the Ministry of Privacy test page	55
Figure 30: View of Facebook cookies set by employment agency Randstad.nl	55
Figure 31: View of Facebook cookies set by Bol.com	56
Figure 32: Cookie consent request when visiting test Page	57
Figure 33: Datr cookie set in browser of non-user	57
Figure 34: Facebook cookie wall	58
Figure 35: Single cookie set by Meta transparency Page	58
Figure 36: Six cookies with unique identifiers set by Facebook homepage	59
Figure 37: Facebook information about device information	59
Figure 38: Facebook further explanation identifiers	60
Figure 39: Facebook interface for users to access and manage information	63
Figure 40: Facebook screenshots in 2019 with logic why content is shown	69
Figure 41: Advertising topics initially shown to both test users	72
Figure 42: Empty menu with Ad topics a user may be interested in	72
Figure 43: Pull down menu with Ad topics a user may be interested in	73
Figure 44: Subcategories in main category 'beer'	73
Figure 45: Facebook controls for Page admins	79
Figure 46: Management interface of the test Page	79
Figure 47: Facebook cookie options for end users	80
Figure 48: Facebook statistics about FISA orders	92
Figure 49: Slide from Facebook engineer Zhao about Machine Learning	104
Figure 50: Facebook machine learning services	105
Figure 51: FBLeanner platform generates interest predictions	105
Figure 52: Process new ePrivacy Regulation	109

Figure 53: Retention period Insights	111
--------------------------------------	-----

TABLES

Table 1: 'Essential' cookies set by Facebook in browser of logged-in test user C	53
Table 2: Facebook description of observed cookies	60
Table 3: Correspondence with Facebook about data subject access requests	63
Table 4: Files obtained via Facebook's DYI	65
Table 5: Facebook events shown in reply to the access request	70
Table 6: Facebook purposes and sub-purposes	82
Table 7: Overview of US law to obtain personal data from EU Customers	87
Table 8: Specific purposes mentioned by Facebook, with legitimate interest	119
Table 9: Risk matrix based on the ICO model ¹⁸⁴	143
Table 10: Overview of Meta's responses to the high risks	147
Table 11: Response Privacy Company to Meta's view on the high risks	150

Change log

Version	Date	Summary of input
0.2	15 July 2022	First completed clean draft of part A
0.3	21 July 2022	Track changes after internal review
0.4	21 July 2022	Clean version for BZK review
0.5	24 August 2022	Track changes after input BZK and PAR
0.6	24 August 2022	Clean version to be shared with Facebook
0.7	29 September 2022	First completed draft (including parts B,C and D)
0.8	4 October 2022	Track changes after input Facebook on part A
0.9	4 October 2022	Clean version for BZK
1.0	12 October 2022	Clean version (incl new USA developments)
1.1	16 November 2022	Public version with an appendix with the view of Meta, and the response of Privacy Company

Summary

This Data Protection Impact Assessment (DPIA), commissioned by the Dutch Ministry of the Interior and Kingdom Relations, assesses the risks of the use of Facebook Pages by the Dutch government.

This DPIA is combined with a separate Human Rights Impact Assessment (HRIA), focussed on the risks for data subject's rights to non-discrimination, freedom of thought, conscience and religion, and freedom of expression and information.

Facebook/Meta

In January 2022 Facebook changed its corporate name to Meta Platform Inc. In this report 'Facebook' will be used for the social media platform, to prevent confusion with other apps offered by Meta, such as Instagram and WhatsApp.

Anyone with a Facebook account can create a Facebook Page to share contact information, post updates, share news items and interact with an audience of friends or a larger unknown public. Formerly Facebook Pages for organisations were known as *Fan Pages*. There is no separate name anymore for Pages created by businesses, brands, organisations and public figures.

Facebook users who like or follow a Page will get updates from that organisation in their *News Feed*. The *News Feed* is a dynamic list of content on every users' Facebook home Page with status updates, photos, (live) videos, links, app activity and likes from people, Pages and groups. The content is influenced by the activities and likes of friends.

Scope of the DPIA

The scope includes the generation and use of website analytics (the Insights from the Meta Business Suite) and the Activity Log, about interactions of visitors with the content of the Page. Facebook makes such statistics available to the Facebook Page owner.

This DPIA assesses the risk of the data processing by Facebook as a result of visits to a government Page. This processing includes showing individual recommendations to visitors of the Facebook test Page, and recommendations in the visitors' News Feed as a result of interacting with recommended articles or hyperlinks.

Because Facebook does not offer the possibility to create business accounts, the creation and maintenance of Facebook Pages of government organisations is often done with the private Facebook accounts of the employees of government organisations. For this reason the processing of personal data in relation to this use is also assessed in this DPIA.

This DPIA finally includes an assessment of the legal (not technical) risks of unlawful access by US government authorities to personal data processed by Facebook as a result of the use of a government Page.

Test set-up

For the purpose of this DPIA a government test Page was created (Ministry of Privacy), and two new personal Facebook accounts. During one month the two testers acted as daily visitors of the government test Page. An existing Facebook user acted as Page administrator, and interacted with the two new accounts. The two new accounts did not 'befriend' anybody but each other and the single exception mentioned below, but were given distinct behaviours. One account followed all Dutch political party leaders and (indiscriminately) liked their posts, as well as two ministries (BZK and OCW) and three public institutions (RIVM, ProDemos and KNMI) the other account befriended public LGBTI persons and the ministry of Defence and similarly liked their posts. When following Pages resulted in recommendations for other Pages, some of these recommendations were followed, resulting in the following of other Pages. All outgoing network traffic was intercepted, and automated screenshots were made every 5 seconds of the News Feed of the two test accounts, and the contents of the test Page. After completion of the test, two data subject access requests were filed with the Page administrator, and through the Page administrator, with Facebook.

Outcome: 7 high and 1 low data protection risks

The outcome of this DPIA is that there are 7 high and 1 low data protection risk when government organisations use a Facebook Page to communicate with a mass audience. This DPIA recommends a number of measures Facebook could take to mitigate these risks. Though government organisations can take some measures to partially mitigate some risks, government measures cannot mitigate all high risks. Even if the European Commission and the government of the United States conclude a new transatlantic data agreement, Facebook's global data processing may still cause risks related to the accessibility of data in other third countries without adequate data protection.

Purposes, roles and legal grounds

The report identifies 15 purposes, with additional sub purposes for which Facebook processes the personal data relating to a visit to a government Page. These purposes include many types of processing related to profiling and targeted advertising, partially based on the use of tracking cookies and unique device identifiers.

Facebook only offers a joint controller agreement for the creation of Insights, not for any other data processing by Facebook as a result of interaction with government Page content. However, this DPIA concludes that government organisations and Facebook are joint controllers for the processing of all personal data related to visits to a government Page. However, because Facebook insists on a role as independent data controller, the government organisations with Pages must have a legal ground for the sharing of all personal data to Facebook as independent third party, and Facebook must have its own legal ground. Nor Facebook, nor the government organisation can successfully invoke a legal ground, due to the multiple reasons. Facebook processes sensitive inferred data about web surfing behaviour, and does not obtain the legally required explicit consent. Facebook is not transparent about the logic of its personalisation algorithms, and what personal data it infers from website visits and communication actions. Government admins cannot opt-out from data processing of their Page visitors for commercial purposes, and Facebook makes deceptive use of tracking cookies. Technically, Facebook's big data processing can be characterised as 'obscurity by design'.

One of the purposes for which Facebook processes data, is to comply with orders from government authorities in third countries without an adequate data protection regime, such as the USA. It follows from Facebook's public reports about such disclosures that there is a realistic possibility of disclosure of personal data relating to visits to Dutch government pages to US law enforcement and secret services.

Risks and mitigating measures

The table below shows the 7 high and 1 low protection risks for data subjects, with the mitigating measures the government organisations and Facebook can take.

No	High risk	Measures government	Measures Facebook
1.	Inability to exercise data subject rights	Stop using Facebook Pages until Facebook provides meaningful access to the logic of its data processing	Provide meaningful access to the logic of the personalised content, including inferences and interest predictions and enable users to remove wrong data. Create meaningful tooling to provide such access with each posting in the News Feed.
2.	Chilling effect on other fundamental rights	Make all information also available on public webpages, outside of the Facebook platform. Warn Page admins to log-in with the Page Admin account after Page creation	Provide access for vetted researchers to actual data processed by Facebook relating to popular government Pages, to investigate if following a government Page results in an increase or decrease of different views represented in the personalisation. Additionally, researchers must be able to perform A/B testing in an isolated lab, with model accounts. Currently, Facebook prohibits the use of test accounts.
3.	Lack of transparency purposes of the processing	-	Amend the joint controller agreement for Insights to include all data processing related to government Page visits, from users and non-users, including inferred data and the prediction of the interests of users Do not force acceptance of datr cookie for non-users Use privacy by default settings with regard to cookies for users. Do not use dark design patterns.
4.	Loss of control due to further processing by Facebook	If Facebook provides a data minimisation setting: use it	Create an opt-out for government Page admins for any further processing beyond the agreed purposes in the joint controller agreement Do not force acceptance of the datr cookie

		If Facebook creates a control to limit data storage: minimise the retention period	Create a control for government Page admins to determine the retention period of the raw data relating to Page visits
5.	Loss of control due to personal data sharing with third parties	Instruct visitors to empty the cookie jar in their browser after a visit to a government Page	Do not force acceptance of tracking cookies
			Delete all Facebook cookies when users log out. Only read device IDs/cookies if there is an authentication cookie that signals that the user has logged in.
			Obtain <u>explicit</u> , informed consent for all tracking cookies, to take account of the sensitive nature of surfing data
			Obtain <u>explicit</u> , informed consent for all potential data transfers to third parties.
6.	Loss of control, re-identification of pseudonymised data due to disclosure to US authorities	Stop using Facebook Pages (reconsider if there is a new transatlantic data agreement)	Stop transferring personal data from Dutch government Page visitors to the USA. Reconsider the refusal to open a dedicated EU cloud
			Provide detailed statistics to Dutch government organisations about disclosure of personal data of visitors to Dutch government Pages
			Do not retain personal data about visits to Dutch government Pages longer than 1 week, and create weekly Insights.
7.	Filter bubble: missed messages	Invite Page visitors to subscribe to a dedicated mailing list or other non-algorithmic communication channel	Comply with Art. 29 of the DSA and offer users the option to select a non-personalised News Feed
			Enable users to opt-in to always receive messages from a government Page in the top 10 messages of the News feed.
No	Low risk	Measures government	Measures Facebook
8.	Chilling effect due to government access to Insights	No measures needed	Do not lower the aggregation level

Conclusions

This DPIA concludes that government organisations should stop using Facebook Pages if Facebook does not take measures to mitigate the high data protection risks. The Dutch government will immediately open a dialogue with Facebook.

Introduction

This report, commissioned by Ministry of the Interior and Kingdom Relations, is a Data Protection Impact Assessment (DPIA) about the use of Facebook Pages by organisations that are part of the central Dutch government. This DPIA is combined with a separate HRIA, a Human Rights Impact Assessment, focussed on the risks for data subject's rights to non-discrimination, freedom of thought, conscience and religion, and freedom of expression and information.

In January 2022, Facebook changed its corporate name to Meta. In this report 'Facebook' will be used for the social media platform, to prevent confusion with other apps offered by Meta such as Instagram and WhatsApp.

Facebook Pages

Anyone with a Facebook account can create a Facebook Page to share contact information, news items and interact with friends or a larger unknown public. Facebook Pages can be customised with stories, events and more.

Formerly Facebook Pages for organisations were known as Fan Pages. There is no separate name anymore for Pages created by businesses, brands, organisations and public figures. Government organisations can and want to use Facebook Pages to reach a broad audience, and directly communicate with people in a way they are used to, and through the platform where they already spend a lot of time. This report is about the data processing through Pages created by Dutch government organisations. The test Page created for this purpose is called government Page, but Facebook does not distinguish between commercial or government ownership of Pages.

A Facebook Page from a government organisation can be viewed by both Facebook users and non-Facebook users. Facebook users who like or follow a Page will get updates from that organisation in their News Feed. Even if they do not follow the government Page, they may see a recommendation if their friends follow the Page, or like a post on such a Page.

Legal background

The European Court of Justice ruled in 2018 that the owner of a Facebook Page is a joint controller with Facebook for the initial collection of personal data by Facebook when a user visits the Page.¹ In the Fashion ID case, about the use of a Facebook Like button by external websites, the CJEU nuanced its earlier stance, and ruled that a company or person cannot be qualified as joint controller for subsequent operations for which it does not determine either the purposes or the means.²

In June 2021 the federal German DPA issued a letter recommending all German government organisations to close their Facebook Pages by the end of the year to mitigate privacy risks.³ A few months later, in September 2021, the Norwegian DPA

¹ CJEU, Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, 5 June 2018, ECLI:EU:C:2018:388.

² CJEU, C-40/17, 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629.

³ Bundesdatenschutzbeauftragter, letter dated 16 June 2021, Facebook-Auftritte von öffentlichen Stellen des Bundes, URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2021/Facebook-Auftritte-Bund.pdf?__blob=publicationFile&v=1

published a DPIA on its own possible use of a Facebook Page and concluded the communication benefits did not outweigh the risks for data subjects.⁴ In June 2022 a law firm drafted a reply to this DPIA on behalf of Facebook.⁵

In November 2021 the appellate administrative court of Schleswig-Holstein (to whom the 2011 Page case was referred back by the CJEU) issued its ruling (after 10 years of legal proceedings). It concluded that the school indeed had to close its Facebook Page, due to violations of cookie and data protection law. The court concluded that the data processing of user data by Facebook as a result of visiting a Page was not based on any legal ground, nor could it be based on consent from the users. In particular, because the data subjects were not sufficiently informed about the data collection and processing purposes that result from the visit to a Page.⁶ The court explicitly ruled that Facebook and the Page owner were joint controllers for the Page Insights and for the lack of adequate information.

In response to this ruling, the German State DPAs formed a Taskforce Facebook-Fanpages. They concluded on 18 March 2022 that Facebook and Page owners share responsibility to obtain consent from Page visitors for three tracking cookies: datr, c-user and fr from users, and datr from non-users.⁷ The German DPAs substantiate why Facebook does not obtain this consent. The German DPAs also insist on joint controllership for the collection and further processing by Facebook of Page visitor data, contrary to the ruling of the appellate administrative court. This will be discussed in more detail in Section 5 of this DPIA. On 23 March 2022 the data protection conference of State and Federal DPAs confirmed the conclusion that use of Pages violates data protection laws, and should be stopped, and decided to investigate and enforce compliance by public authorities.⁸

Questions Dutch parliament

As a result of questions asked by the Dutch Parliament about the use of Facebook Pages, the Minister of the Interior and Kingdom Relations (hereinafter: BZK)

⁴ Press release Norwegian DPA, Norwegian Data Protection Authority choose not to use Facebook, 22 September 2021, URL: <https://www.datatilsynet.no/en/news/2021/norwegian-data-protection-authority-choose-not-to-use-facebook/>

⁵ Law firm Schjodt, Memo on the Norwegian DPA's assessment of Facebook pages, June 2022, provided by Facebook to the Ministry of BZK on 5 July 2022.

⁶ The title of the press release from the appellate administrative court of Schleswig-Holstein is: *Wirtschaftsakademie ist wegen datenschutzrechtlicher Verstöße verpflichtet, Facebook-Fanpage zu deaktivieren*. 27 November 2021, URL: https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/OVG/Presse/PI_OVG/2021_10_27_Ausbaubeitrag_hat_Bestand_kopie.html. Text of ruling: Schleswig-Holsteinisches OVG, Urteil vom 25.11.2021 - 4 LB 20/13, URL: <https://openjur.de/u/2383902.html>.

⁷ Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook - Fanpages, 18 March 2022, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf

⁸ Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Zur Task Force Facebook-Fanpages vom 23. März 2022, URL: https://datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf. See also the FAQ of 22 June 2022 why use of Facebook Pages is problematic, URL: https://www.datenschutzkonferenz-online.de/media/oh/20220622_oh_10_FAQ_Facebook_Fanpages.pdf.

committed to investigate how the central government uses Facebook Pages, what the roles of parties are and what the contents are of agreements with Facebook. The Minister committed to use this information to assess whether a DPIA would need to be performed in order to evaluate whether additional measures were necessary.⁹ In April 2022 the State Secretary sent an update to the Dutch parliament.¹⁰ In the update the State Secretary explained it had ordered an independent company to conduct a DPIA *"because of recent developments, such as [the ban on Pages] of the German supervisory authority, and because of the high technical and legal complexity of this specific data processing."*¹¹

DPIA

Under the terms of the General Data Protection Regulation (GDPR), an organisation may be obliged to carry out a data protection impact assessment (DPIA) under certain circumstances, for instance where it involves large-scale processing of personal data. The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

A DPIA used to be called PIA, *privacy impact assessment*. According to the GDPR, a DPIA assesses the risks for the rights and freedoms of individuals. Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as for example freedom of expression.

The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains: *"This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity"*.

This DPIA follows the structure of the DPIA model mandatory for all Dutch government organisations.¹²

Because the data processing resulting from a visit to a government Page takes place for profiling purposes, on a large scale, and the data processing involves location data

⁹ Letter Minister BZK to the Lower House (in Dutch), 15 September 2021, URL:

<https://www.rijksoverheid.nl/documenten/kamerstukken/2021/09/15/kamerbrief-reactie-op-artikel-duitse-privacy-waakhond-regering-moet-facebookpaginas-sluiten>.

¹⁰ Letter Minister BZK to the Lower House (in Dutch), Voortgang reactie op NRC-artikel 'Duitse privacy-waakhond: regering moet Facebookpagina's sluiten', File 32 761, no. 221, 26 April 2022, URL:

https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022Z08424&did=2022D17028.

¹¹ Idem.

¹² *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (Revised model, 9 November 2021). For an explanation and examples (in Dutch) see:

<https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/verplichte-kwaliteitseisen/data-protection-impact-assessment>.

and data about the communication (be it content or metadata), and involves data that can be used to track the activities of visitors of Facebook Pages, it is mandatory for the Dutch government organisations to conduct a DPIA based on the criteria published by the Dutch data protection authority.¹³

This DPIA report has been written by the Dutch privacy consultancy firm Privacy Company.¹⁴

Scope of this DPIA

This DPIA report assesses the risks of personal data processing by Facebook and by the government organisation during the creation, the use and the maintenance of a Facebook Page by a Dutch government organisation. For this purpose, a specific test Page was created, of a non-existent Ministry of Privacy. The scope includes both registered users of a Facebook page, and visitors to a government Page that do not have a Facebook account (non-users).

The scope includes the collection of off platform data about non-users (with cookies) as these people may seek government information that is only available on Facebook, or inadvertently visit a public Facebook page as a result of a search query without having accepted Facebook's terms and conditions. This type of data processing is in scope because the data processing (with the cookie) originates from a visit to a government Page and is processing of personal data by persons visiting the Page.

The scope includes the generation and use of website analytics (the Insights from the Meta Business Suite). Facebook makes such statistics available to the Facebook Page-owner.

The scope includes the processing necessary for Facebook to show recommendations to visitors of the government Facebook Page, including recommendations created by Facebook's algorithms to rank content based on inferred preferences. This is in scope because the data processing occurs on a government page and is processing of personal data by persons visiting the page.

Because Facebook does not offer the possibility to create business accounts, the creation and maintenance of Facebook Pages of government organizations is often done using the private Facebook accounts of the employees of government organisations. For this reason the processing of personal data in relation to this (admin) use of the government Facebook page is within scope of this DPIA.

This report also assesses the legal (not technical) risks of unlawful US government access to personal data processed by Facebook as a result of the maintenance of, and visits to, the governmental Page.

¹³ Source: Dutch DPA, (information available in Dutch only), Wat zijn de criteria van de AP voor een verplichte DPIA? URL: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667>. Similar criteria (data processed on a large scale, systematic monitoring and data concerning vulnerable data subjects and observation of communication behaviour) are included in the guidelines on Data Protection Impact Assessment (DPIA), WP249 rev.01, from the data protection authorities in the EU, URL: http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236.

¹⁴ Privacy Company, URL: <https://www.privacycompany.eu/>

Outside the scope of this report

Technically only the data processing via the browser was tested, in Chrome on a MacBook: not via mobile apps, because this DPIA focusses on processing as a result of visits to a web Page. The scope does not include data processing by WhatsApp or Instagram.

The government guidelines on advertising stipulate that the use of 'custom audiences' and 'lookalike' audiences is not recommended, as this processing might pose unnecessary data protection risks for citizens. The standard, adopted by the Dutch central government, is to only advertise contextually, and non-personal data categories such as age, zip code, city of residence, sex and education (never on special categories of data). That is why the use of these two specific advertising options by Facebook is out of scope of this DPIA.¹⁵

In sum, the following elements are out of scope:

- Data processing via mobile Facebook apps¹⁶
- Facebook's advertising services, including 'custom audiences' and 'look a like' audiences.
- Data processing by WhatsApp and Instagram
- Data processing by third party apps or websites when a logged in Facebook user installs an app or visits a website through a hyperlink offered in the *News Feed*
- Facebook processing of personal data unrelated to the visits to a government Page

Methodology

Privacy Company applied five investigation methods:

1. Capturing screenshots of the contents shown on the test Page, the News Feed of the test users and recommendations from Facebook for friends and content.
2. Intercepting the outgoing network traffic from the test users
3. Accessing the Page analytics provided by Facebook
4. Downloading personal data relating to the test users made available by Facebook through Download Your Information
5. Filing Data Subject Access Requests for the three test users

This investigative method was chosen in order to establish the technical nature and extent of the data processing. Organisations cannot rely on legal assurances such as agreements when they assess their role and ensuing responsibilities for the processing, including the data protection risks. A very common risk is a loss of control because the processor or controller agreement is incomplete, and omits to mention the existence of diagnostic data processing, or omits to mention essential purposes of the processing. Another common risk is a unlawful further processing, if an organisation thinks it engages a party as a data processor, but it follows from the

¹⁵ Ministerie van Algemene Zaken, Dienst Publiek en Communicatie, Richtlijnen voor privacyproof en effectief campagne voeren, (Guidelines for privacy proof and effective campaigning), 25 May 2018.

¹⁶ Inclusion in the scope would have required extensive testing, technically complex traffic interception and analysis, and would not meaningfully change the main findings related to the legitimacy for government organisations to use a Facebook Page.

technical investigation that the party factually has to be qualified as independent or joint data controller.¹⁷

Privacy Company performed the analysis on a MacOS version 10.15.7, with Chrome browser 98.0.4758.102, between 27 February 2022 and 30 March 2022, with separate tests relating to the cookies set in the browsers of non-users on 30 June 2022.

Every working day an automated test run was performed with a clean browser. The test run lasted approx. 15 minutes every day, in which each of the three test accounts visited and interacted with the test Page of the Ministry of Privacy.

Two of the three test accounts were brand new, created for the purpose of this DPIA by individual Privacy Company employees (Sjoera and Winfried). The third account was an existing account that acted as the system administrator of the Page (Floor). Hereinafter the three test users are named A for Floor, B for Sjoera and C for Winfried.

Activities on Facebook

- The two new accounts B and C only befriended each other, and the existing account A.
- Account B followed 17 leaders of the 20 political parties elected in the Lower House in the Netherlands.¹⁸ Some party leaders did not have public Pages, or had reached the limit of followers. This scenario was chosen to prevent a political bias in the content shown to the test user, and to compare this with the content selected by Facebook to show to the user. Account B also followed/liked two Dutch ministries (BZK, Buitenlandse Zaken and OCW), as well as four public institutions (RIVM, KNMI, NPO Politiek and ProDemos).
- Account C followed public persons and Pages from organisations with a known LHTBI-background, as well as a government organisation with a distinct profile, the Ministry of Defence. This profile was chosen to see if these two distinct interests would be reflected in the contents shown to the user.
- Accounts B and C liked and interacted with content items on the test Page.
- Accounts B and C incidentally followed Pages suggested by Facebook as 'Suggested for you' or 'Similar Pages' (in a banner on top of a Page) or as 'Recommended Pages' (in a banner in the user's News Feed).
- All three test accounts interacted with general timeline content like posts, ads and video's.
- All three test accounts used Facebook Chat to share and comment on posts made in the Page.

Privacy Company ensured that the research is reproducible and repeatable. This was achieved by limiting the number of actions. There was a pause of approx. 30 seconds

¹⁷ See for example EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, 7 July 2021, URL:

[https://edpb.europa.eu/system/files/2021-](https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf)

[07/eppb_guidelines_202007_controllerprocessor_final_en.pdf](https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf). See for example par. 21:

"Having said that the concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis."

¹⁸ Liane den Haan, Laurens Dassen, Kees van der Staaij, Lilian Marijnissen, Geert Wilders, Esther Ouweland, Lilianne Ploumen, Pieter Omzigt, Nilüfer Gündoğan, Wybren van Haga, Joost Eerdmans, Jesse Klaver, Thierry Baudet, Farid Azarkan, Gert-Jan Segers and Sylvana Simons.

between each action. Screenshots were made automatically every 10 seconds, capturing all actions. All data were recorded. The observed network termination points and the captured data are summarised in Section 2.2 of this report.

Privacy friendly settings in the browser

The default configuration of the Chrome test browser was changed with the purpose to eliminate any traffic to Google as a result of cloud functionality of the browser. Chrome also had to be configured to accept the use of mitmproxy. To this end the settings were used from the *chromedp* library.¹⁹ Changes to Chrome's default configuration are listed in Appendix 1 of this DPIA.

Data subject access requests

As part of the methodology to understand the data processing, the researchers at Privacy Company filed data subject access requests, both directly, as data subjects of test accounts B and C that visited the test Page, and indirectly, by filing a data subject access request with the system administrator of the Ministry of Privacy Page (test account A). The outcomes are discussed in Section 2.5 of this report.

Replies Facebook

Facebook has twice provided a written view on the DPIA. Per letter of 29 September 2022 Facebook has provided its view on part A of the DPIA, shared 24 August 2022. On 11 November 2022, Facebook provided a view on the completed report. This second view is summarised in Appendix 1 included in this DPIA, with a reply from Privacy Company.

Facebook's letters are both marked CONFIDENTIAL / CONTAINS META PLATFORMS IRELAND LTD TRADE AND BUSINESS SECRETS. Therefore, none of Facebook's literal input can be included in the DPIA. Very high over, Facebook's reply on the facts in part A can be summarised as follows.

Facebook has provided legal opinions about for example the location of the responsible Facebook entities, about the scope of the DPIA, and about joint controllership. In the latter point, Facebook quotes from the 2021 German appellate administrative court ruling described above. As this ruling is public, Facebook's arguments in that case are used to reflect Facebook's views. Facebook concludes from this ruling that Facebook and the fan page operator are only joint controllers for the creation of the statistics, but not for the storage of the link between fan page visits and the data of a Facebook member in profiles and their use for advertising purposes. Facebook quotes the German appellate court that there is no joint decision on the purpose of the data processing. Facebook also quotes that the court that the data processing is not carried out in the interest of the plaintiff, and does not offer any advantages to the plaintiff. Therefore, there would not be any objective connecting factors for the assumption of an at least tacit joint decision by the fan page owner.

This line of arguing was already included in Section 5 of this DPIA, but has been expanded with a reply refuting this argument, on the foot of the decisions of the German Federal and State DPAs.

Facebook's arguments do not change the conclusion of this DPIA that Facebook and the Dutch government organisations that open a Page, must factually be qualified as joint controllers for all the data processing related to visits to a government Page, by

¹⁹ <https://github.com/chromedp/chromedp>

users and by non-users. However, subsidiarily, this DPIA also argues that if the government organisation with a Page is not a joint controller, Facebook has to be qualified as an independent third party. That means the government organisation has to have a legal ground for the transfer of personal data to a third party. Section 11.2 of the DPIA concludes that this 'further processing' by Facebook, for Facebook's own commercial purposes, is incompatible with the purpose for which a government organisation allows Facebook to initially collect the personal data of Page visitors: to technically facilitate the communication with a mass audience, and to create website analytics (Page Insights). The analysis in Section 11.1 is supplemented with some additional arguments from the German DPAs why Facebook cannot rely on any legal ground for its current data processing.

Facebook also points to alleged factual errors, and asks for a more detailed explanation of some findings. Where necessary, some descriptions have been removed, and some explanations have been expanded.

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).²⁰ This model uses a structure of four main sections, which are reflected here as "parts".

- A. Description of the factual data processing
- B. Assessment of the lawfulness of the data processing
- C. Assessment of the risks for data subjects
- D. Description of mitigating measures

Part A explains the data processing resulting from the visits to the Facebook test Page. This starts with a description of the technical way Facebook collects personal data and how some data are shown to the government Page administrator. This section describes the categories of personal data and data subjects that may be affected by the processing, the purposes of the data processing, the different roles of the parties, the different interests related to this processing, the locations where the data are stored and the retention periods.

Part B provides an assessment (by Privacy Company, with input from BZK) of the lawfulness of the data processing. This analysis starts with an analysis of the legal grounds for the processing in relation to the legal qualification of the roles of Facebook as provider of the Page service, and the Dutch government organisation as the party providing the content on the Page. Subsequently, conformity with the key principles of data processing is assessed, including transparency, data minimisation, purpose limitation, as well as the necessity and proportionality of the processing. In this section the legitimacy of the transfer of personal data to countries outside of the EEA is separately addressed, as well as how the rights of the data subjects are respected.

In Part C the risks for data subjects are assessed, as caused by the processing activities related to the collection of data related to the visits to the government Facebook Page, but also related to the risks of undue access to the personal data by US government services.

²⁰ The Model Data Protection Impact Assessment federal Dutch government (PIA). For an explanation and examples (in Dutch) see: <https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia>

Part D assesses the measures that can be taken by either Facebook and the individual government organisations that operate a Page to further mitigate the risks as well as their impact.

Part A. Description of the data processing

This first part of the DPIA provides a description of the characteristics of the personal data processing by Facebook as a result of the creation and maintenance of a government Facebook Page.

This section continues with a description of the personal data Facebook processes, the categories of data subjects that may be affected by the processing, the locations where data may be stored, processed and analysed, the purposes of the data processing as provided by Facebook and the roles of the government organisations as (joint) data controllers with Facebook. This section also provides an overview of the different interests related to this processing, and of the retention periods.

1. The processing of personal data

This section provides an overview of the technical scope of the processing of personal data.

Facebook generates and processes three types of personal data: Content Data, User Activity Data and Inferred Data. The descriptions below are limited to the data processing related to the visits to a government Facebook page by the three test users.

1. **Content Data** are data actively provided or published by Facebook users, as well as advertisements and sponsored posts shown by Facebook to a specific user. Facebook users interact with Content Data on a government Facebook Page in three roles: as visitor to the Page, as administrator of the Page, or as person mentioned in a posting on the Page.
2. **User Activity Data** are the data generated, observed and (further) processed by Facebook as a result of the creation of the government Page, and the interactions with the Page by visitors. These personal data can be subdivided in three subcategories:
 1. User activity on Facebook;
 2. User activity outside of Facebook collected with the help of cookies set by the government Page;
 3. Data collected from non-users when they visit a government Page.Facebook's processing of data in these subcategories is discussed in more detail below, in Sections 1.2.1, 1.2.2 and 1.2.4.
3. **Inferred Data** are the predictions Facebook makes about the interests of a user, to decide what Content Data it shows to the user (what Post comes on top of the *News Feed*, what related Pages or Groups or friends are recommended, and what personalised advertisements are shown). Facebook's processing of data in this subcategory is discussed in Section 1.2.3 below, to the extent related to the visit to a government Facebook page by the three test users.

This section starts with a brief description of the company owning the social network, where it is located, its market share in the Netherlands, and how it earns revenue with targeted advertising. This section continues with a more detailed description of Facebook's processing of User Activity Data and Inferred Data, and describes how Facebook is technically able to personalise the content shown to each end user.

1.1 About Facebook/Meta

The US American company Meta Platforms Inc. (called Facebook in this report when the report refers to the data processing by the social platform) explains it has more than 3 billion users that share 140+ billion messages a day.²¹ Meta had over 77,800 full-time employees worldwide at the end of the first quarter of 2022.²²

1.1.1 *Establishment and applicable law*

Facebook has offices in over 80 cities worldwide, including an office in Amsterdam.²³ Facebook has its headquarters in the USA, but for data processing purposes, Facebook has a lead establishment in Ireland, Facebook Ireland Limited. Facebook Ireland [official name Meta Platforms Ireland Limited] is the data controller for the data processing of Dutch users.

The Dutch DPA (Autoriteit Persoonsgegevens) is competent to provide advice in a prior consultation as defined in Article 36 of the GDPR, or provide advice following Article 58(3) of the GDPR. However, in practice, the Dutch DPA will refer requests or complaints to the lead supervisory authority for Facebook, the Irish Data Protection Commissioner, hereinafter: Irish DPC.

1.1.2 *Revenue and reach in the Netherlands*

In a financial report about the first quarter of 2022 Facebook reports that it had almost 2 billion daily active users worldwide, and almost 3 billion monthly active users.²⁴

According to its annual financial report over 2021 (Form 10-K), Meta generated a total revenue of 115,6 billion USD in the fiscal year 2021, resulting in a net income of 39,7 billion USD.²⁵ Almost all revenue was earned by advertising (114,9 billion USD). Facebook explains that its advertising revenue increased with 30+ billion USD, or 37%, compared to 2020, as a result of increases in both the average price per ad and the number of ads delivered.²⁶

These financial results include the earnings from WhatsApp, Messenger and Instagram. Meta calls these 'Family of Apps (FOA)'. These results exclude the earnings from Reality Labs.

In the first quarter of 2022 Meta generated a global revenue of 27,9 billion USD with Facebook and its other apps (almost 27 billion USD from advertising), resulting in a net income of almost 7,5 billion USD.

²¹ Meta Platforms Inc., Company Info, last visited 28 June 2022, URL: <https://about.facebook.com/company-info/>.

²² Infotechlead, Facebook parent Meta expects slowdown in jobs, freezes hiring, 5 May 2022, URL: <https://infotechlead.com/digital/facebook-parent-meta-aims-at-slowing-growth-in-number-of-employees-72376>

²³ Meta Platforms Inc., Company Info, last visited 28 June 2022

²⁴ Meta, Meta Reports First Quarter 2022 Results, 27 April 2022, URL: <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-First-Quarter-2022-Results/default.aspx>.

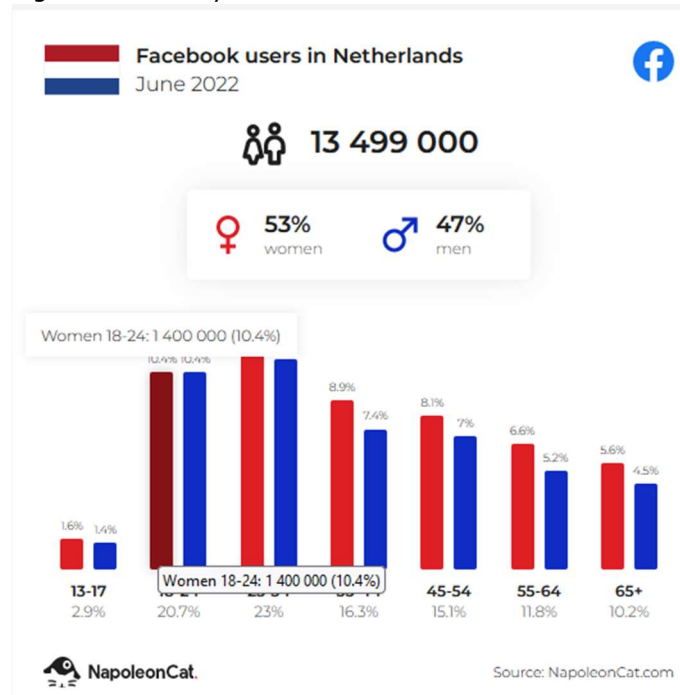
²⁵ Meta Platforms Inc, Form 10-K filed with the United States Securities And Exchange Commission, 3 February 2022, URL: <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf>.

²⁶ Idem, p. 65.

Meta performs a calculation of the combined Facebook and Messenger revenue per user per global region, based on the total revenue in a given geography during a given quarter, divided by the average of Facebook and Messenger Monthly Active Users (MAUs) in the geography at the beginning and end of the quarter. These metrics show that in the year 2021, Facebook earned a quarter of its revenue (over 29 billion USD) from European users, with an average earning of almost 20 USD per European user at the end of the year.²⁷

Meta writes: “We generate substantially all of our revenue from advertising. Our advertising revenue is generated by displaying ad products on Facebook, Instagram, Messenger, and third-party affiliated websites or mobile applications. Marketers pay for ad products either directly or through their relationships with advertising agencies or resellers, based on the number of impressions delivered or the number of actions, such as clicks, taken by users.”²⁸

Figure 1: Monthly active Facebook users in the Netherlands in June 2022²⁹



For Dutch government organisations, the use of Facebook is attractive because the service reaches between 10.3³⁰ and 13.6 million Dutch users³¹, on a total population

²⁷ Idem, p. 58.

²⁸ Idem, p. 63.

²⁹ Source: NapoleonCat, based on Facebook’s marketing API about the total available audience in the Netherlands.

³⁰ The estimate of 10.3 million Dutch users in 2022 comes from the Dutch marketing research organisation Marketingfacts, based on its Nationale Social Media Onderzoek 2022 (National Social Media Survey 2022), URL: <https://www.marketingfacts.nl/berichten/social-media-in-nederland-2022/>.

³¹ The high estimate of 13.6 million Dutch users in 2022 comes from Statista. *In March 2022, around 13.6 million people in the Netherlands used Meta’s Facebook, a number that makes up*

of 17,742 million, of which 15.287 million are aged 13 and older (24 August 2022).³² This means Facebook reaches between 67% and 89% of Dutch inhabitants aged 13 and older. This reach would even be higher if users were counted younger than 13 years. They are excluded because formally they are not allowed to open a Facebook account.³³

There are no recent separate public statistics about the average amount of time Dutch users spend on Facebook on a daily basis, but there is a number for time spent on all social media platforms together based on the Dutch National Social Media Survey 2022. On average Dutch people spend 107 minutes a day on social media, with an even higher reported figure of 138 minutes a day for young adults (20-39 years).³⁴

According to highlights from surveys published by Statista, Facebook remains the most widely used network, with a slight majority of female users. 25% of the Facebook users belongs to the age group of the so called Millennials (between 25 and 34 years)³⁵, while only 12,5% of the Dutch population belongs to this age group. Statista predicts a continued usage growth of Facebook through to 2025, when Facebook is expected to be used by 62 percent of the Dutch population and Dutch advertisers are predicted to spend 262 million USD on mobile advertising.

The Dutch marketing organisation is less optimistic about Facebook's reach: they highlight that less than 20% of children/young people in the Netherlands uses Facebook, and that a decrease is visible in the age group 20-29 year old. The daily Facebook use in that age group decreased from 60 to 48% in 2022.³⁶

1.1.3 Personalised content

Every user on Facebook has an individual profile, with a *News Feed* (sometimes abbreviated by Facebook to 'Feed').³⁷ The content shown on this profile is personalised, and generated *on the fly* by Facebook, based on what Facebook describes as "*hundreds of pieces of information from the social graph. Users see News Feed stories; comments, likes, and shares for those stories; photos and check-ins from their friends — the list goes on.*"³⁸

around 78.8 percent of the country's population. Statista, Netherlands monthly number of Facebook users 2018-2022, URL: <https://www.statista.com/statistics/1058680/monthly-number-of-facebook-users-in-the-netherlands/> .

³² CBS, Bevolkingsteller, real time prognosis of the Dutch population on 24 August 2022, URL: <https://www.cbs.nl/nl-nl/visualisaties/dashboard-bevolking/bevolkingsteller> . The amount of inhabitants aged 13 and older is based on statistics from 1 January 2022.

³³ CBS Statline, Bevolking op eerste van de maand; geslacht, leeftijd, migratieachtergrond Last updated 30 June 2022, <https://opendata.cbs.nl/#/CBS/nl/dataset/83482NED/table?ts=1658229073739>.

³⁴ [Marketingfacts, Social media in Nederland 2022](#), see footnote 24.

³⁵ Statista, Total number of users of Facebook in the Netherlands from 2013 to 2021 in millions, 28 April 2022, URL: <https://www.statista.com/statistics/880850/number-of-facebook-users-in-the-netherlands/>

³⁶ Marketingfacts, Social media in Nederland 2022.

³⁷ Facebook, What's the difference between a profile, Page and group on Facebook?, URL: <https://www.facebook.com/help/337881706729661>.

³⁸ Facebook, TAO: The power of the graph, 25 June 2013, URL: <https://engineering.fb.com/2013/06/25/core-data/tao-the-power-of-the-graph/>

This section describes five types of content personalisation relevant for this DPIA:

1. Postings shown in the News Feed from people or organisations the user has chosen to follow
2. Postings shown in the News Feed based on Facebook's algorithmic recommendations
3. Advertisements shown as 'related' or 'recommended' pages' when visiting another Page, or as 'Discovery' in the profile of the user
4. Advertisements shown as 'sponsored' posts or videos in the News Feed of users
5. Advertisements shown as 'sponsored' in the top right corner of the user profile

The content shown in the News Feed can include postings from (government) Pages people follow, as well as profiles from friends, but also from people or organisations the user does not know or follow. Facebook explained how the second category works:

"Our recommendations help users discover new and relevant content. For example, we suggest posts in their News Feed from Pages and Groups that they don't already follow, but we think they may be interested in. Several factors influence their suggested posts in News Feed such as:

- *Related engagement: A post may be suggested for users if other people who interacted with the post also previously interacted with the same group, Page or post as they did.*
- *Related topics: If they've recently engaged with a certain topic on Facebook, we may suggest other posts that are related to that topic. For example, if users recently liked or commented on a post from a basketball Page, we could suggest other posts about basketball.*
- *Location: Users may see a suggested post based on where they are and what people near them are interacting with on Facebook."*³⁹

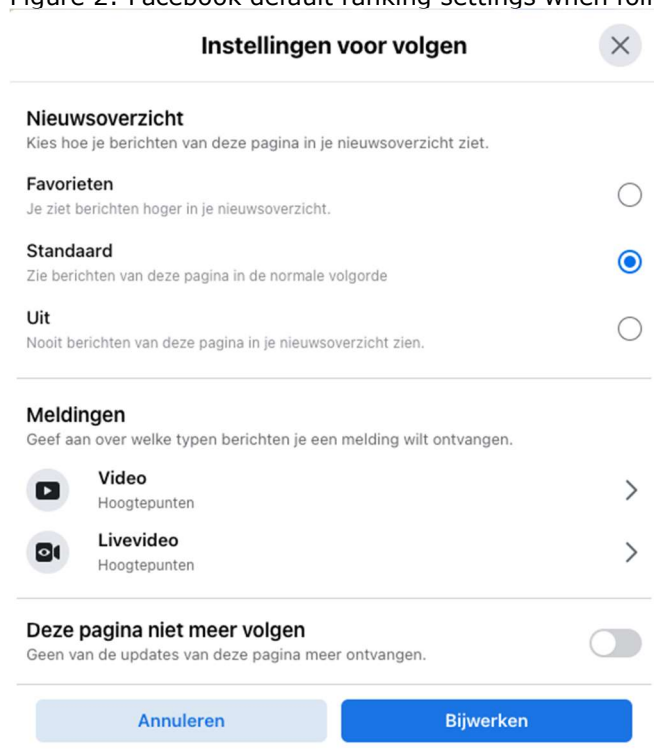
Facebook also told Privacy Company and the ministry of the Interior that users would be able to see why Facebook recommends content. However, Facebook's interfaces only allow users to mute, increase or report postings/videos from a certain source, without any possibility for users to find out why certain posting are shown to them in the *News Feed*.⁴⁰ See [Figure 7](#), two pages below.

As described in the Introduction, the test users had distinct profiles. When following a person or Page, the two new test users B and C always selected Facebook's default options, to see posts from a followed Page in the 'standard' ranking.

³⁹ Facebook Netherlands mail to the Ministry of the Interior, 20 June 2022.

⁴⁰ On 22 June 2022 Facebook wrote: "To help users understand why they may have been recommended content, users can use the "Why am I seeing this?" feature on Feed to get more context."

Figure 2: Facebook default ranking settings when following a Page



Instellingen voor volgen

Nieuwsoverzicht
Kies hoe je berichten van deze pagina in je nieuwsoverzicht ziet.

Favorieten ☐
Je ziet berichten hoger in je nieuwsoverzicht.

Standaard ☒
Zie berichten van deze pagina in de normale volgorde

Uit ☐
Nooit berichten van deze pagina in je nieuwsoverzicht zien.

Meldingen
Geef aan over welke typen berichten je een melding wilt ontvangen.

Video ☐ **Hoogtepunten** >

Livevideo ☐ **Hoogtepunten** >

Deze pagina niet meer volgen ☐
Geen van de updates van deze pagina meer ontvangen.

Annuleren **Bijwerken**

Personalised postings

How this personalisation works in practice is illustrated with screenshots from the test Page of the Ministry of Privacy. [Figure 3 below](#) is an example of the first category of personalisation. It shows a posting from the Ministry of Privacy test page in the news feed of one of the test users. Both test users followed this Ministry of Privacy page, and (following the government policy) the Ministry of Privacy did not engage in any type of advertising or other paid promotion of its postings to users. Hence the appearance of this posting in the News Feed is a direct result of the conscious action by both users to follow this Page.

An example of the second category, postings selected by Facebook's algorithms, is shown in [Figure 4 below](#). User B did not follow this Page from a radical anti-covid vaccination organisation, but based on the inferred interests of the user, Facebook injected this post in the News Feed. More examples of such radical anti-government content are shown in [Figure 5](#) and [Figure 6](#). These postings were a result of following a Page recommended by Facebook.

Figure 3: Posting from the Ministry of Privacy in the News Feed of test user C

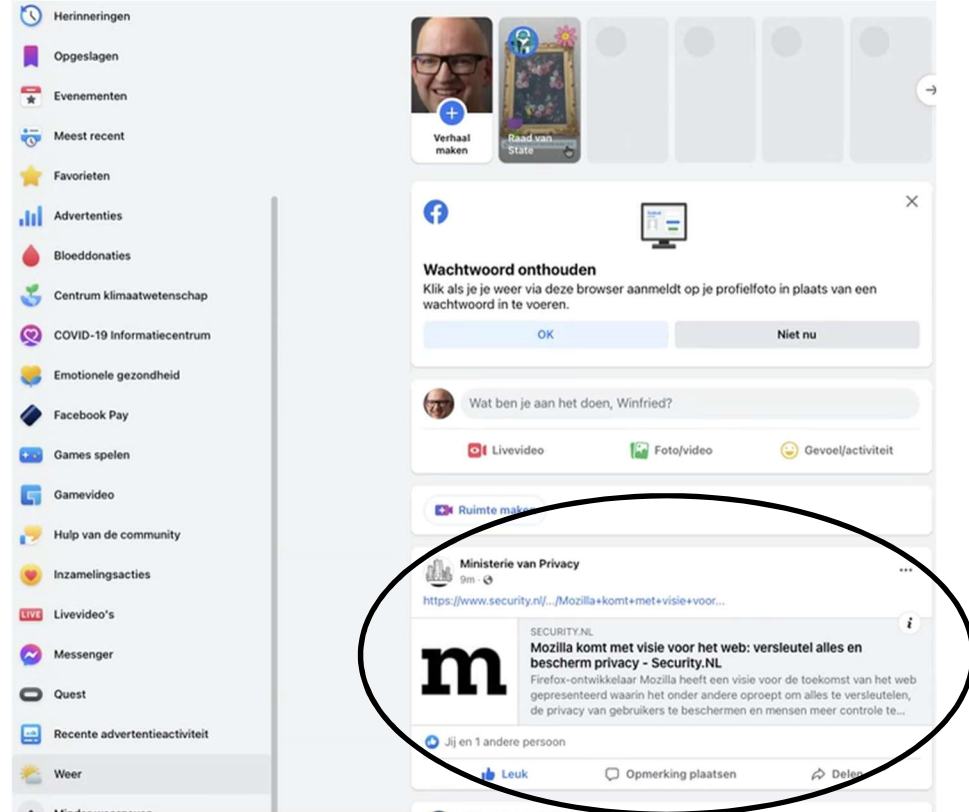
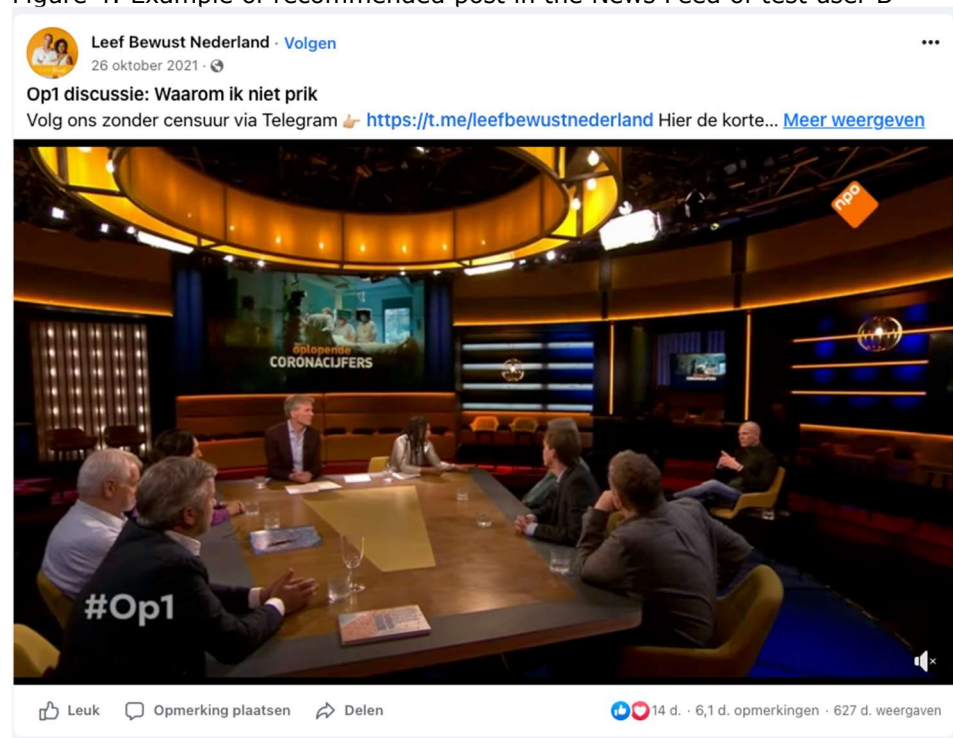


Figure 4: Example of recommended post in the News Feed of test user B⁴¹



⁴¹ Screenshot no. 1292 of test user B, captured on 25 March 2022.

Following a recommendation from Facebook to follow Pages (discussed below, under advertisements), test user B liked a specific Page, without knowing what the contents of this Page would be.

Following this Hotspot Page resulted in the prominent appearance in the News Feed of test user B of a number of anti-government anti-vaccination posts. See [Figure 5](#) and [Figure 6](#) below. In total 6 messages from this organisation were shown to the test user. The posting states that if a government makes vaccination mandatory it can equally make sterilisation, euthanasia and organ donation mandatory. As mentioned in the Introduction, the profile of the test user was designed to be politically neutral. However, the content of recommended postings showed an increasing bias towards anti-government content.

Figure 5: Anti-government Covid posting in the News Feed⁴²



Facebook did not offer any explanation why these specific posting were ranked to be shown in the first results of the News Feed. When the user clicked on the three dots on the right top of the posting, Facebook offered intervention options, to save the Post, Hide it, unfollow a person or organisation, or report a post to Facebook, but no

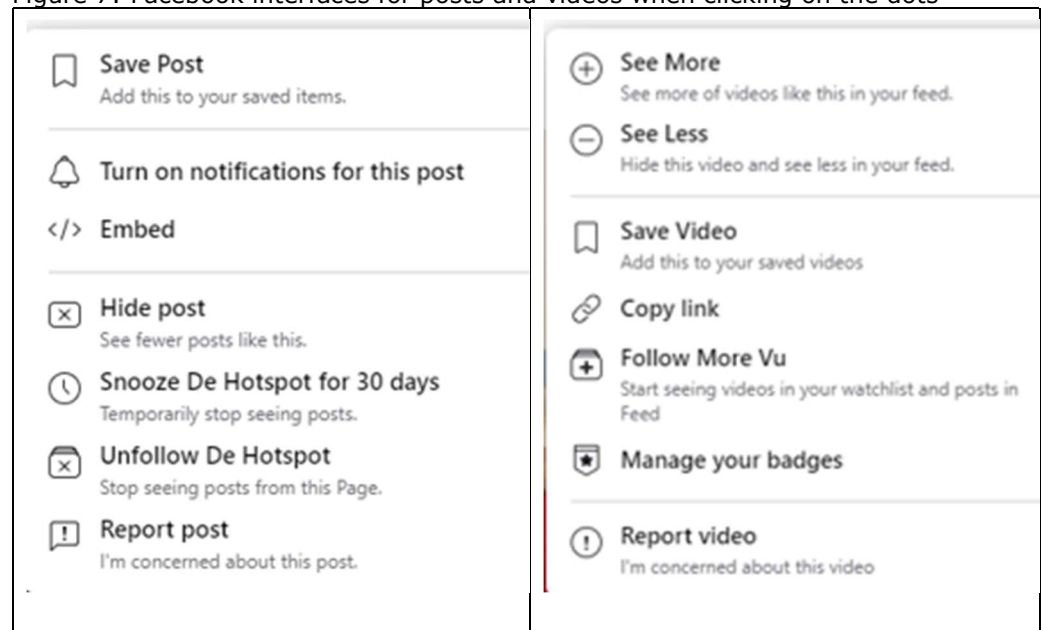
42

access to the logic. Facebook itself does not describe any other options in its explanation why a user sees content in their News Feed.⁴³

Figure 6: Another posting from the same source shown in the News Feed.⁴⁴



Figure 7: Facebook interfaces for posts and videos when clicking on the dots



⁴³ Facebook, Why do I see suggested content in my Facebook Feed? URL: <https://www.facebook.com/help/485502912850153>

⁴⁴ Screenshot made 25 March 2022 in the News Feed of test user B, no. 1192.

In total, test user B followed 25 Pages. Though the News Feed did contain messages from the followed politicians and public sector organisations, the amount of anti-government content messages stood out in comparison to other neutral postings.

Advertisements

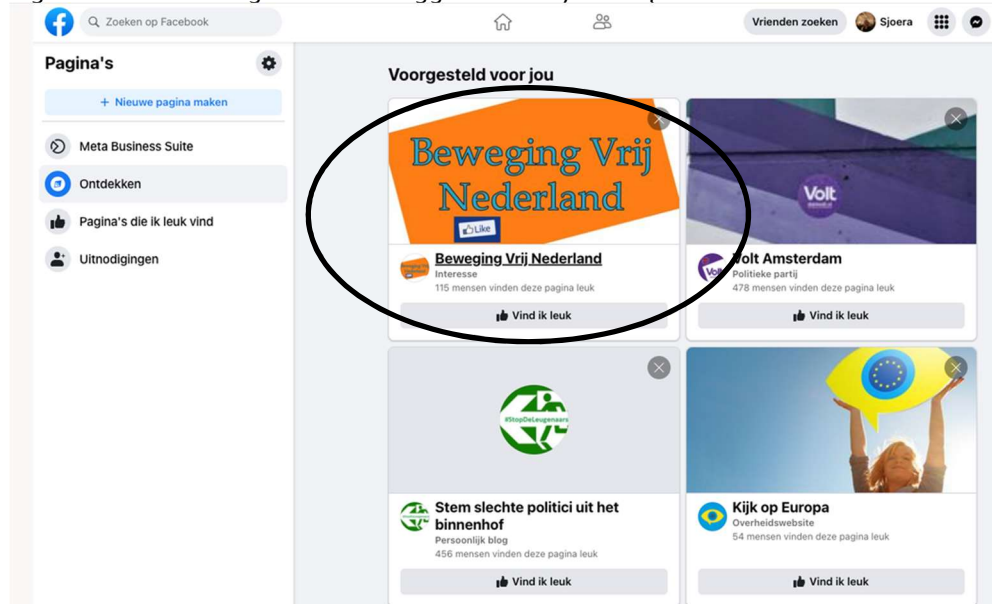
As described above, Facebook shows advertisements in three different ways:

1. Advertisements shown as 'related' or 'recommended' pages' when visiting another Page, or as 'Discovery' in the profile of the user
2. Advertisements shown as 'sponsored' posts or videos in the News Feed of users
3. Advertisements shown as 'sponsored' in the top right corner of the user profile

A few days before test user B was shown the recommended post from the anti-covid vaccination organisation (shown in [Figure 4](#) above), this same radical organisation was proposed as Page to follow to the user in Facebook's general Page recommendations in the profile of user B. Test user B clicked on this Page, but did not follow. Nonetheless, Facebook inferred an interest and inserted a post from this organisation in the News Feed of the user.

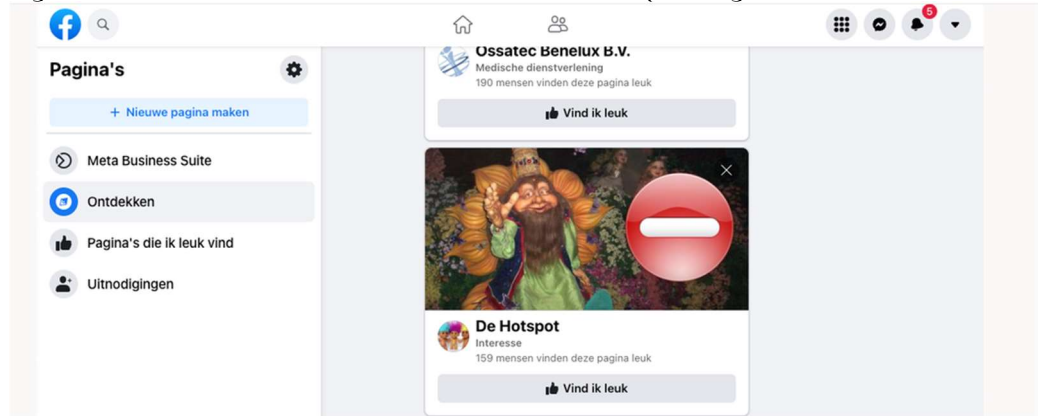
Facebook offers a separate interface to users with a list of recommended Pages, as shown in [Figure 8](#) below. The no. 1 recommendation was an anti-covid-vaccination conspiracy Page. Facebook does not offer any hyperlinks to information (such as the three dots) why this information was recommended to the user.

Figure 8: Radical organisation 'suggested for you' in profile of test user B⁴⁵



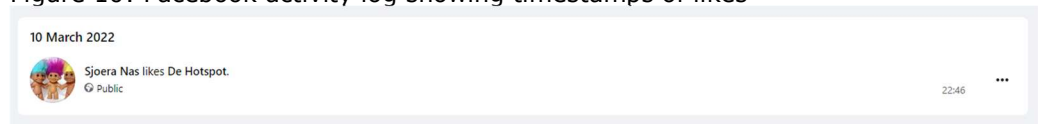
Another Page recommended by Facebook in the overview of 'Discover Pages', was the Page called Hotspot described above. The test user followed this Page, thinking it was related to an entertainment park called Efteling (due to the picture of a gnome).

⁴⁵ Screenshot no. 968 of test user B, captured on 23 March 2022.

Figure 9: Facebook recommendation to like 'De Hotspot' Page⁴⁶

The liking of this Page is reflected in the activity log of the user, as shown in [Figure 10](#) below.

Figure 10: Facebook activity log showing timestamps of likes



Other ways in which Facebook advertises other Pages are shown in [Figure 11](#) and [Figure 12](#) below. In the test scenario test user B followed the Page of the Dutch Ministry of the Interior and Kingdom Relations and the Page of the Dutch Ministry of Education. As shown in on both Pages a horizontal bar was shown to this test user with recommendations for other content. This content was only partially related to the content on the ministerial Page: both recommended 'related' Pages contained completely unrelated commercial content Pages, related to construction wood and auctions. Facebook does not provide an interface to users to be informed why these pages were recommended to them by Facebook. The admin of the government Page does not have access either, and cannot influence these contents. It appears Facebook has made changes to its interface after completion of this research, and no longer shows these banners.

In the banner 'Voorgesteld voor jou' Facebook does not show the three dots or other interface to explain the logic behind these recommendations. Facebook does show these three dots in the second banner of 'Related Pages'. However, when clicking on this interface, Facebook only offers the option to save, hide, or snooze the suggestion, not any explanation about the logic.

⁴⁶ Shown to test user B on 10 March 2022, screenshot no. 892.

Figure 11: Related pages shown on the Page of the Ministry of the Interior⁴⁷

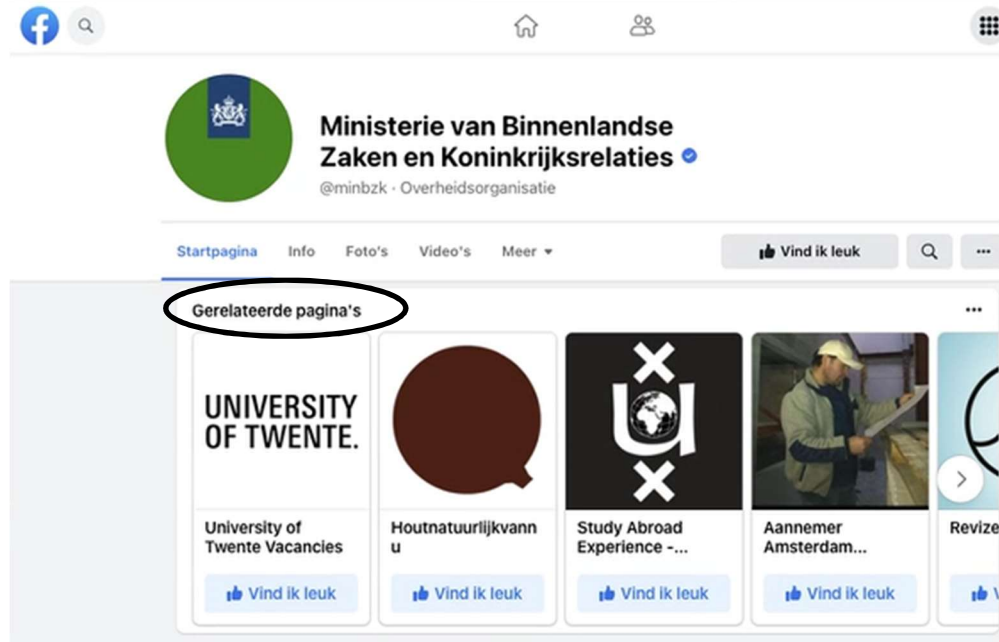
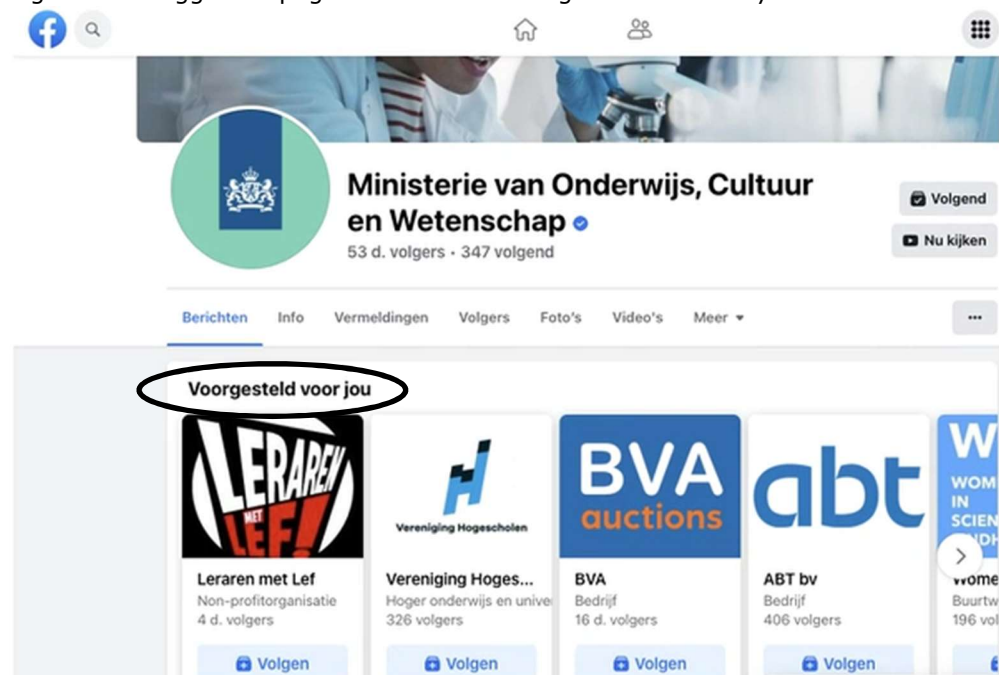


Figure 12: Suggested pages shown on the Page of the Ministry of the Education⁴⁸

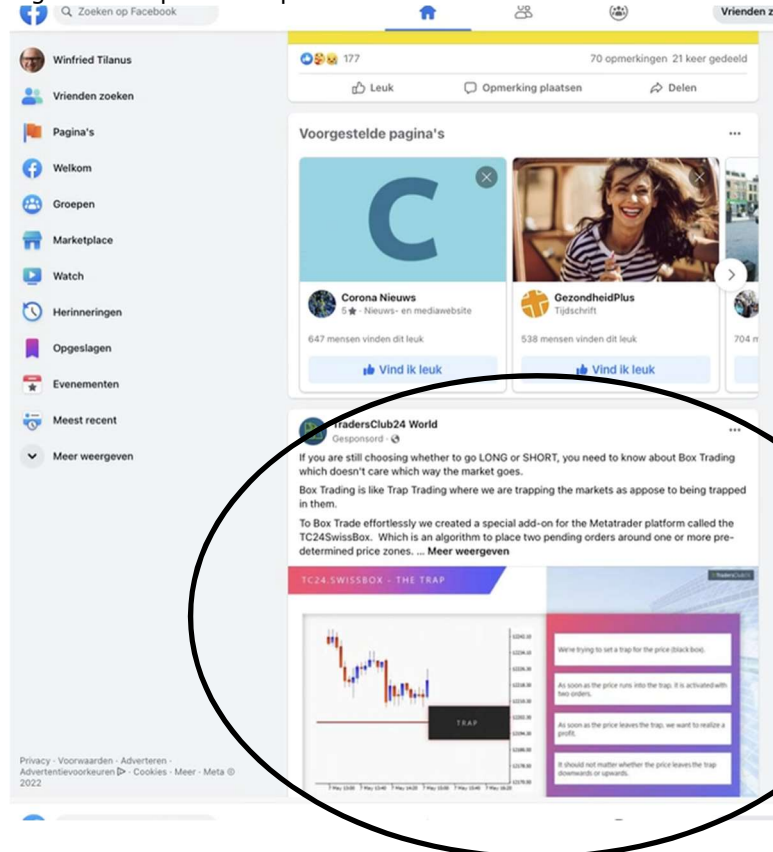


Facebook also shows advertisements as 'sponsored' posts or videos in the News Feed of users. See [Figure 13](#) below.

⁴⁷ Test user B, screenshot made on 1 March 2022

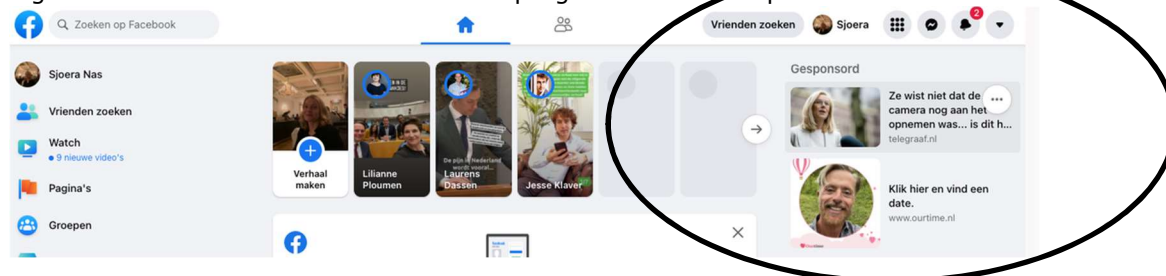
⁴⁸ Test user B, screenshot made on 1 March 2022.

Figure 13: Sponsored post in the News Feed of test user C for investment platform



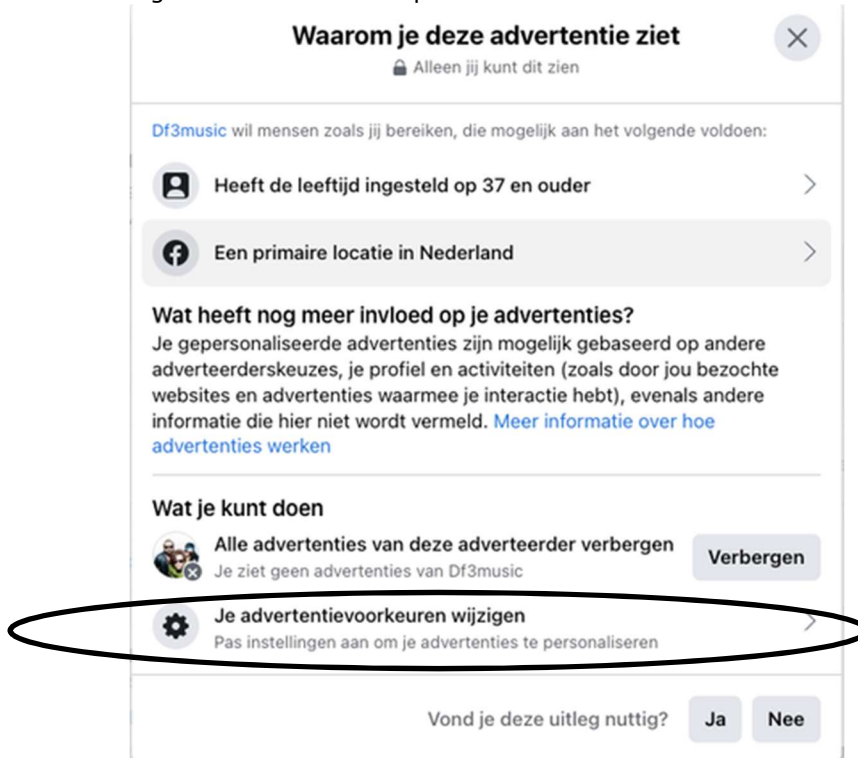
Facebook also uses information about user behaviour and interactions with content to show personalised advertisements in the top right corner of the user profile. See [Figure 14](#) below.

Figure 14: Advertisement shown in the top right corner of the profile



The ad shows a picture of minister Kaag, with the text 'She didn't know the camera was still recording... is this...', and a reference to Dutch newspaper Telegraaf. At first sight, this could be related to a privacy topic, and inferred from the user's interest in the Ministry of Privacy. However, when the ad was selected (by hovering over the ad, the user can see the three dots), as shown in [Figure 15](#) below, Facebook provided two generic explanations: age above 37 and primary location in the Netherlands. Facebook does not provide a more detailed explanation, but only refers to a generic information page how Facebook shows ads.

Figure 15: Facebook explanation about this advertisement



Facebook explains that the ads may be based on other advertiser choices, the user profile and activities such as websites visited outside of Facebook, “as well as other information not listed here”.⁴⁹

Figure 16: Facebook generic explanation to users why ads are shown



⁴⁹ Facebook explanation provided in the pop-up ‘Why you’re seeing this ad’.

If a user clicks on the option to 'change ad preferences', Facebook opens a generic information page, with a generic explanation what types of personal data it may use to select ads.

When the user clicked on the top ad shown in [Figure 14](#), a page from clothes store Zara was shown. See [Figure 17](#) below. This was reported to Facebook as misleading content. During the test, the users were seldom shown ads from known/renowned companies or organisations. Most of the ads lead to websites about bitcoin scams, including ads that claimed to be about Tesla cars.

Figure 17: Misleading content of ad shown to test user B

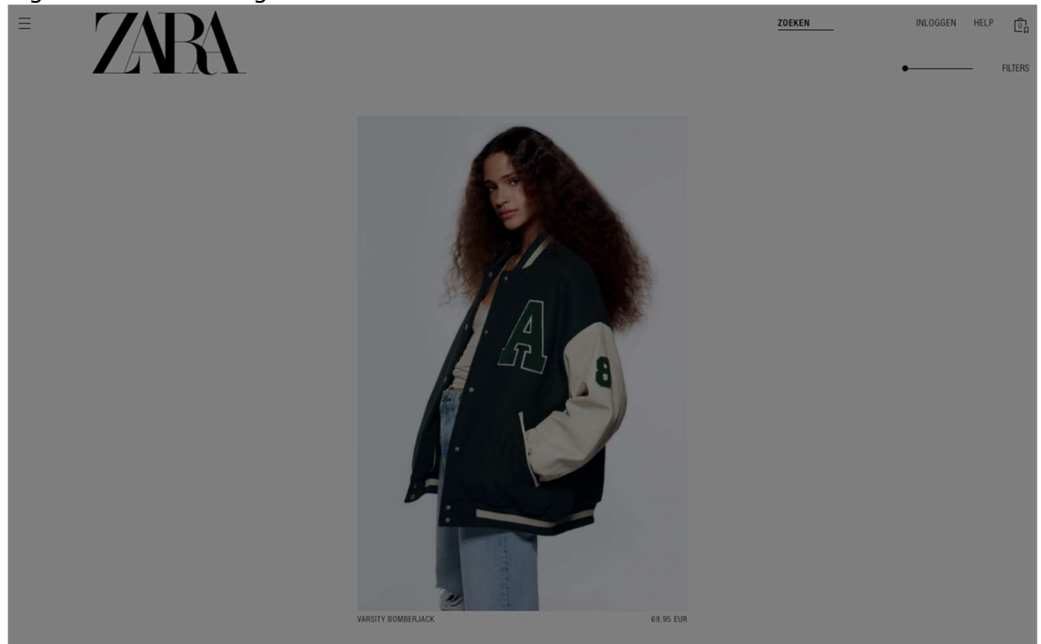
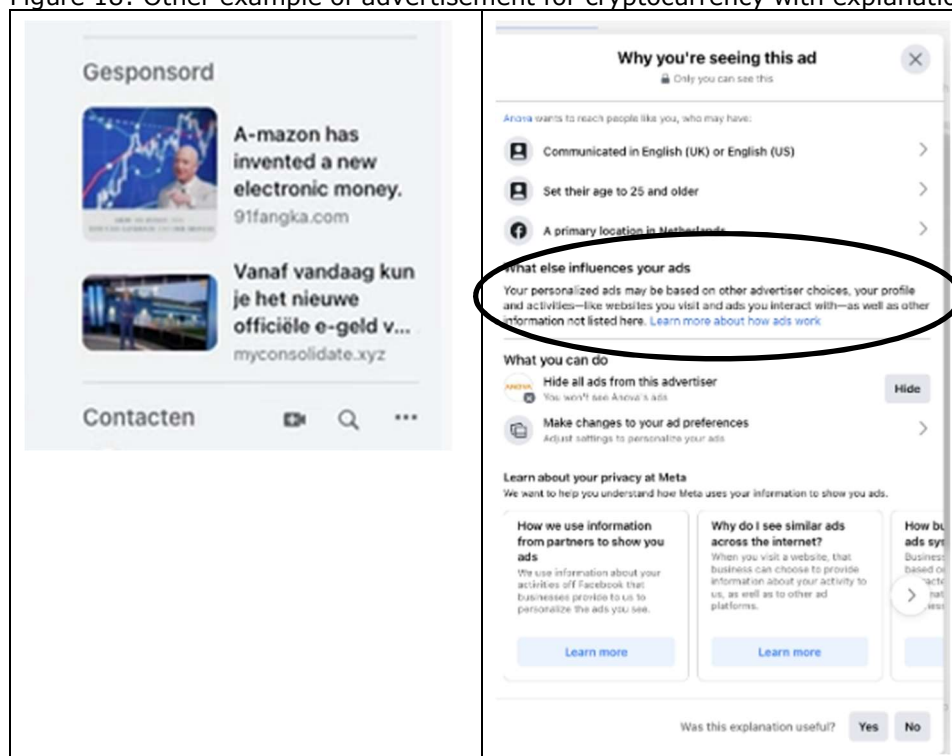


Figure 18: Other example of advertisement for cryptocurrency with explanation



As shown in [Figure 18](#) above, the three relevant selection criteria for these ads were the age of the user (above 25 years), primary location in the Netherlands and having communicated in English. However, these three criteria are not limitative.

It is not possible to draw hard statistical conclusions from this very small experiment. The only hard conclusion that can be drawn is that Facebook does not provide access to information why it showed specific advertisements to a specific user, in other words, about the individually applied logic of the ranking.

It is not feasible to conduct a test on a larger scale without following a large amount of people over a long period of time, because of Facebook's real name policy and prohibition on the use of bots. Additionally, the amount of screenshots to be studied from this small experiment already was 3.769, and this amount would increase linearly with the amount of test users and the total amount of time spent on Facebook to perform and record the tests.

To be able to draw conclusions about the logic behind Facebook's recommendations on an individual level, the right to data subject access was invoked. The results are described in Section 2.5.

To draw statistically relevant conclusions about larger populations, access to Facebook's raw data is necessary, relating to a much larger group of users, over a longer period of time. This will be regulated in the Digital Services Act. Four months after their designation by the European Commission, 3 months after the entry into

force, very large platforms will have to comply with this access requirement.⁵⁰ Entry into force will happen in the autumn of 2022.⁵¹

1.2 Processing of four categories of personal data

Facebook processes different kinds of data about the individual use of the platform, and interactions with other Facebook customers, including Pages from government organisations and advertisers. According to Facebook's explanations in an ongoing US consumer class action case in California about Facebook's sharing of private information with third parties (advertisers and parties such as Cambridge Analytica), these data can be divided into three broad categories:

1. Data collected from user activity on Facebook
2. Data collected from user activity outside of Facebook
3. Data inferred from user activity on and outside of Facebook⁵²

Additionally, Privacy Company identified a fourth category not mentioned by Facebook in the court case that is relevant for this DPIA:

4. Data collected from non-users when visiting a (public) government Page.

The personal data processed in these four categories are described in more detail below. The description also uses the explanations Facebook provides to Page owners in its unilateral joint controller agreement: the *Insights Addendum*.⁵³ Some extra explanations were used that were recently provided by a law firm on behalf of Facebook to the Norwegian DPA about the personal data processed to create Insights for Page administrators.⁵⁴

1.2.1 Data collected from user activity on Facebook

The first category of data concerns data actively provided by logged-in Facebook users, as well as data observed by Facebook. Or in other words: both Content and User Activity Data (as explained in Section 1).

Quoting from the court case: "User-provided data includes profile data, user-generated content (e.g., posts, videos, photos, comments, stories), message content,

⁵⁰ European Commission, Questions and Answers: Digital Services Act. "Once designated by the Commission, providers of very large platforms and very large online search engines have four months to comply with the DSA. Designation by the Commission takes place on the basis of user numbers reported by these services providers, which service providers will have three months after entry into force of the DSA to provide." URL:

https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

⁵¹ European Commission press release, 'Digital Services Package: Commission welcomes the adoption by the European Parliament of the EU's new rulebook for digital services', 5 July 2022, URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4313

⁵² Consumer Privacy User Profile Litigation, Northern District of California, Case no. 3-18-MD-02843, launched in 2018. Court (limited) overview of documents: <https://www.cand.uscourts.gov/judges/chhabria-vince-vc/in-re-facebook-inc-consumer-privacy-user-profile-litigation/>. Wider overview (including paid access links), URL: <https://www.courtlistener.com/docket/7067512/in-re-facebook-inc-consumer-privacy-user-profile-litigation/>

⁵³ Facebook Insights Addendum, undated, last viewed 15 July 2022, URL: https://www.facebook.com/legal/terms/Page_controller_addendum.

⁵⁴ Law firm Schjodt, June 2022, Memo on the Norwegian DPA's assessment of Facebook pages.

friends, location check-ins, linked accounts in the Facebook family of products, and language choices.

*Observed data includes clicks, profiles, Pages, Groups, and Events a user has visited, usage data, device data, networks and connections, data about user's activity level, advertisers with which the user has interacted, Pages (user Pages, Pages a user liked or recommended, Pages a user follows, Pages a user has unfollowed), **IP address when sending a message**, users that a user has chosen to "see less" or "see first" in News Feed, **time spent watching from a Page**, people whose profile a user has visited, last location, last active time, whether a user viewed someone's birthday story, people a user blocked on Messenger, Page notifications, Pages a user recommended, time zone, **email address verification**, Marketplace notifications, and interactions [emphasis added by Privacy Company].⁵⁵*

Only part of these user activity data are relevant for this DPIA, namely, the data relating to interactions with a government Page.

In its Insights (joint controller) Addendum (and memo to the Norwegian DPA), Facebook specifies the statistics are based on events such as actions, and information about the action, the person taking the action and the browser/app used for the action. Facebook explicitly only provides examples, not a limitative list. *"Events are made up of varying data points **such as the following** depending on the specific event"* [emphasis added by Privacy Company].⁵⁶

- Viewing a Page, post, video, story or other content associated with a Page
- Interacting with a story
- Following or unfollowing a Page
- Liking or un-liking a Page or post
- Recommending a Page in a post or comment
- Commenting on, sharing or reacting to a Page's post (including the type of reaction)
- Hiding a Page's post or reporting it as spam
- Hovering over a link to a Page or a Page's name or profile picture to see a preview of the Page's content
- Clicking on the website, phone number, Get Directions button or other button on a Page
- Having a Page's event on screen, responding to an event including type of reaction, clicking on a link for event tickets
- Starting a Messenger communication with the Page

⁵⁵ Facebook Inc Consumer Privacy User Profile litigation at the United States District Court Northern District of California, Case no. 3-18-MD-02843-VC, Document 913, Administrative Motion to File Under Seal - Motion to Consider Whether Another Party's Materials Should Be Sealed - filed by Facebook, Inc.. (Attachments: # (...) (5) Redacted Version of Exhibit 41, filed 12 April 2022, URL: <https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.913.5.pdf>).

⁵⁶ Facebook Insights Addendum (see footnote 40).

- Viewing or clicking on items in Page's shop
- Information about the action, the person taking the action, and the browser/app used for it such as the following:
- Date and time of action
- Country/City (estimated from IP address or imported from user profile for logged in users)
- Language code (from browser's http header and/or language setting)
- Age/gender group (from user profile for logged in users only)
- Website previously visited (from browser's http header)
- Whether the action was taken from a computer or mobile device (from browser's user agent or app attributes)
- FB user ID (for logged in users only)

This list does not mention that Facebook also uses time spent 'watching' a Page (the time a Page is shown on screen), a datapoint mentioned by Facebook in the ongoing Californian court case.

Technically, Facebook automatically collects and stores the IP address from both users and non-users when they interact with any content on a government Page, as well as cookie identifiers. However, Facebook explains that it only stores the Facebook unique user id to create Insights, not any of the other unique identifiers it collects such as IP addresses and cookie IDs.⁵⁷

Facebook writes: *"To our knowledge, events used to create Insights do not store IP addresses, cookie IDs or any other identifiers associated with people or their devices aside from a FB user ID for people logged in to Facebook."*⁵⁸

As emphasised in Facebook's quote in the ongoing court case above, Facebook does use the IP address of non-users to estimate the country/city of the visitor, but apparently, it does not separately store the IP addresses or cookie identifiers as dataset for Insights. This does not mean Facebook does not store these data in its data systems for use for its own purposes.

1.2.2

Data collected from user activity outside of Facebook

The second category of data is out of scope of this DPIA for logged-in Facebook users (but not for non-users). It covers *"information provided to Facebook by third-party advertisers, app developers, and publishers about user interactions. User interactions are things like opening a third-party developer app that integrates Facebook business tools, and visiting websites that integrate the Facebook business tools providing information about the user viewing content, searching for items, adding an item to a shopping cart, or making a purchase."*⁵⁹ This category also includes lists with hashed identifiers advertisers can upload to target their customers, or a look-a-like audience.

⁵⁷ Ibid.

⁵⁸ Law firm Schjodt, June 2022, Memo on the Norwegian DPA's assessment of Facebook pages, p. 3. In the Insights Addendum, Facebook states: *"Events used to create Insights do not store IP addresses, cookie IDs or any other identifiers associated with people or their devices aside from a FB user ID for people logged in to Facebook."*

⁵⁹ Facebook Inc Consumer Privacy User Profile litigation at the United States District Court Northern District of California, Case no. 3-18-MD-02843-VC, Document 913, Exhibit 41.

As mentioned in the Introduction, the section 'Out of Scope', the government guidelines on advertising recommend not to use personal data for advertising.

1.2.3 *Data inferred from user activity on and outside of Facebook*

The third category contains data that are created or collected by Facebook based on the content posted/viewed by Facebook users, and their behaviour (User Activity Data). This *"includes information regarding ads interests; music recommendations based on genres of music a user has interacted with on Facebook; "your topics," which is a collection of topics determined by a user's activity on Facebook that is used to create recommendations for users in different areas of Facebook such as News Feed, News, and Watch; primary location; primary public location; friend peer group; creator badges (including labels like "visual storyteller" or "conversation starter" based on activity in Groups); time zone; language preferences (including preferred language for videos, languages you may know, preferred language); and mobile service provider and country code."*⁶⁰

None of the inferred data in this comprehensive listing are mentioned in Facebook's non-limitative list of personal data processed to create Insights, except for language preferences and Country code. See the quoted bullet list above from the joint controller agreement for Insights. Facebook provides a different explanation about the origin of the country code in its joint controller agreement, and in its explanation to the Californian court. The country code stems from the mobile service provider according to the Californian court case, while it stems from the user profile or IP address according to the joint controller agreement for Insights.

1.2.4 *Data collected from non-users when they visit a government Facebook Page*

When a non-user visits a public government Page, Facebook may collect some of the personal data described in Section 2.1, limited to the actions that non-users can take. Non-users cannot 'like' or 'share' posts and do not have the unique Facebook user identifiers, hence Facebook cannot collect these personal data.

This section is focussed on the data collected by Facebook mentioned in Section 1.2.2 about the visits of non-users to websites outside of Facebook, after they have visited a government Page.⁶¹

Facebook is able to collect information about visits to off-platform websites with the help of cookies, both about users and non-users. As mentioned above, the collection of data about logged-in users about off platform activity is out of scope of this DPIA. However, the collection of off platform data about non-users is in scope of this DPIA, as these people may seek government information that is only available on Facebook. They may also inadvertently visit a public Facebook page as a result of a search query without having accepted Facebook's terms and conditions.

If a non-user visits a government Page, Facebook sets a datr cookie with a unique identifier for that user. If that non-user visits a website outside of Facebook that has an interaction option with Facebook, that website allows Facebook to retrieve the existing Facebook datr cookie from the browser of the visitor. This data exchange occurs without any conscious action from the website visitor. Facebook reads the cookie information when an interaction button or a tracking pixel is present on a web

⁶⁰ Idem.

⁶¹ Facebook, Hard Questions, What Data Does Facebook Collect When I'm Not Using Facebook, and Why? 16 April 2018, URL: <https://about.fb.com/news/2018/04/data-off-facebook/>

page, without any click on a like, share or comment button. A Facebook product management director explained in a blog post: *"When you visit a site or app that uses our services, we receive information even if you're logged out or don't have a Facebook account. This is because other apps and sites don't know who is using Facebook."*⁶²

Such interaction buttons are frequently present on popular Dutch government and commercial websites.⁶³ It is hard to find hard statistics about the presence of interactions with Facebook, as most websites have consent pop-ups that prevent automated testing on a large scale. According to a recent article in Dutch newspaper Trouw researchers from the Technical University Delft found tracking cookies from third parties on approximately 4% of Dutch decentralised government websites.⁶⁴

Prior to 2014, Facebook promised it would never use information from such external websites. However, in 2014 Facebook changed course and announced it would start to use this information for targeted advertising.⁶⁵

In sum, its use of the datr-cookie enables Facebook to link the information collected from the visited websites to specific non-users that have visited a government Page. See Section 2.4.2 for the factual findings with regard to the datr cookie.

Early in July 2022 Facebook changed the accessibility of (some) Pages. As shown in [Figure 19](#) below, non-users are strongly encouraged with a banner to log-in to view the contents, even though the admin settings for access to the test Page was and is public.

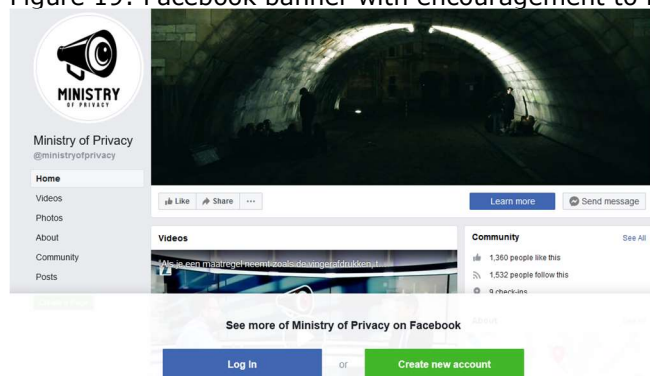
⁶² Blogpost David Baser on Facebook, as quoted by Newsweek, 'Facebook Is Tracking You Online, Even If You Don't Have an Account', 17 April 2018, URL: <https://www.newsweek.com/facebook-tracking-you-even-if-you-dont-have-account-888699>.

⁶³ A conservative estimate, based on the appearance of the Like button, is around 8,5% of the top 10.000 most visited websites in the .nl domain. Source: <https://trends.builtwith.com/widgets/Facebook-Like-Button>. On 19 July, this site listed almost 30.000 websites with a Dutch owner. URL: <https://trends.builtwith.com/websitelist/Facebook-Like-Button/Netherlands>

⁶⁴ Trouw, Overheid schendt eigen regels door cookies van derden toe te laten op websites, 4 July 2022, URL: <https://www.trouw.nl/binnenland/overheid-schendt-eigen-regels-door-cookies-van-derden-toe-te-laten-op-websites~b1a217c2/>. Questions were raised on 6 July 2022 in the Dutch Lower House, 2022Z14322. To date, these questions were not answered (89 days).

⁶⁵ Marketingweek, 12 June 2014, 'Facebook to serve ads based on web browsing history', URL: <https://www.marketingweek.com/facebook-to-serve-ads-based-on-web-browsing-history/>

Figure 19: Facebook banner with encouragement to log-in for non-users



1.3 Processing for ranking and profiling

As explained in Section 1.1.3 Facebook shows personalised content to each user, including paid promotions and advertisements, based on assumptions about the interests of the user.

In order to decide what content to show to the user, Facebook processes the three types of personal data described above: data directly provided by users in their profile, data observed about user behaviour in and outside of the Facebook platform, and data inferred from user activity.

Facebook publishes an information Page about its approach to ranking.⁶⁶ Facebook explains that it makes a personalised prediction about each post of how likely it is of interest to the user: *"for example, whether it's from your friends or family, how likely you might be to comment on it, how likely it is to foster a meaningful interaction, how likely you might be to find it on your own or if it contains a quality indicator (if a piece of news is original content, the algorithm assigns it a higher personalised relevance score, and it will often appear closer to the top of your Feed)."*⁶⁷

Facebook measured and analysed the effectivity of its predictions with the log data. In 2018 Mark Zuckerberg explained in a personal post that Facebook would rank the content higher that people interacted more with.

*"The impact will vary from Page to Page, driven by factors including the type of content they produce and how people interact with it. Pages making posts that people generally don't react to or comment on could see the biggest decreases in distribution. Pages whose posts prompt conversations between friends will see less of an effect."*⁶⁸

Additionally, Facebook runs surveys to measure the effectivity of its postings. Facebook explains:

"We also run a number of surveys asking people whether a post was "worth your time", and based on those survey responses, we predict how likely people are to find

⁶⁶ Meta Transparency Center, Our approach to ranking, last updated 17 June 2022, URL: <https://transparency.fb.com/en-gb/features/ranking-and-content/>

⁶⁷ Idem.

⁶⁸ Facebook, Bringing People Closer Together, 11 January 2018, URL: <https://about.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/>

a post worthwhile. Posts that are predicted to be more worthwhile are shown higher up in Feed.”⁶⁹

One example of a survey question Facebook mentions is related to political content.

“Better understanding content people want to see less of: Increasingly, we’re hearing feedback from people that they’re seeing too much content about politics and too many other kinds of posts and comments that detract from their News Feed experience.”⁷⁰

On the information page about ranking, Facebook refers to a blog post with more information about the predictions.⁷¹ The post explains the big scale (more than 2 billion people worldwide, that each may see 1000 potential posts in their *News Feed*).

“for each person on Facebook, there are thousands of signals that we need to evaluate to determine what that person might find most relevant. So we have trillions of posts and thousands of signals — and we need to predict what each of those people wants to see in their feed instantly.”

(...)

“the ranking system is not just one single algorithm; it’s multiple layers of ML models [Machine Learning, addition Privacy Company] and rankings that we apply in order to predict the content that’s most relevant and meaningful for each user. As we move through each stage, the ranking system narrows down those thousands of candidate posts to the few hundred that appear in someone’s News Feed at any given time.”⁷²

Facebook explains that a personalised score is determined in four distinct phases.

1. First a score is assigned to each of the 1.000 possible posts in the personal *inventory* of the user, based on the type and similarity to other items the user tends to interact with.
2. Second, the integrity of the post is assessed, and the pool of posts is narrowed down to 500.
3. The third step is where most of the personalisation happens, when the specific order is determined for each of the 500 posts in relation to the specific behaviour of the user.⁷³
4. Finally, a contextual filter is applied, to prevent that the user only gets one type of technical content, such as video posts.

⁶⁹ Meta Transparency Center, Our approach to ranking. See also: Facebook, 'Incorporating More Feedback Into News Feed Ranking', 22 April 2021, URL: <https://about.fb.com/news/2021/04/incorporating-more-feedback-into-news-feed-ranking/> . This type of survey was introduced in 2019. In 2021 new questions were added, if people found a post inspirational.

⁷⁰ Facebook, 'Incorporating More Feedback Into News Feed Ranking'.

⁷¹ Facebook, How Does News Feed Predict What You Want to See?, 26 January 2021, URL: <https://about.fb.com/news/2021/01/how-does-news-feed-predict-what-you-want-to-see/>

⁷² Idem.

⁷³ Idem.

Technically, Facebook processes the User Activity Data in a collection of different databases. The technical details of this data processing are described in Section 8.2 of this report (*Big Data Processing*).

2. Personal data and data subjects

The Dutch government DPIA model requires that this section provides a list of the kinds of personal data that are processed by Facebook, and per category of data subjects, what kind of personal data will be processed by the product or service for which the DPIA is conducted. However, this DPIA cannot provide a limitative answer to these questions.

It is up to each individual government organisation to map what categories of personal data and what different kinds of data subjects may be affected by the data processing by Facebook. This depends on the nature of the Content Data provided by the government organisation. For example: a posting on a Facebook Page from the Ministry of Health, Welfare with Covid health advice may lead to a heated debate about vaccinations. This can lead to the processing of (the special category of) health data, both directly and indirectly. People may actively and publicly explain their experiences with the disease and/or vaccinations in reply to a posting on a government Page. But Facebook may also include 'likes' and inferred information about responses to such content in its algorithmic recommendations for Content the user is presumed to be interested in: both in the form of recommended other Pages, in the form of other postings shown in the News Feed, and in the form of advertisements.

Or, a posting from the Ministry of Education, Culture and Science about free access to museums or cultural events for people under 16 may reach children. Depending on such content and the intended audience, Facebook can process different diagnostic data about the interactions of Page visitors.

This section contains 6 subsections:

1. Definitions of personal data
2. Network traffic
3. Insights and Activity logs
4. Cookies
5. Results data subject access requests
6. Categories of data subjects

2.1 Definitions of personal data

This first subsection provides a summary of the legal definition of personal data, Facebook's descriptions of personal data processing in its (new) Privacy Policy, and explanations about unique user identifiers Facebook recently provided to a Californian court.

The definition of personal data is defined as follows in Article 4(1) of the GDPR:

'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."

Facebook collects data directly from identified customers and indirectly, through the use of its services.

In its current Data Policy (dated 4 January 2022) Facebook uses the terms 'information' and 'data', without specifying when they qualify as personal data. The term 'personal data' is only used once, without definition.⁷⁴

At the end of May 2022 Facebook announced a major update of its policy per 26 July 2022, and a renaming to 'Privacy Policy'. In a blog announcing the changes to its privacy policy, Facebook says nothing changes. In the new Privacy Policy Facebook only provides more information about the processing.⁷⁵ *"While the text looks different in both, these updates don't allow Meta to collect, use or share your data in new ways."*⁷⁶ Facebook provides a summary of updates.⁷⁷ In this summary, Facebook explains it provides additional details about the purposes of the processing, retention periods, data transfers and visibility of information shared with Facebook. Facebook specifically mentions metadata: *"We also provide additional details around what metadata is and how we use it."*

The text of this new Privacy Policy will be used in this report, to the extent relevant for the scope of this DPIA.⁷⁸ The new policy still uses the terms information and data, but also contains a description of the term personal data. *"When we talk about "processing personal data", we mean the ways we collect, use and share your information, as we described in the other sections of this Policy above."* This is not a definition, or a reference to the GDPR definition. However, in the unilateral (non-negotiable, non-signable) joint controller agreement that Facebook offers for Insights, the term personal data is used with reference to the GDPR, in the sentence: *"This Insights Addendum applies only to the processing of personal data within the scope of Regulation (EU) 2016/679 ("GDPR"). "personal data", "processing", "controller", "processor", "supervisory authority" and "data subject" in this Insights Addendum have the meanings set out in the GDPR."*⁷⁹

In the new Privacy Policy, in the section 'How do we use your information' Facebook uses the verbs de-identify, aggregate and anonymize without reference to a definition

⁷⁴ Facebook Data Policy, URL: <https://www.facebook.com/privacy/policy/version/20220104> . The term personal data is used in an explanation about the legal basis for the processing, in the sentence: *"as necessary for our (or others') legitimate interests, including our interests in providing an innovative, personalised, safe and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of **personal data**."*

⁷⁵ Facebook blog, Here's What You Need to Know About Our Updated Privacy Policy and Terms of Service. 26 May 2022, URL: <https://about.fb.com/news/2022/05/metas-updated-privacy-policy/>

⁷⁶ Idem.

⁷⁷ Facebook, Summary of updates to Meta Privacy Policy and Terms of Service, URL: https://www.facebook.com/help/policysummary?locale=en_GB&vanity=policysummary&maybe_redirect_pol=true

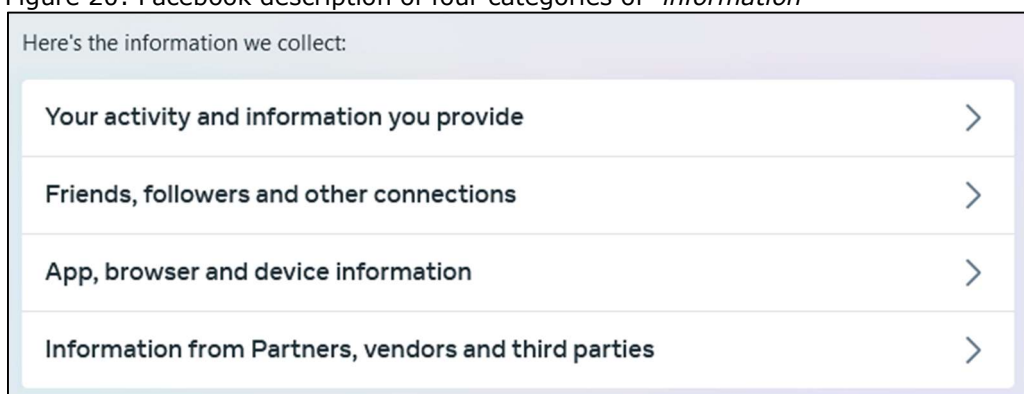
⁷⁸ Facebook Privacy Policy (into effect on 26 July 2022), URL: <https://www.facebook.com/privacy/policy>

⁷⁹ Facebook Insights Addendum.

or technical explanation. *"To use less information that's connected to individual users, in some cases we de-identify or aggregate information. We might also anonymize it so that it no longer identifies you."*⁸⁰ The policy does not mention pseudonyms.

As shown in [Figure 20](#) below, in its Privacy Policy Facebook provides a description of four types of information it collects.

Figure 20: Facebook description of four categories of "information"



With regard to Pages, in the section 'Your activity and information that you provide' Facebook writes it collects:

"Views of and interactions with a Facebook Page and its content, to provide the Page admin with aggregated information about how people use their Page and its content. Meta is jointly responsible with Page admins. [Learn more](#) about the joint processing for Insights."

The hyperlink under '[Learn more](#)' refers to a public information page with the list of information used to create the analytical data for Page administrators, the Insights described in Section 1.2 of this report above.⁸¹ Privacy Company did not find a definition or description of the term metadata in the new Privacy Policy, only references to 'metadata about content/and or messages'. There is one pop-up with a brief explanation of the term 'related metadata' and describes that Facebook can collect the date and time a photo and video was made if a user gives access to the camera roll on the device.

It follows from the ongoing Californian consumer privacy court case that Facebook uses four types of unique identifiers for user data: *"Facebook primarily uses four types of internal identifiers for user data: (1) a user identifier (UserID), (2) Replacement ID, (3) Separable ID, and (4) App Scoped Identifiers."*⁸² The fourth type of identifier is out of scope of this DPIA, as this DPIA focusses on the risks of browser-based visits to government Facebook Pages.

⁸⁰ Facebook Privacy Policy (into effect on 26 July 2022).

⁸¹ Facebook, Information about Insights Data, URL:

https://www.facebook.com/legal/terms/information_about_page_insights_data

⁸² Facebook Inc Consumer Privacy User Profile litigation at the United States District Court Northern District of California, Case no. 3-18-MD-02843-VC, Document 913, Exhibit 41.

2.1.1 UserID.

"Facebook uses an industry-wide technique called pseudonymization to represent users on the Facebook platform. In essence Facebook creates a **canonical unique identifier that encapsulates information about the user (such as First Name, Last Name, email, phone numbers, etc).** The encapsulation can be accessed by an identifier called a user identifier (or UserID); this is similar to a row being stored in a database table with the primary key being the userid and information of the user being values in the other columns. UserIDs are unique in Facebook's systems, such that two users cannot have the same UserID, and they are not recycled, meaning even after a user deletes their account, no other user can have the same UserID. The User ID is the canonical identifier to represent a Facebook user and is used in nearly all Facebook systems."

2.1.2 Replacement ID (RID)

"The RID is an identifier that supports Facebook's deletion practices by irreversibly disassociating data from a user. **Every user is assigned an RID for the lifetime of their account.** In data systems that do not support deletion (e.g. Hive), any user data retained for more than 90 days can only be retained with an RID. When a user deletes her account, Facebook deletes the record connecting the UserID to the RID so that data stored with that RID can no longer be connected to that user. Like the UserID, the RID represents a single user. Two users cannot have the same RID, and RIDs are not recycled."

2.1.3 Separable ID (SID).

The SID is similar to the RID, but allows Facebook to permanently disassociate Off Facebook Activity data from a user. Data Facebook receives from third parties about a user is associated with an SID (rather than UserID), and Facebook maintains a separate mapping between SIDs and UserIDs that can be accessed when data is processed. Through Facebook's Off Facebook Activity tool, users are able to clear their Off Facebook Activity. When a user does this, Facebook removes the mapping between the users' SID and UserID, which irreversibly dissociates the data stored with an SID from the user. Facebook then generates a new SID to be associated with the user's account moving forward."

The fact that Facebook uses and retains three unique user identifiers, and not only timestamps, means that it is technically possible to query non-indexed databases for data related to these three identifiers. These pseudonyms are personal data, as they can be related to identified natural persons. As long as Facebook is capable of relating SIDs with the UserIDs, the SID is also a pseudonym. Absent a clear technical explanation and independent audit what 'irreversible dissociation' means, SIDs are not assumed to be anonymous, as Facebook holds so many individual datapoints about a user over time that identification may very well be possible based on other points that relation to the UserID. It follows from the ongoing Californian court case that Facebook is able and ordered to query its 'cold storage' (offline) Hive tables for identified user data with existing search tools. This includes data currently not shown via the Download Your Information tool.⁸³

⁸³ Special Masters Order Regarding Production of Named Plaintiff Data. (Stein, Deborah) (Filed on 8/6/2022) paragraph 19: "(...) Plaintiffs argued "new evidence has come to light in two 30(b)(6) depositions related to those questions" showing that (1) Facebook selected [X] Hive tables and put them in "cold storage" precisely because they were relevant to this litigation;

2.2 Network traffic

This second subsection describes the analysis of the network traffic generated through the limited tests with the (fictive) Ministry of Privacy Page,

As described under 'Methodology' in the Introduction, all outgoing network traffic was intercepted during the visits to the Ministry of Privacy Page and other scripted activities by the (newly created) test accounts. Since all of Facebook's data processing takes place remotely, on Facebook's servers, it is not possible to intercept any Diagnostic Data sent from the end user device to Facebook (no Telemetry Data).

As expected, no traffic to third parties was observed in the network traffic to Facebook. Different from other advertising based services, Facebook itself is one of the largest advertising networks in the world, and hence, does not need to share visitor data with third parties to show targeted advertisements. Facebook also does not need to engage a third party analytics provider, as it operates its own (Big Data) analytics.

However, the analysis of the network traffic does not provide any clues about possible data sharing with third parties. Facebook can technically share any of the collected User Activity or Content Data with a third party through its own Application Programming Interface (API). Such traffic cannot be seen (or intercepted) by an end user, as it would take place remotely, on Facebook's servers.

2.3 Insights and Activity log of Page

This third subsection describes Facebook's data processing to produce Activity Logs and Insights for the Page administrators.

2.3.1 Insights

With Insights, Facebook shows analytics about the amount of visits to the Page, amount of visitors and their specific interactions with content on the Page. See [Figure 21](#) below.

If a Page does not have enough interactions, Facebook doesn't show more details about the visitors. As shown in [Figure 22](#) below, the test Page did not meet the threshold of at least 100 page visits or follows.

(2) Facebook is capable of searching offline Hive tables using [X] and the tool [X]; (3) the DYI file is not the most complete or usable compilation of user data; and (4) Facebook has withheld from production at least 52 snapshots of Named Plaintiff data using a never-before revealed tool more commonly used to collect user data called [X]. See Exhibit V (Plaintiffs' June 7, 2022 Submission)." This led to the following revised order in paragraph 31: "No later than August 8, 2022, Facebook is to produce the following types of Named Plaintiff data in Hive regardless of whether it appears in the DYI files: off-platform activity, ad interests, ad click data, ad impressions data, and custom audience data. Facebook will also provide the names of the tables from which the Hive data described above will be produced, how Facebook identified the tables, and the schema for such data." URL: <https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.982.0.1.pdf>.

Figure 21: Facebook Page performance results⁸⁴

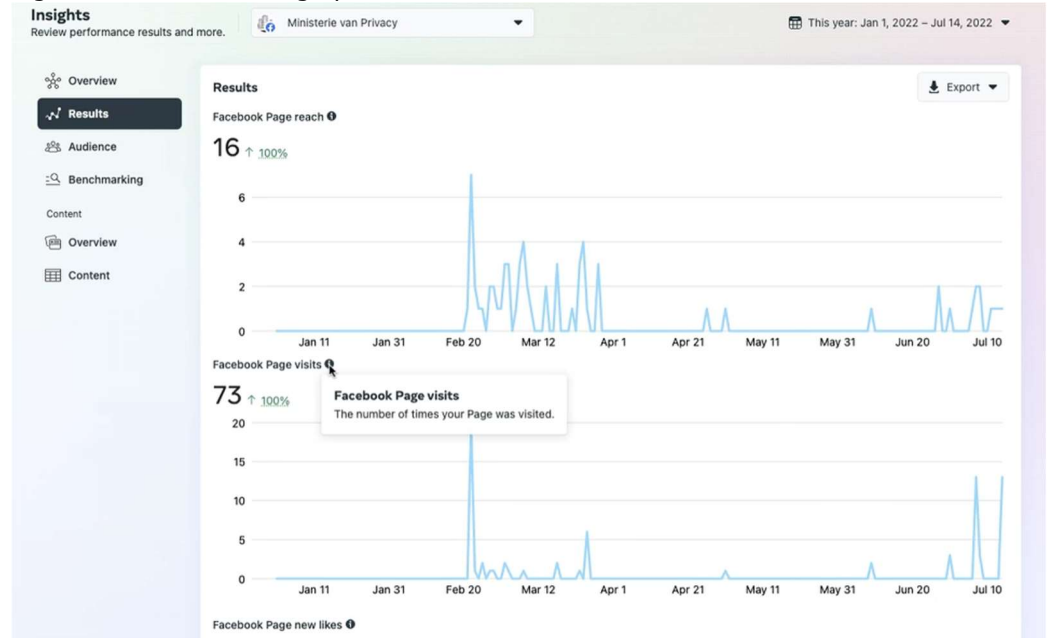
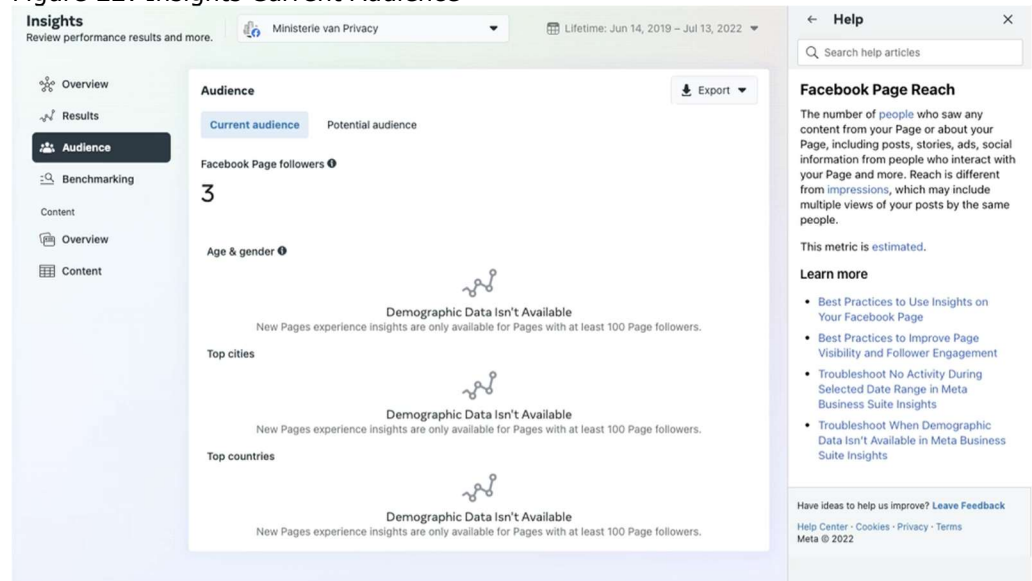
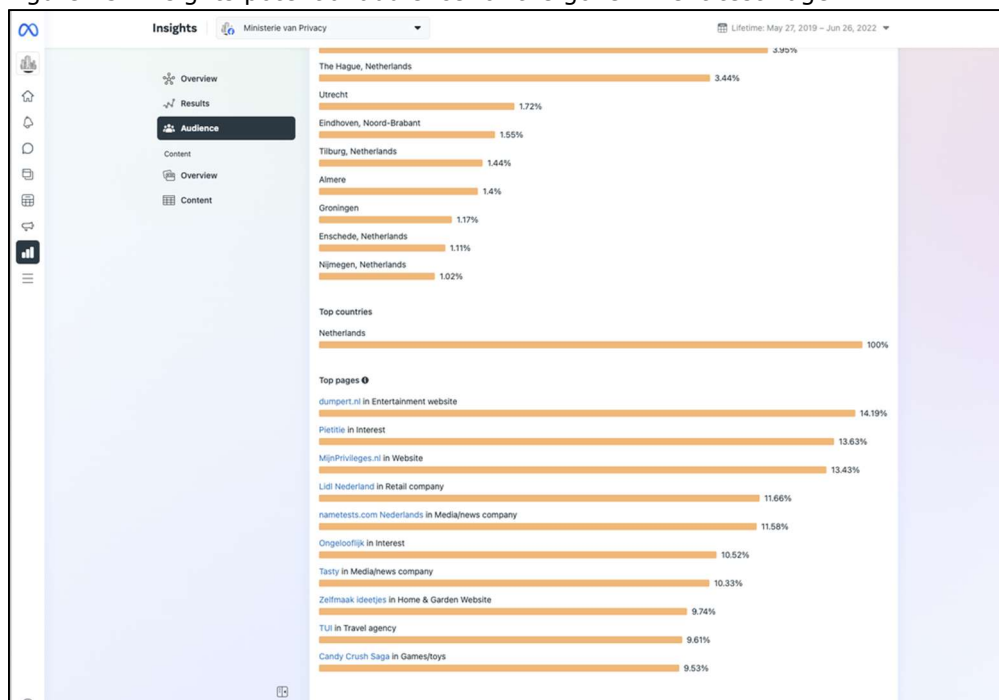


Figure 22: Insights Current Audience⁸⁵



⁸⁴ Screenshot made on 13 July 2022

⁸⁵ Idem.

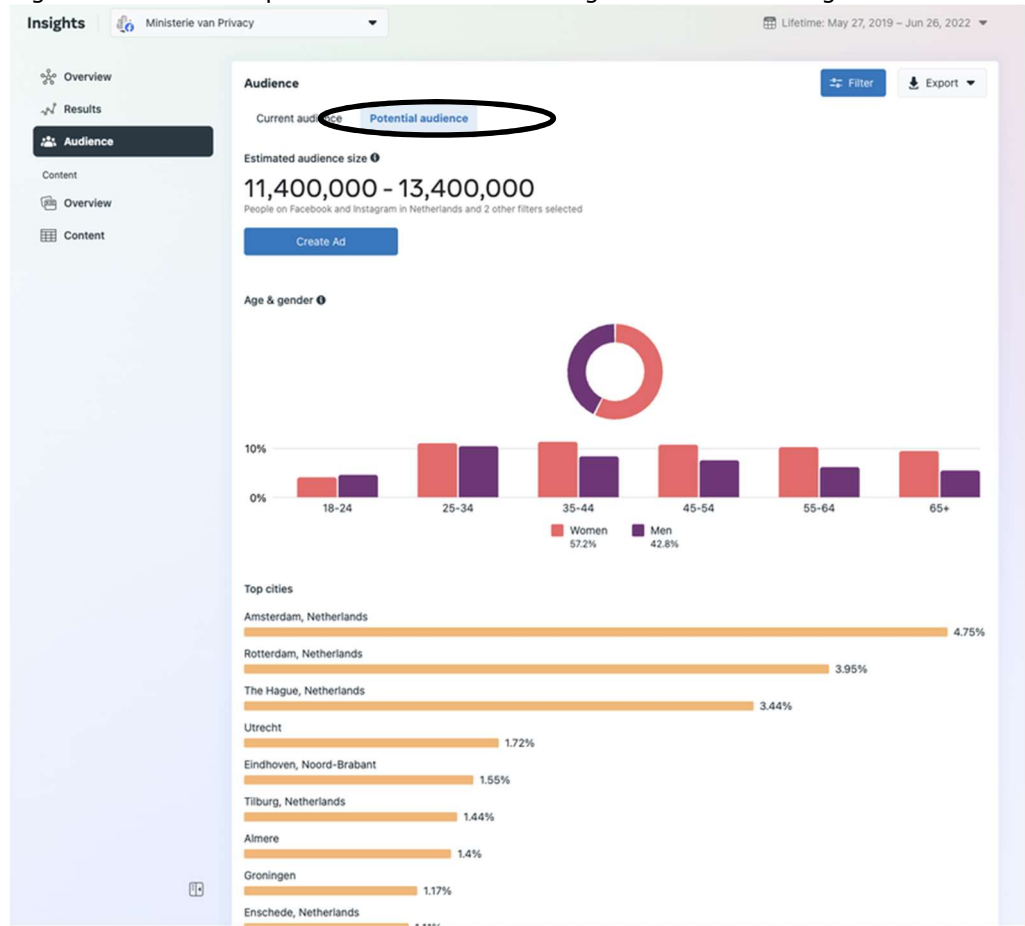
Figure 23: Insights potential audience for the government test Page⁸⁶

The bottom half of [Figure 23](#) above includes a list of Top Facebook pages. Facebook explains that it generates this metric based on an estimate of pages liked by the (potential) audience. In a deeper layer, Facebook explains such estimates are based on statistical sampling or modelling. *“Our metrics that count people (including reach and unique metrics) are sampled because it takes a large amount of data to calculate them”*. And: *“Modelling uses data from several different sources (...)”*, with the example of people remembering having seen an ad based on *“similar campaigns, people’s interactions with an ad and other signals to make these estimates.”*⁸⁷

Facebook also provides an estimate of the potential audience of the Page, per age group and gender. As shown in [Figure 24](#) below, Facebook estimates the audience size to be between 11.4 and 13.4 million Dutch users. Facebook explains that the estimate is *“not intended to match population or census data”*, but based on *“factors such as targeting selections, ad placement and how people were shown ads on Facebook in the past 30 days.”* For the test Page, Facebook also shows analytics about visitors’ interactions with the Page: how many likes and reactions, and how many replies. These are simple statistics, without reference to the personal data of the visitors. See [Figure 25](#) below.

⁸⁶ Idem.

⁸⁷ Facebook ‘Help’ side bar when clicking on the (i) for ‘estimated metrics’ in Insights.

Figure 24: Facebook potential audience for the government test Page⁸⁸

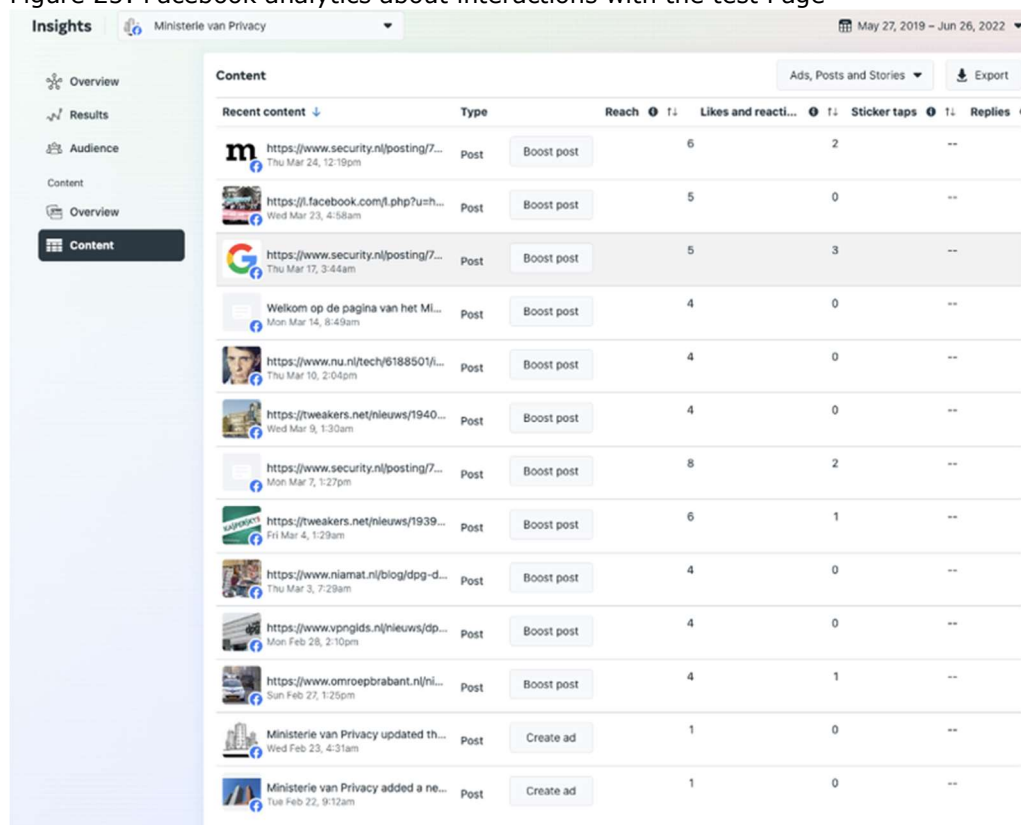
Facebook describes that only Facebook determines what personal data are used for the Insights, and that the Page administrators only have access to statistics, not to the raw data.

*"Page admins do not have access to the personal data processed as part of events but only to the aggregated Insights. (...) The events logged by Facebook in order to create Insights are solely defined by Facebook and cannot be set, changed or otherwise be influenced by Page admins."*⁸⁹

As quoted in Section 1.2.1 Facebook provides a list of the data it 'may' use to create the analytics. Facebook explains in the joint controller agreement and in its reply to the Norwegian DPA it does not separately store the IP addresses, cookie IDs or other identifiers associated with people or devices to create the analytics, but that doesn't mean that Facebook doesn't access these data when creating the analytics. It follows from Facebook's public explanations to advertisers that it accesses both the user-provided location data, and the observed user location data in order to geotarget advertisements. Facebook's explanation about the use of geolocation data directly applies to Facebook's data processing of visitors of government Pages.

⁸⁸ Screenshot made on 13 July 2022

⁸⁹ Facebook Insights Addendum.

Figure 25: Facebook analytics about interactions with the test Page⁹⁰

Facebook explains that advertisers can for example select "*People recently in this location*: Includes people who list their most recent location as your selected area. (This may include international travel)."⁹¹ And: "Selecting People living in or recently in this location option may include people who were recently in that location, even though their home location is somewhere else."⁹²

Facebook also allows advertisers to select "*People travelling in this location*: Includes people in your selected area who are in their home country, but more than 125 miles/200 km from their home location (determined by device and connection information)."⁹³

The fact that Facebook stores the IP addresses at log-in, and derives geolocation information (country, region, city) from these log-in data, is also shown in the results of the data subject access requests (as discussed below, in Section 2.5).

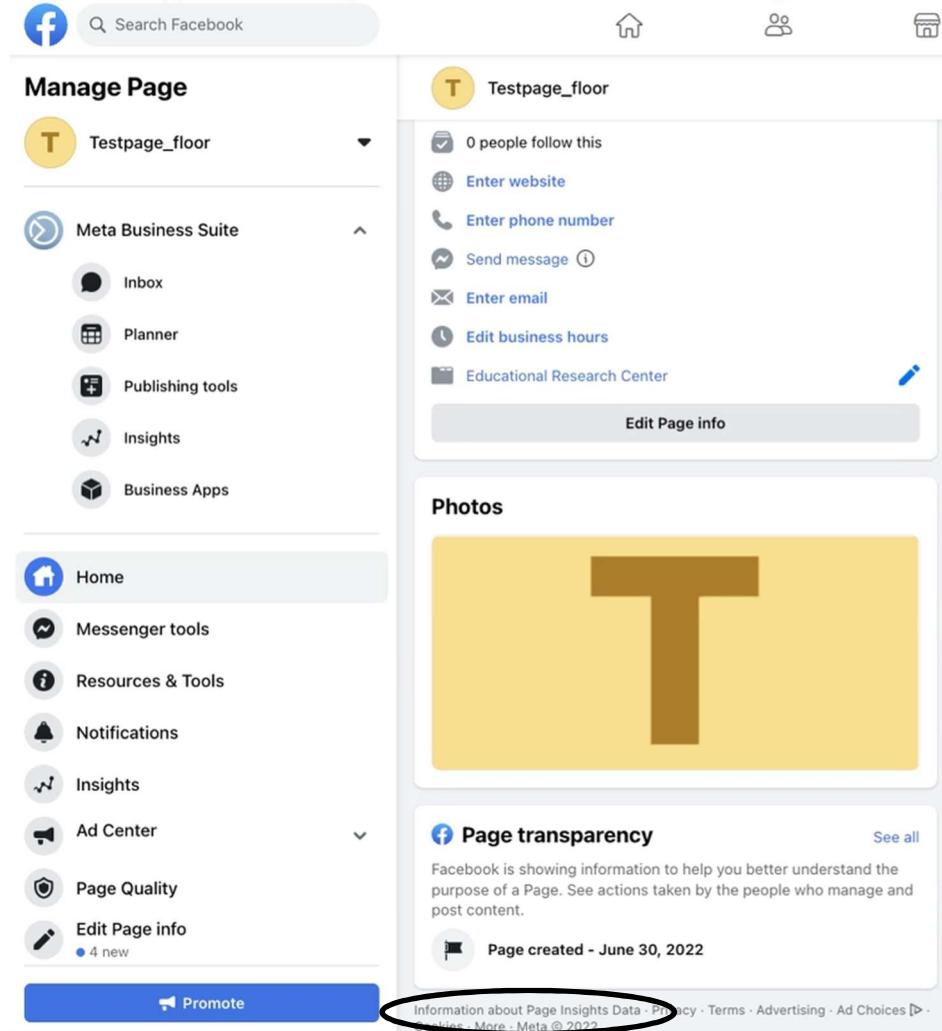
Facebook does not actively inform the administrator of a Page about this (sensitive) nature of the data processing.

⁹⁰ Screenshot made on 13 July 2022

⁹¹ Facebook, Use location targeting, URL: <https://en-gb.facebook.com/business/help/365561350785642?id=176276233019487>

⁹² Idem.

⁹³ Ibid.

Figure 26: Hyperlink to Insights Addendum after creation of Page⁹⁴

When the test Page was created, the admin was not shown any reference to the *Insights Addendum*. Only after the Page was created, a hyperlink at the very bottom of the Page appeared, in a tiny size, in a grey font in a light grey box, with "*Information about Insights Data*". See [Figure 26](#) above. This page in turn contains a hyperlink to the joint controller agreement, the *Insights Addendum*.⁹⁵

2.3.2

Activity Log

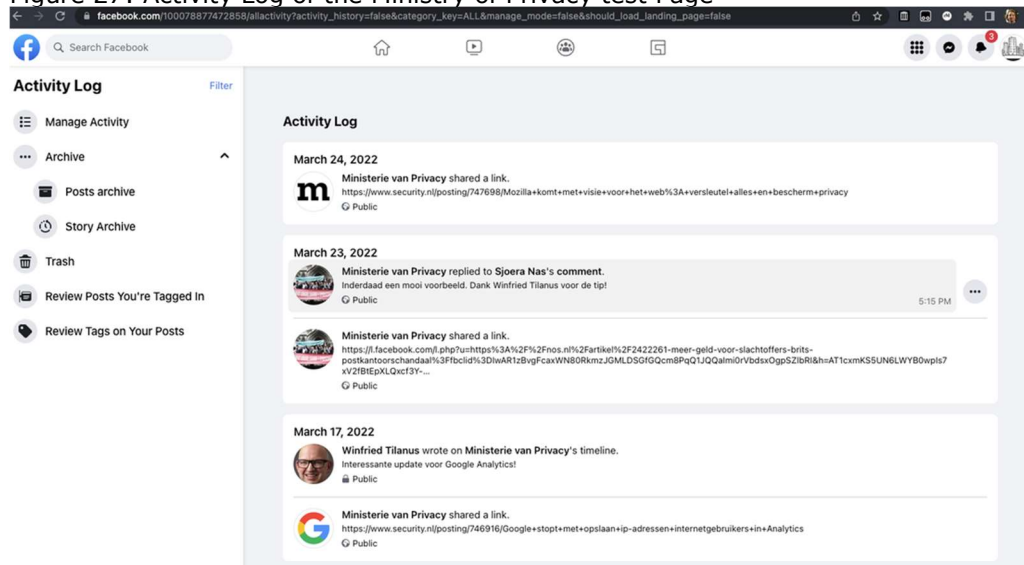
All Facebook users have access to an Activity log, both private users with a profile, and private users that manage a (government) Page.⁹⁶ Page administrators can use their 'Page' identity to access the Page Activity Log. This provides an overview of interactions with the (government) Page, including admin activity and the contents of responses to Posts from Facebook users. [Figure 27](#) below shows that test user C wrote a public response to a Post.

⁹⁴ Page last viewed 21 July 2022.

⁹⁵ Idem.

⁹⁶ Facebook, What's included in my Facebook activity log?, URL: <https://www.facebook.com/help/256333951065527>

Figure 27: Activity Log of the Ministry of Privacy test Page⁹⁷



2.4 Cookies and device identifiers

This subsection describes three ways in which Facebook sets cookies and reads device identifiers.

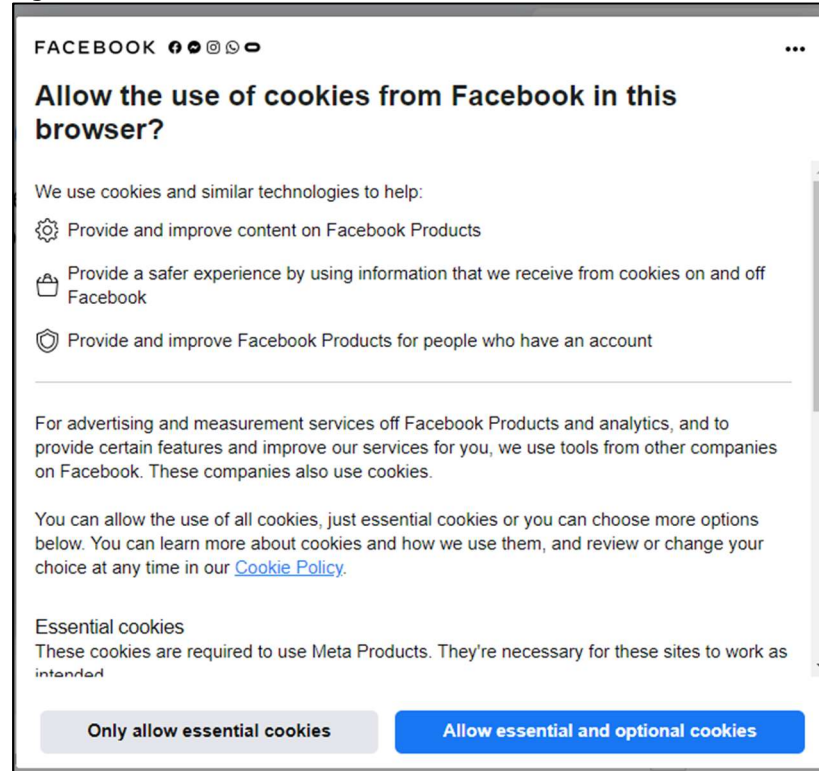
7. when a logged in Facebook user visits the Ministry of Privacy test Page,
4. when a non-user visits the Ministry of Privacy test Page, and
5. when a logged in Facebook user visits Meta's transparency center to learn more about the data processing on the government Page.

The fourth subsection in this part of the DPIA summarises the information Facebook provides about its cookies and device identifiers.

2.4.1 Cookies set in browsers of logged-in users by the Ministry of Privacy test Page

When a Facebook user directly visits the Ministry of Privacy test page, Facebook shows a cookie consent banner. This banner forces users to choose between 'essential' and 'essential and optional cookies'. As shown in [Figure 28](#) below, the two options are graphically designed in such a way to give clear preference to the button to accept optional cookies. The light grey 'only allow essential cookies' button attracts less attention than the blue button.

⁹⁷ Page last viewed on 13 July 2022.

Figure 28: Facebook cookie consent banner⁹⁸

In accordance with the test scenarios all three test users selected 'Only allow essential cookies'. Because the tests were performed with a clean browser, Facebook presented this banner to a user every time before he/she was able to sign in.

In the 'essential' cookie modus, Facebook sets 5 cookies from multiple of its own domains with contents that are long enough to contain unique identifiers in the browsers of logged-in Facebook users, as shown in [Table 1](#) below. These cookies are:

1. Datr – lifespan 2 years
2. Sb – lifespan 2 years
3. c.user – lifespan 1 year
4. xs – lifespan 1 year
5. fr – lifespan 90 days

Table 1: 'Essential' cookies set by Facebook in browser of logged-in test user C⁹⁹

Domain	Cookies and content
facebook.com	1 request, no cookies.
Edge-chat.facebook.com	2 websocket connections with the following cookies datr =dBEzYjDIcc3TrLqUN26ZNpSK; sb =gREzYgfJwOvmiQYXZGK5TBj; c_user =100078069608872; xs =9%3AwQSBwwELEvBOTw%3A2%3A1647513986%3A-1%3A-1; oo =v1; fr =05aTFMQnijiO4iSnH.AWW6CfDscddODEz-aur-Ty55enw.BiMxGF.8R.AAA.0.0.BiMxGF.AWXkPhjBRUw

⁹⁸ Cooke banner last viewed on 21 July 2022.

⁹⁹ Test user C, recorded on 17 March 2022.

gateway.facebook.com (same identifiers)	1 websocket connection with the following cookies datr =dBEzYjDICc3TrLqUN26ZNpSK; sb =gREzYgfJwOvmiQYXZGK5TBj; c_user =100078069608872; xs =9%3AwQSBwwELEvBOTw%3A2%3A1647513986%3A-1%3A-1; oo =v1; fr =05aTFMQnijiO4iSnH.AWW6CfDscddODEz-aur-Ty55enw.BiMxGF.8R.AAA.0.0.BiMxGF.AWXkPhjBRUw
www.facebook.com	247 requests datr =dBEzYjDICc3TrLqUN26ZNpSK; _js_datr =dBEzYjDICc3TrLqUN26ZNpSK; sb =gREzYgfJwOvmiQYXZGK5TBj; c_user =100078069608872; xs =9%3AwQSBwwELEvBOTw%3A2%3A1647513986%3A-1%3A-1; oo =v1; fr =05aTFMQnijiO4iSnH.AWW6CfDscddODEz-aur-Ty55enw.BiMxGF.8R.AAA.0.0.BiMxGF.AWXkPhjBRUw presence =C%7B%22t3%22%3A%5B%5D%2C%22utc3%22%3A1647513997585%2C%22v%22%3A1%7D c_user =100078069608872;
accounts.google.com	2 requests caused by the Chrome browser, not by Facebook.
Clients1.google.com	1 request caused by the Chrome browser, not by Facebook.
www.google.com	1 request for a single pixel gif in the context of a Google ad on the Facebook homepage, not the Ministry of Privacy Page.
Content-autofill.googleapis.com	3 requests, no cookies.
Update.googleapis.com	6 requests, no cookies.
Edgedl.me.gvt1.com	5 requests caused by the Chrome browser, not by Facebook.
Googleads.g.doubleclick.net	1 request for a single pixel gif served on www.facebook.com , not on the Page in scope. Test_cookie=CheckForPermission; expires=Thu, 17-Mar-2022 11:01:37 GMT; path=/ domain=.doubleclick.net; Secure; SameSite=none
external-ams4-1.xx.fbcdn.net	10 requests, no cookies.
Scontent.xx.fbcdn.net	13 requests, no cookies.
Scontent-ams4-1.xx.fbcdn.net	99 requests, no cookies.
Scontent-amt2-1.xx.fbcdn.net	95 requests, no cookies.
Static.xx.fbcdn.net	317 requests, no cookies.
Video-ams4-1.xx.fbcdn.net	205 requests, no cookies.
Video-amt2-1.xx.fbcdn.net	129 requests, no cookies.

The exchange of cookie data was tested with two popular websites in the Netherlands: an employment agency (Randstad) and an online shop / e-commerce platform (Bol.com), while the user had only accepted 'essential' cookies from Facebook. Figure 29 below shows the Datr-cookie set by the Ministry of Privacy test page.

Figure 29: Datr cookie set by the Ministry of Privacy test page¹⁰⁰

The screenshot shows a browser's developer tools with the 'Network' tab selected. A request to 'https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.niamat.nl%2Fblog%2Fdpq-de-avg-en-de-ophef-bij-tweakers%2F%3Ffbclid%3DIwAR2ydHK57R0KRL07GonRXbTf5u0K4Jrc0yTxE69LEcbBXedZsXKVU5Z9GU&h=AT1chUrIjF2cHgNgpKL6PKXfLxLIGTpTAC-z-4Z_jGXPkyw5PN25Izmpc-Tmd79cT684eDQ53RwVBfam1y4RGFMDD3sQ_fBAb0WhgdR8YXI4SFCLCS9h_u17L3JtPHoqIBEnWrpF98J6eHATcGbPJDbkDVw&__tn__=%2CmH-R&c[0]=AT1oYnASledt3l-SZSj3PIQGS-B8Q0tWqTMP_un_f5Iuw8y1U24kugna0ByX8ZoyZSeMqGer7Mw13UetSP0VvrK9Y24rRLKYf0Mwv5diFiN9d10rvGZDoRpX0MqJ_P1rXfL7DbFcYVSMwi9lsCbKvYpWktJGiaamBqRRKwpY6778Lw HTTP/1.1' is highlighted. The 'Response' tab shows the following details:

- Host:** l.facebook.com
- Connection:** keep-alive
- sec-ch-ua:** "Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
- sec-ch-ua-mobile:** ?0
- sec-ch-ua-platform:** "macOS"
- Upgrade-Insecure-Requests:** 1
- User-Agent:** Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36
- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
- Sec-Fetch-Site:** same-site
- Sec-Fetch-Mode:** navigate
- Sec-Fetch-User:** ?1
- Sec-Fetch-Dest:** document
- Referer:** https://www.facebook.com/
- Accept-Encoding:** gzip, deflate, br
- Accept-Language:** en-GB,en;q=0.9
- Cookie:** datr=K98gYipvatA0YSZZHe_2fQeh; oo=v1%7C3%3A1646321469; sb=Pd8gYiPvElqgAM7dvEPRBYAo; c_user=100078157352716; xs=14%3AuaRVmvpIcg6Y4A%3A2%3A1646321469%3A-1%3A13734; presence=C%7B%22t3%22%3A%5B%5D%2C%22ut3%22%3A1646321479366%2C%22v%22%3A1%7D

The 'Query' tab shows the request parameters:

- u:** https://www.niamat.nl/blog/dpq-de-avg-en-de-ophef-bij-tweakers/?fbclid=IwAR2ydHK57R0KRL07GonRXbTf5u0K4Jrc0yTxE
- h:** AT1chUrIjF2cHgNgpKL6PKXfLxLIGTpTAC-z-4Z_jGXPkyw5PN25Izmpc-Tmd79cT684eDQ53RwVBfam1y4RGFMDD3sQ_fBAb0WhgdR8YXI4SF
- __tn__:** ,mH-R
- c[0]:** AT1oYnASledt3l-SZSj3PIQGS-B8Q0tWqTMP_un_f5Iuw8y1U24kugna0ByX8ZoyZSeMqGer7Mw13UetSP0VvrK9Y24rRLKYf0Mwv5diFiN9d10rvGZDoRpX0MqJ_P1rXfL7DbFcYVSMwi9lsCbKvYpWktJGiaamBqRRKwpY6778Lw

Figure 30: View of Facebook cookies set by employment agency Randstad.nl¹⁰¹

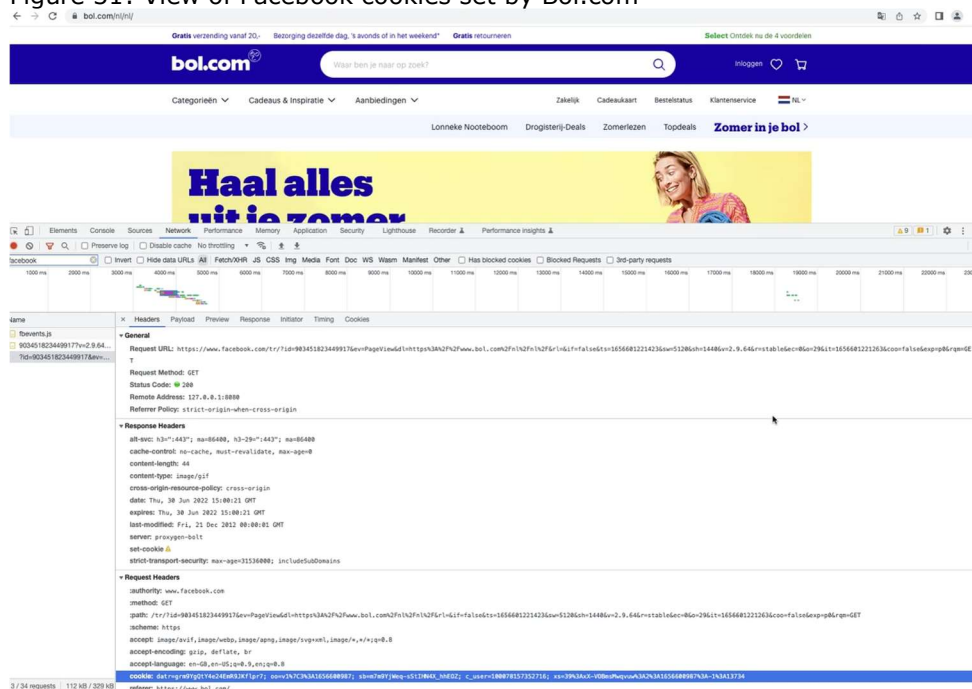
The screenshot shows a browser's developer tools with the 'Network' tab selected. A request to 'https://www.facebook.com/r/11id-223868522743156v=TrackCustomId=https3A2F%2Fwww.randstad.nl%2Fv-l4i-falsektv-s56681891396cd(content_name)=qvist5cd(action)=156cd(content_category)=qvist56w51286sh-s4486sd(external_id)=8324f4694aa3cf5c4627f8a2481d9785e72f6cd4e039ef33ab7fa87bu2.9.646rnsstabdec-26w296fprfb.1.155681854181.2497314511-s56681877586confalseqndET' is highlighted. The 'Response' tab shows the following details:

- General:**
 - Request URL:** https://www.facebook.com/r/11id-223868522743156v=TrackCustomId=https3A2F%2Fwww.randstad.nl%2Fv-l4i-falsektv-s56681891396cd(content_name)=qvist5cd(action)=156cd(content_category)=qvist56w51286sh-s4486sd(external_id)=8324f4694aa3cf5c4627f8a2481d9785e72f6cd4e039ef33ab7fa87bu2.9.646rnsstabdec-26w296fprfb.1.155681854181.2497314511-s56681877586confalseqndET
 - Request Method:** GET
 - Status Code:** 200
 - Remote Address:** 127.0.0.1:8080
 - Referer Policy:** strict-origin-when-cross-origin
- Response Headers:**
 - alt-svc:** h3="443"; ma=86400, h3-29="443"; ma=86400
 - cache-control:** no-cache, must-revalidate, max-age=0
 - content-length:** 44
 - content-type:** image/gif
 - cross-origin-resource-policy:** cross-origin
 - date:** Thu, 30 Jun 2022 14:58:11 GMT
 - expires:** Thu, 30 Jun 2022 14:58:11 GMT
 - last-modified:** Fri, 21 Dec 2022 00:00:00 GMT
 - server:** proxygen-bolt
 - set-cookie:** datr=K98gYipvatA0YSZZHe_2fQeh; oo=v1%7C3%3A1646321469; sb=Pd8gYiPvElqgAM7dvEPRBYAo; c_user=100078157352716; xs=14%3AuaRVmvpIcg6Y4A%3A2%3A1646321469%3A-1%3A13734; presence=C%7B%22t3%22%3A%5B%5D%2C%22ut3%22%3A1646321479366%2C%22v%22%3A1%7D
 - strict-transport-security:** max-age=31536000; includeSubDomains
- Request Headers:**
 - authority:** www.facebook.com
 - method:** GET
 - path:** /r/11id-223868522743156v=TrackCustomId=https3A2F%2Fwww.randstad.nl%2Fv-l4i-falsektv-s56681891396cd(content_name)=qvist5cd(action)=156cd(content_category)=qvist56w51286sh-s4486sd(external_id)=8324f4694aa3cf5c4627f8a2481d9785e72f6cd4e039ef33ab7fa87bu2.9.646rnsstabdec-26w296fprfb.1.155681854181.2497314511-s56681877586confalseqndET
 - scheme:** https
 - accept:** image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
 - accept-encoding:** gzip, deflate, br
 - accept-language:** en-GB,en-US;q=0.9,en;q=0.8
 - cookie:** datr=K98gYipvatA0YSZZHe_2fQeh; oo=v1%7C3%3A1646321469; sb=Pd8gYiPvElqgAM7dvEPRBYAo; c_user=100078157352716; xs=14%3AuaRVmvpIcg6Y4A%3A2%3A1646321469%3A-1%3A13734
 - referer:** https://www.randstad.nl/
 - sec-ch-ua:** "Not A;Brand";v="99", "Google Chrome";v="103", "Chromium";v="103"
 - sec-ch-ua-mobile:** ?0
 - sec-ch-ua-platform:** "macOS"

¹⁰⁰ Datr-cookie recorded in the browser of test user C on 17 March 2022.¹⁰¹ Recorded 30 June 2022.

Figure 30 and Figure 31 show that Facebook receives the information from the datr cookie when test user C visited two well-known Dutch websites, of employment agency Randstad, and of shop platform Bol. The user had accepted the recommended 'optimal' and 'marketing' cookies from Randstad and Bol respectively.

Figure 31: View of Facebook cookies set by Bol.com¹⁰²



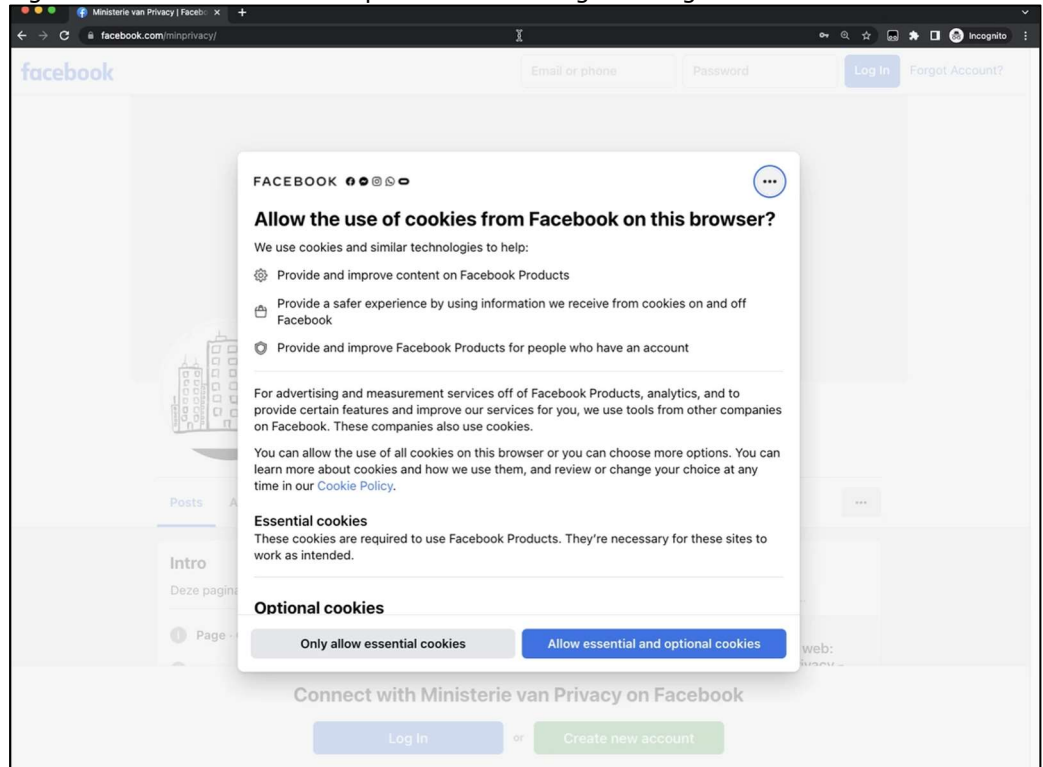
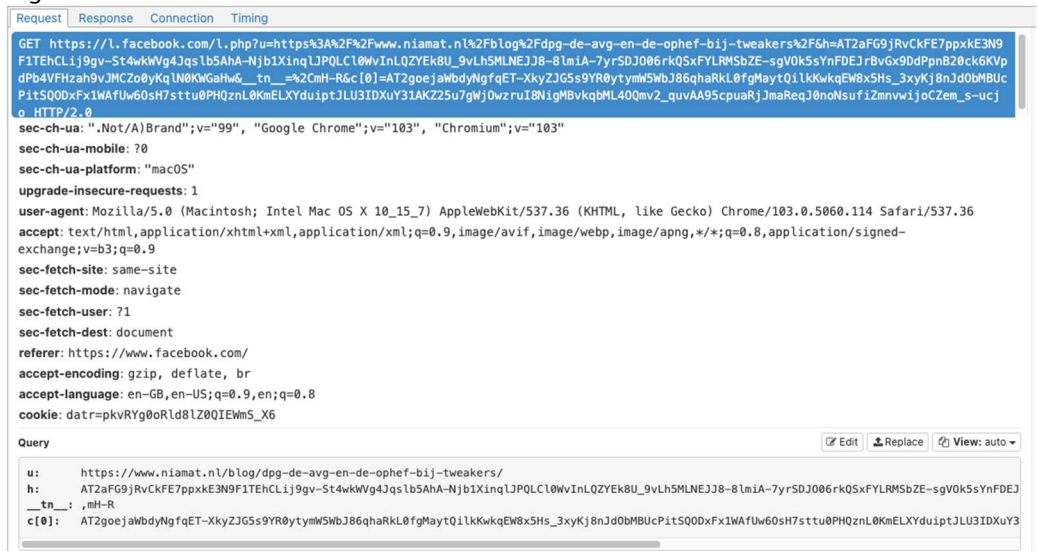
The recent expert opinion from the German State and Federal DPAs confirms this analysis. They concluded on 18 March 2022 that a choice of only essential cookies does not change Facebook's data processing: instead of cookies, Facebook uses web storage. The DPAs write: "*Werden beim Betreten einer Facebook-Seite nur erforderliche Cookie ausgewählt, ändert sich am Verhalten der Website nichts, sowohl Cookies als auch Objekte im Web Storage werden in gleicher Weise gesetzt.*"¹⁰³

2.4.2 Datr cookie set in browser of non-user

Facebook shows a cookie consent request when a non-user visits the Ministry of Privacy test page. When the user chooses the minimum option of 'essential cookies' Facebook sets the datr cookie and the _js_datr cookie (with the same content), with a lifespan of 2 years. See Figure 32 and Figure 33 below. Since early in July 2022, Facebook shows a banner to non-users inviting them to create a Facebook account or sign-in. Non-users can still see (scroll through) the contents of the Page, but are not able to interact without a Facebook account.

¹⁰² Idem.

¹⁰³ Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook - Fanpages, 18 March 2022, p. 34, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf.

Figure 32: Cookie consent request when visiting test Page¹⁰⁴Figure 33: Datr cookie set in browser of non-user¹⁰⁵

2.4.3

Cookies set when reading general privacy information

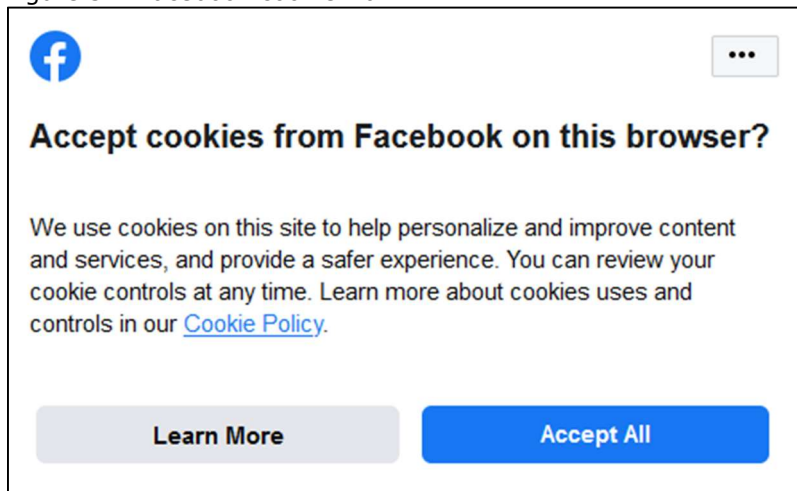
When one of the signed-in test users visited Meta's Transparency Center to read information about the data processing underlying the ranking of content in the News Feed, Facebook showed a different cookie banner, without an option to refuse advertising cookies, only an option to 'learn more'. The 'learn more' Page did not offer

¹⁰⁴ Recorded 30 June 2022

¹⁰⁵ Recorded on 30 June 2022

a means to refuse cookies, other than a reference to browser guidance to refuse third party cookies. Such a banner is commonly referred to as 'cookie wall'. As shown in [Figure 34](#) below, the two options are graphically designed in such a way to give clear preference to the 'accept all' button. The light grey 'learn more' button attracts less attention than the blue 'Accept All' button.

Figure 34: Facebook cookie wall¹⁰⁶



When the test user 'accepted' all cookies, to be able to read the public information from Facebook, this resulted in the placing of one cookie on the end user device, a cookie with the name 'cb'. See [Figure 35](#) below. The value of this cookie contains the date the cookie was set (day, month, year), and a validity of two years. This cookie was not a tracking cookie, as the identifier was not unique.

Figure 35: Single cookie set by Meta transparency Page¹⁰⁷

Name	Value	Domain	Path	Expires / Max-Age	Size	Http...	Secure	Sam...
cb	3_2022_06_29	.fb.com	/	2024-06-28T13:...	14	✓	✓	None

However, after having visited this Page, the test user surfed on to the Facebook homepage. Facebook did not show any cookie banner anymore, because the user had already accepted 'all cookies'. The visit to the homepage resulted in the placing of six cookies with unique identifiers and a retention period between 'session' and 5 years. One of these cookies is the datr cookie, the five other cookies were presence (a session cookie), xs, c_user, sb and oo. See [Figure 36](#) below. The same cookies would

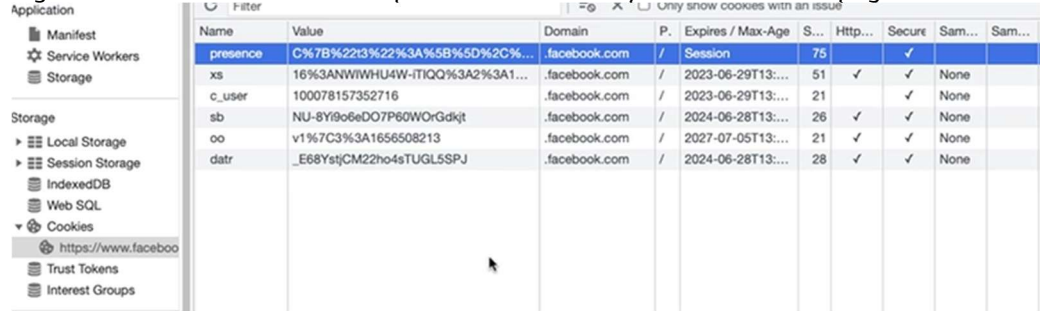
¹⁰⁶ Pop up on the URL: <https://transparency.fb.com/en-gb/features/ranking-and-content/>.

Recorded on 30 June 2022 with test account B. Last viewed 21 July 2022.

¹⁰⁷ Recorded on 30 June 2022 (in the Netherlands).

have been set if the test user had visited any other Facebook Page, including another Government Page.

Figure 36: Six cookies with unique identifiers set by Facebook homepage¹⁰⁸



Name	Value	Domain	P.	Expires / Max-Age	S...	Http...	Secure	Sam...	Sam...
presence	C%7B%22%3A%5B%5D%2C%...	.facebook.com	/	Session	75		✓	None	
xs	16%3ANWU4W-ITIQ%3A2%3A1...	.facebook.com	/	2023-06-29T13:...	51	✓	✓	None	
c_user	100078157352716	.facebook.com	/	2023-06-29T13:...	21		✓	None	
sb	NU-8Yi9o6eDO7P6OWOrGdkjt	.facebook.com	/	2024-06-28T13:...	26	✓	✓	None	
oo	v1%7C3%3A1656508213	.facebook.com	/	2027-07-05T13:...	21	✓	✓	None	
datr	_E68YstjCM22ho4sTUGL5SPJ	.facebook.com	/	2024-06-28T13:...	28	✓	✓	None	

2.4.4

Facebook's information about cookies and device identifiers

In its Privacy Policy, Facebook provides a list of 8 types of device information it collects. See [Figure 37](#) below. One of these types is 'identifiers'. Facebook provides as examples: "Identifiers we collect include device IDs, mobile advertiser ID or IDs from games, apps or accounts you use. We also collect Family Device IDs or other identifiers unique to Meta Company Products associated with the same device or account."

Figure 37: Facebook information about device information

App, browser and device information

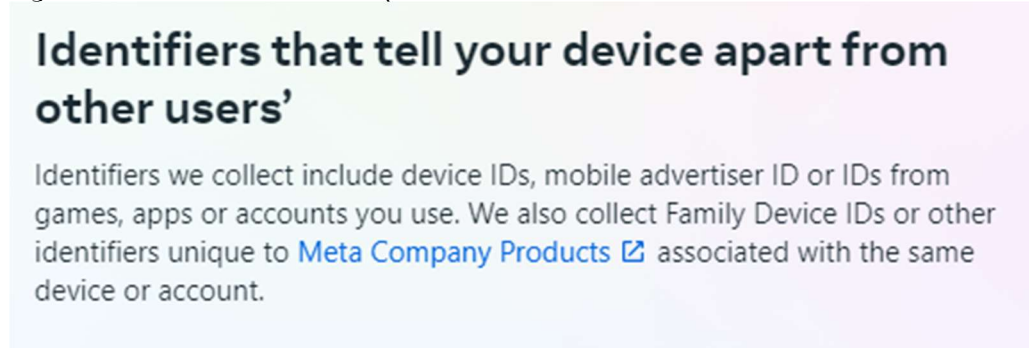
We collect and receive information from and about the different [devices](#) you use and how you use them.

Device information we collect and receive includes:

- The device and software you're using, and other device characteristics. [See examples.](#)
- What you're doing on your device, like whether our app is in the foreground or if your mouse is moving (which can help tell humans from bots)
- Identifiers that tell your device apart from other users', including Family Device IDs. [See examples.](#)
- Signals from your device. [See examples.](#)
- Information you've shared with us through device settings, like GPS location, camera access, photos and [related metadata](#)
- Information about the network you connect your device to, including your IP address. [See more examples.](#)
- Information about our Products' performance on your device. [Learn more.](#)
- Information from cookies and similar technologies. [Learn more.](#)

¹⁰⁸ Idem.

Figure 38: Facebook further explanation identifiers



Facebook does not provide an exhaustive list of the cookies it uses. In its Cookie Policy Facebook provides generic purpose descriptions and some examples. This does not include a description or explanation about the datr cookie.¹⁰⁹

Table 2: Facebook description of observed cookies

Name of cookie	Description by Facebook	Description German DPAs ¹¹⁰
Presence	<i>We use cookies such as the session-based "presence" cookie to support your use of Messenger chat windows.</i>	Only stored in the browser's memory. Purpose unclear. Possibly for the Status of Facebook Messenger or Chat?, retained during session
Xs	<i>For example: We use cookies to keep you logged in as you navigate between Facebook Pages. Cookies also help us remember your browser so you don't have to keep logging in to Facebook and so you can more easily log in to Facebook via third-party apps and websites. For example, we use the "c_user" and "xs" cookies, including for this purpose, which have a lifespan of 365 days.</i>	Unique session ID, retention period 1 year
C_user		Unique Facebook account identifier, retention period 1 year
Sb	<i>We also use cookies to store information that allows us to recover your account in the event that you forget your password, or to require additional authentication if you tell us that your account has been hacked. This includes, for example, our "sb" and "dbln" cookies, which enable us to identify your browser securely.</i>	Stores information about the browser (source: https://cookiedatabase.org/cookie/facebook/sb/), retention period 2 years

¹⁰⁹ Facebook Cookie Policy, undated, last viewed 15 July 2022, URL: <https://www.facebook.com/policy/cookies>

¹¹⁰ Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook - Fanpages, 18 March 2022, p. 4.

Oo	<i>We also use cookies, such as our "oo" cookie, which has a lifespan of five years, to help you opt out of seeing ads from Meta based on your activity on third-party websites.</i>	Only set when a user chooses 'essential' cookies. Stays on the device after log-out.
Fr	<i>For example, the "fr" cookie is used to deliver, measure and improve the relevancy of ads, with a lifespan of 90 days.</i>	Same explanation as Facebook, retention period 3 months
datr	No explanation provided in the cookie policy	Unique identifier, is also set elsewhere by Facebook for non-members or non-registered page visitors, retention period 2 years

Facebook's datr cookie, with a lifespan of 2 years, is also set and read by all websites visited by a Facebook user that have an interaction with Facebook. For example, when they publish a hyperlinked Facebook icon or other interaction option such as a like button. The use of this datr cookie was inspected by the Belgian data protection authority in 2014/2015, and played a role in the case from the Schleswig-Holstein data protection authority against a German school that had a Facebook fan Page. Hence Facebook's use of the datr cookie led to two CJEU rulings.

In the court case instigated by the Schleswig-Holstein DPA the European Court of Justice provided the following summary of the datr cookie:

*"According to the documents before the Court, the data processing at issue in the main proceedings is essentially carried out by Facebook placing cookies on the computer or other device of persons visiting the fan Page, whose purpose is to store information on the browsers, those cookies remaining active for two years if not deleted. It also appears that in practice Facebook receives, registers and processes the information stored in the cookies in particular when a person visits 'the Facebook services, services provided by other members of the Facebook family of companies, and services provided by other companies that use the Facebook services'. **Moreover, other entities such as Facebook partners or even third parties 'may use cookies on the Facebook services to provide services [directly to that social network] and the businesses that advertise on Facebook'.**"¹¹¹*

And:

*"As noted in paragraphs 33 and 34 above, the processing of personal data at issue in the main proceedings, carried out by Facebook Inc. jointly with Facebook Ireland, consisting in collecting personal data by means of cookies installed on the computers or other devices of visitors to fan Pages hosted on Facebook, **is intended, in particular, to enable Facebook to improve its system of advertising**, in order better to target its communications."*

¹¹¹ European Court of Justice, Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388, par 33, URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543>.

In their recent expert opinion on Facebook Pages, the German State and Federal DPAs argue that the retention period of the datr cookie is too long to be necessary for security purposes. They first quote the conclusion from the appellate German administrative court that the function of the datr-cookie has remained unclear, in spite of Facebook's denial that it is only used to protect the social network, and is not used for behavioural advertising. The German DPAs write: [as translated by Privacy Company]:

*"If the datr cookie were indeed used exclusively to ensure the security of the social network, the exception under Section 25 para. 2 no. 2 TTDSG [German law implementing the ePrivacy Directive, note Privacy Company] would only apply if the associated processes are necessary for this purpose. When assessing the absolute necessity, the criteria set out in the ePrivacy guidance from the German data protection authorities¹¹² are to be taken into account. In particular, it must be examined whether the duration of the storage of the datr-cookie and the associated possible access is necessary for the intended purpose. This is not the case with a retention period of 2 years. Therefore, even for the purpose of fraud prevention, the specific technical design of the datr-cookie cannot be considered necessary."*¹¹³

2.5 Results data subject access requests

This subsection summarises the results of the data subject access requests filed by the three Facebook accounts used to test the data processing for this DPIA.

As part of the methodology to understand the data processing, the researchers at Privacy Company filed data subject access requests, both directly, as data subjects B and C that visited the test Page, and indirectly, by filing a data subject access request with test user A, the administrator of the Ministry of Privacy Page. Additionally, this test user A also filed a data subject access request for the personal data relating to his own personal account.

Facebook offers its users four dedicated online tools to obtain information about the data processing.¹¹⁴

1. Download Your Information (DYI)
2. Activity log
3. View and manage ads preferences¹¹⁵
4. Why am I seeing this ad?¹¹⁶

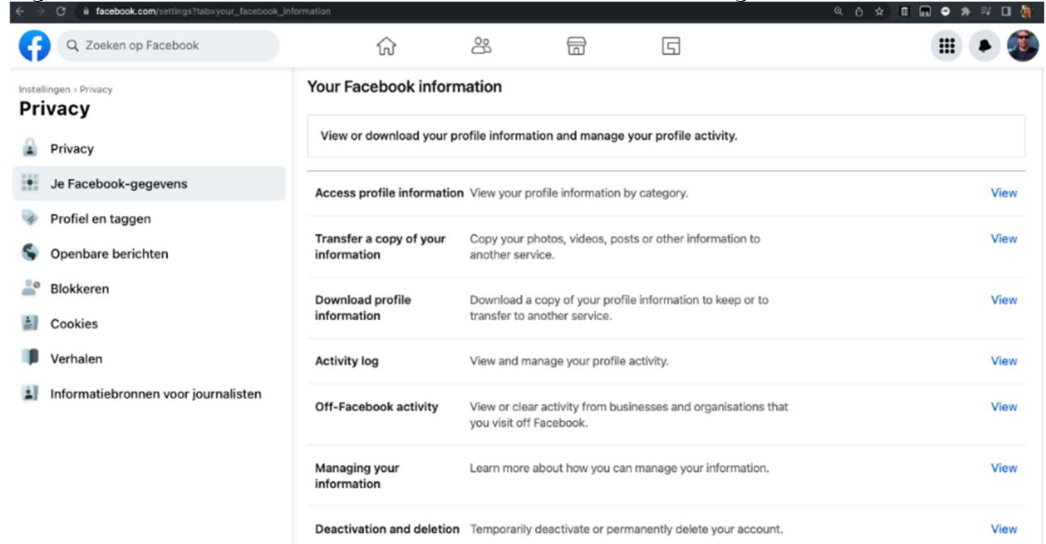
¹¹² Orientierungshilfe der DSK für Telemedienanbieter ab dem 01.12.2021 (OH Telemedien 2021), URL: https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf.

¹¹³ Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook - Fanpages, 18 March 2022, p. 34, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf.

¹¹⁴ Logged in users can visit the page Your Facebook Information at URL: https://www.facebook.com/settings?tab=your_facebook_information.

¹¹⁵ URL https://www.facebook.com/adpreferences/ad_settings

¹¹⁶ In 2019 Facebook introduced a tool that enabled users to see why a certain post was recommended in their News Feed, but this functionality has disappeared. See: <https://about.fb.com/news/2019/03/why-am-i-seeing-this/>

Figure 39: Facebook interface for users to access and manage information¹¹⁷

The first two tools are visible in the interface for users to manage their privacy settings. See [Figure 39](#) above. The other two tools are added by Facebook in the mails it sent to the 3 test users, as illustrated in [Table 3](#) below.

Table 3: Correspondence with Facebook about data subject access requests

Date	Test account A (Page admin)	Test account B	Test account C
28 March	Access request filed through ODPO contact form. Facebook confirms receipt of the forward of the requests of the two tests accounts B and C.	Access request filed with Page admin (test account A) who forwarded the request on the same day. Facebook confirms receipt of the request to the DPO for access	Same as test account B
29 March	Responded the same day notifying Facebook that access to personal data not available through the DYI was not provided and not explicitly refused.	Response in Dutch from Facebook to access request consisting of a reference to Facebook's Help Center, the DYI tool and an explanation on how to request access without a Facebook account.	Same as test account B
30 March		Lengthier mail from Facebook in English with instructions how to use DYI tool, how to see ad preferences, see your uploaded content via the Activity Log Tool, and a copy	Same as test account B

¹¹⁷ Page last viewed 22 July 2022.

		of the contents of the Privacy Policy to explain what personal data Facebook processes	
5 April	Request sent to Facebook to confirm proof of identity of test users B and C is satisfactory. This e-mail has remained unanswered.		
28 April	Facebook notified that the deadline of one month had passed for the requests from B and C. Update requested to communicate to the data subjects.		
4 May	Facebook notified of the passing of deadline and not receiving a response to e-mail of 29 March.		
13 May	Facebook responds to e-mail of 4 May. Facebook reiterates that in its opinion the previous reply is sufficient. Facebook adds: <i>"Highly technical data in its original form is likely to be meaningless to the average Facebook user and providing such data would be inconsistent with Facebook's obligations under applicable data protection laws."</i>	Same mail as test user A (in English). Facebook invokes 3 exceptions to not provide access to all personal data: <i>"Finally, we would note that the right of access is not absolute. It is subject to various exceptions. For example some data may be omitted from your download to (1) avoid adversely affecting the rights and freedoms of other users, or where another exception applies, such as (2) the protection of trade secrets or (3) the manifestly excessive nature of the request."</i>	Same as test account B
25 May	Facebook responds to the e-mail of 28 April informing the Page admin that test users B and C have	Mail (in English) with reference to the Privacy Policy and the conclusion that Meta has fully complied with its data subject rights' obligations. Meta mentions 1	Same as test account B

	been contacted by e-mail.	exception not to provide access: <i>Please note that the right of access and obtaining a copy of your data is not absolute and is subject to various exceptions. For example some personal data may be omitted from your download because providing it would adversely affect the rights and freedoms of others.</i>	
--	---------------------------	--	--

Table 4 below show the data provided by Facebook through the Download Your Information (DYI) tool.

Table 4: Files obtained via Facebook's DYI

Filename	Description
./friends_and_followers/friends.json	A list of friends
./friends_and_followers/who_you_follow.json	A list of Pages the account follows
./friends_and_followers/friend_requests_received.json	A list of friend requests received
./preferences/language_and_locale.json	A list of languages the account may know and the preferred language of the account.
./messages/inbox	Per account, a record of messages exchanged in Facebook Chat.
./messages/autofill_information.json	Contains information about the account e-mail, name and gender
./messages/secret_groups.json	Contains information about secret groups (unused while testing)
./messages/secret_conversations.json	Contains information about tinycan devices, armadillo devices and calls. Meaning unknown. Not included in test.
./apps_and_websites_off_of_facebook/your_off-facebook_activity.json	Contains information about interactions with ads and websites outside of Facebook.
./posts/album	Contains album-metadata
./posts/media	Contains media uploads like images.
./posts/your_posts_1.json	Contains a list of posts posted by the account.
./other_activity/no-data.txt	Contents unknown: the only information is that the user has no data in this section.
./comments_and_reactions/comments.json	Contains a list of comments left on posts.
./comments_and_reactions/posts_and_comments.json	Contains a list of likes
./communities/no-data.txt	N/A No communities were tested
./music_recommendations/no-data.txt	N/A No music recommendations were used
./facebook_assistant/no-data.txt	N/A Facebook's assistant was not used
./location/timezone.json	Contains the time zone of the user.

./location/primary_location.json	Contain city, province and zip-code of user's primary location
./your_topics/your_topics.json	Contains a list on inferred topics the user is interested in. Does not contain an explanation why.
./other_logged_information/ads_interests.json	Contains a list on inferred advertising topics the user is interested in. Does not contain an explanation why.
./other_logged_information/friend_peer_group.json	Contains an inferred classification of the friends peer group. E.g. "Established Adult Life"
./live_audio_rooms/no-data.txt	N/A Live Audio rooms were not tested
./polls/no-data.txt	N/A The users did not participate in polls during testing
./groups/no-data.txt	N/A The users did not participate in groups during testing
./your_interactions_on_facebook/recently_viewed.json	Contains lists of recently viewed video's, ads and marketplace items
./your_interactions_on_facebook/recently_visited.json	Contains lists of recent profile, Page, event and group visits
./saved_items_and_collections/no-data.txt	N/A Not included in tests
./search/your_search_history.json	Contains a list of recent search queries performed by the user
./facebook_gaming/no-data.txt	N/A Facebook gaming was not included in the tests
./facebook_marketplace/no-data.txt	N/A Facebook marketplace was not included in the tests
./facebook_accounts_center/no-data.txt	N/A Not included in tests
./stories/no-data.txt	N/A Not included in tests
./short_videos/no-data.txt	N/A Not included in tests
./security_and_login_information/ip_address_activity.json	A log containing logging action, combined with IP-address, timestamp and user-agent
./security_and_login_information/your_facebook_activity_history.json	Contains a log of the days the user was active on the Facebook-website, app and on Facebook Messenger
./security_and_login_information/record_details.json	Logs changes in the user account with IP address, user agent and datr cookie.
./security_and_login_information/browser_cookies.json	Contains a list of dates for each datr identifier
./security_and_login_information/mobile_devices.json	N/A Contains a list of mobile devices used, including advertiser_id. Not used for testing.
./security_and_login_information/account_activity.json	Contains a log of account activity (login and session update), includes timestamp, ip address, geolocation (country, region, city) and datr cookie
./security_and_login_information/logins_and_logouts.json	Contains a list of logins and logouts, including timestamp and ip address
./security_and_login_information/where_you're_logged_in.json	Contains a log of account activity, includes timestamp, ip address, geo location (country, region, city) and datr cookie

./security_and_login_information/login_protection_data.json	Contains a log of IP and datr-cookie information
./feed/reduce.json	Contains categories of ways posts in the feed are filtered: Sensitive content, based on fact-checker checks, etc., as indicated by the user.
./fundraisers/no-data.txt	N/A Not included in tests
./facebook_portal/no-data.txt	N/A Not included in tests
./profile_information/profile_information.json	The basic profile information provided by the user
./profile_information/profile_update_history.json	A history of changes to the profile information
./ads_information/advertisers_you've_interacted_with.json	A log of interactions with advertisers (e.g. click on an ad)
./ads_information/advertisers_using_your_activity_or_information.json	A list of advertisers using the users activity or information. Contains: advertiser name, inclusion in a custom audience, remarketing custom audience, in person store visit. Does not show the ad or what data the advertiser uploaded/choose.
./facebook_payments/payment_history.json	N/A Not included in tests
./spark_ar/no-data.txt	N/A Not included in tests
./activity_messages/group_interactions.json	Contains a count of the number of group interactions per group
./activity_messages/people_and_friends.json	Contains log of interactions with user accounts.
./events/your_event_responses.json	N/A Not included in tests
./privacy_checkup/interactions.json	Includes a log of the times the user interacted with Facebook's privacy checkup
./Pages/your_Pages.json	Contains a list of Pages administered by the account, for example the "Ministerie van Privacy" Page
./Pages/Pages_you've_liked.json	List with timestamp of Pages liked
./Pages/Pages_you_follow.json	List with timestamp of Pages followed
./other_personal_information/no-data.txt	No contents provided by Facebook
./journalist_registration/no-data.txt	N/A Not included in tests
./notifications/notifications.json	History of notifications sent by Facebook
./bug_bounty/bug_bounty.json	N/A Not included in tests
./your_places/no-data.txt	N/A Not included in tests
./reviews/no-data.txt	N/A Not included in tests
./your_problem_reports/no-data.txt	N/A Not included in tests

The DYI tool is able to distinguish between activities performed as a user, and activities performed (by that same person) as system administrator. If a user signs in with the test page (in this DPIA, as 'Ministry of Privacy') the DYI tool shows the Page administration activities, and not the activities of the same person as a private

user. As described in Section 2.3.2 the Activity log for users that are Page admins contains an archive of the content posted on the page, as well as replies to posts. The Activity log for admins does not provide any metadata about for example the time spent on the Page, or other raw data relating to the unique user, device, operating system, location and browser identifiers. This does not mean that Facebook does not collect these data.

Though Facebook allows organisations to create a separate 'owner' for (commercial or public sector) Pages, it is still necessary for a Page administrator to have a private Facebook account, to be able to create a Page. Once the Page is created, the page has an owner that can separately sign in. With this distinction Facebook enables organisations to use the name of the Page as publicly visible author of the postings, instead of the private name of the employee. This pseudonymisation however only applies to the publicly visible information on Facebook, not to other personal data generated through the use of a personal account for work purposes. An admin of a Page can also sign in with his or her private account to the professional dashboard with the visitor information, the Insights.

Though the list of data Facebook makes available via the DYI tool and other transparency tools such as the information per ad, looks impressive, it is still incomplete on essential elements. The results of all the tools combined are incomplete for four categories of personal data:

1. the logic behind the ranking of the content in the News Feed and the underlying profile;
2. the logged behavioural data;
3. the inferred data, in particular, the logic behind the advertisements, and
4. The data uploaded by advertisers for custom audiences and look-a-like lists (out of scope of this DPIA).

Facebook's tools are focussed on providing access to the content data actively submitted by the data subject, and content data shown to the user on the home Page, such as recommended friends or posts. However, Facebook is less forthcoming with the data it automatically logs about the behaviour of the user and other metadata, and the data it infers from this behaviour, such as interests in certain topics.

Facebook's explanations about the lack of access to the first three categories of data is explained in more detail below.

2.5.1 *Logic behind the ranking of content*

When asked why the logic behind the ranking of content, suggested friends and recommended posts and Pages, and the underlying profile on which the specific personalised content is based was not shown, Facebook provided a generic explanation about its processing:

"Our recommendations help users discover new and relevant content. For example, we suggest posts in their News Feed from Pages and Groups that they don't already follow, but we think they may be interested in. Several factors influence their suggested posts in News Feed such as:

- *Related engagement: A post may be suggested for users if other people who interacted with the post also previously interacted with the same group, Page or post as they did.*

- *Related topics: If they`ve recently engaged with a certain topic on Facebook, we may suggest other posts that are related to that topic. For example, if users recently liked or commented on a post from a basketball Page, we could suggest other posts about basketball.*
- *Location: Users may see a suggested post based on where they are and what people near them are interacting with on Facebook.*

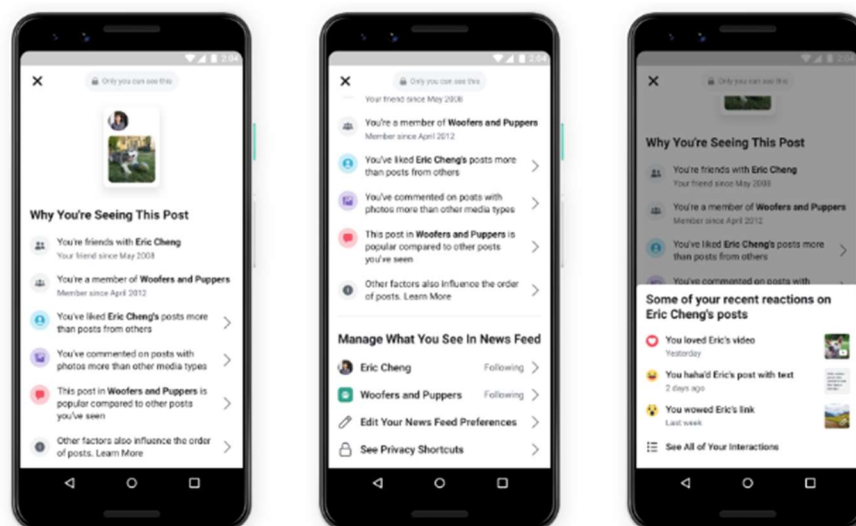
To help users understand why they may have been recommended content, users can use the "Why am I seeing this?" feature on Feed to get more context."¹¹⁸

In this mail, Facebook also refers to a public information Page about its approach to ranking.¹¹⁹ From this answer, users cannot understand why certain content was recommended to them on the government Page, or why contents from government Pages they follow were shown or not shown in their *News Feed*. For this DPIA it is relevant that users cannot obtain information how their interaction with the government Page translated in content in their *News Feed*. In the test set-up, it was unclear why test user B was shown the post with anti-government content. This Page was recommended by Facebook. The test user visited this Page, but did not like or follow. It is unclear whether this Post was a result of interactions with the test Page, or the following of the leaders of one or more specific political parties.

In another case described in [Section 1.1.3](#) the user inadvertently followed a Page with anti-government content. This lead to a high number of postings in the News Feed, higher than from other followed Pages.

Even though Facebook claims it shows information per content item since 2019, the option to see the logic behind a recommendation has apparently since been removed.

Figure 40: Facebook screenshots in 2019 with logic why content is shown¹²⁰



¹¹⁸ Facebook e-mail of 21 June 2022 to Privacy Company and the ministry of BZK.

¹¹⁹ Meta Transparency Center, Our approach to ranking, last updated 17 June 2022, URL: <https://transparency.fb.com/en-gb/features/ranking-and-content/>

¹²⁰ Idem.

As will be explained in [Section 8](#), the way in which Facebook has organised the data processing, with tasks that are performed automatically in Dataswarm on a very big scale, makes it virtually impossible for Facebook to retrieve in retrospect why each piece of content was shown to a user.

2.5.2 *Logged behavioural data*

In the DSAR results, Facebook omits to provide logged behavioural data such as time spent watching/ hovering over, a page, post, video or other content, clicks on a Page, website previously visited (from browser's http header), device and browser information. [Table 5](#) below shows what types of events were and were not included in Facebook's responses.

Table 5: Facebook events shown in reply to the access request

Types of events	Included in DSAR/DYI response
Time spent 'watching' a Page (the time a Page is shown on screen)	No
Viewing a Page, post, video, story or other content associated with a Page	No
Interacting with a story	Stories are not tested.
Following or unfollowing a Page	Yes
Liking or un-liking a Page or post	Yes
Recommending a Page in a post or comment	Yes
Commenting on, sharing or reacting to a Page's post (including the type of reaction)	Yes
Hiding a Page's post or reporting it as spam	Not tested
Hovering over a link to a Page or a Page's name or profile picture to see a preview of the Page's content	No
Clicking on the website, phone number, Get Directions button or other button on a Page	No
Having a Page's event on screen, responding to an event including type of reaction, clicking on a link for event tickets	Events are not tested.
Starting a Messenger communication with the Page	Yes
Viewing or clicking on items in Page's shop	Shops are not tested.

<p>Information about the action, the person taking the action, and the browser/app used for it such as the following:</p> <p>Date and time of action</p> <p>Country/City (estimated from IP address or imported from user profile for logged in users)</p> <p>Language code (from browser's http header and/or language setting)</p> <p>Age/gender group (from user profile for logged in users only)</p> <p>Website previously visited (from browser's http header)</p> <p>Whether the action was taken from a computer or mobile device (from browser's user agent or app attributes)</p> <p>FB user ID (for logged in users only)</p>	<p>Information provided through the DYI tool varies per type of event.</p>
--	--

Facebook's lack of transparency about these observed behavioural data was a bone of contention in the Californian class action case. It follows from the last publicly available court documents to date (the case was settled in August 2022, but no documentation about the settlement was published yet) that Facebook does retain more data in its databases than it provides via the DYI tool. For example, Facebook retains what ads have been shown to each user since 2007, but does not disclose this information via its DYI tool. This was confirmed in the Californian class action by an engineer representing Facebook:

"Q. So does Facebook log which ads a specific user is shown?
A. Yes.
Q. And when did Facebook start logging what ads a specific user is shown?
A. I believe that we have -- have -- we have -- in -- we have logged that since we started to show ads.
Q. Which was in 2007, right?
A. Yes."¹²¹

In a news article in TechCrunch the legal debate about Facebook's omissions when providing data subject access are summarised as follows:

"For two years before that deposition, Facebook stonewalled all efforts to discuss the existence of Named Plaintiffs' data beyond the information disclosed in the Download Your Information (DYI) tool, insisting that to even search for Named Plaintiffs' data would be impossibly burdensome," the plaintiffs write, citing a number of examples where the company claimed it would require unreasonably large feats of engineering to identify all the information they sought — and going on to note that it was not until they were able to take "the long-delayed sworn testimony of a corporate designee that the truth came out" (i.e. that Facebook had identified Hive data linked to the Named Plaintiffs but had just kept it quiet for as long as possible).

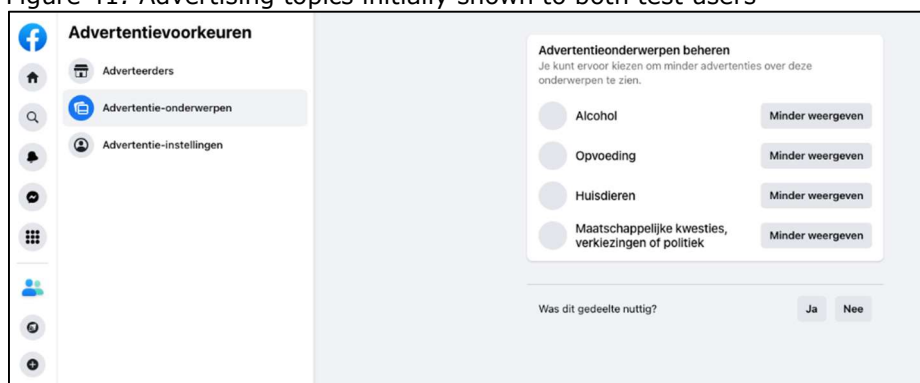
¹²¹ EXHIBIT 98-b, redacted Version of Document Sought to be Sealed, p. 140, <https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.1038.14.pdf>.

"Whether Facebook will be required to produce the data it preserved from 137 Hive tables is presently being discussed," they further observe. "Over the last two days, the parties each identified 250 Hive tables to be searched for data that can be associated with the Named Plaintiffs. The issue of what specific data from those (or other) tables will be produced remains unresolved."¹²²."

2.5.3 Inferred data and the logic behind ads preferences

Facebook did not provide access to the logic behind ads preferences. For example: both of the brand new test accounts saw four ad interests when the ad preferences were accessed: namely (i) alcohol, (ii) education, (iii) pets and (iv) societal issues, elections or politics. See [Figure 41](#) below. This category is relevant for this DPIA because visits to Government Pages may result in inference of new ads preferences. Facebook can use tracking cookies set as a result of the visit to a government Page to show targeted advertising on and off Facebook.

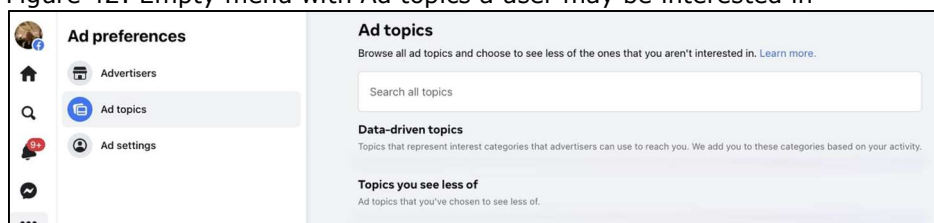
Figure 41: Advertising topics initially shown to both test users



When asked why the data subject was shown these four interest categories Facebook answered that these interests were only shown to make it possible for users to opt-out from advertising based on these interests. "All users are given the possibility to choose to decrease the ads on those topics. This is an additional user control."

After this information exchange took place, Facebook thoroughly changed the Ad preferences. Since the end of June 2022, the two test users no longer see the four ad preferences. Instead, Facebook shows a pull-down menu with a seemingly endless list of categories and subcategories. See the pull down menus in [Figure 42](#) and [Figure 43](#) below.

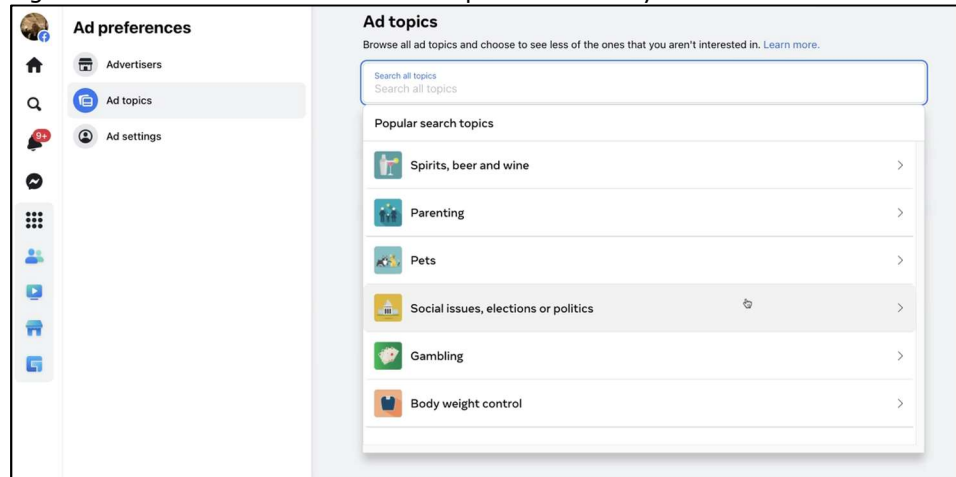
Figure 42: Empty menu with Ad topics a user may be interested in¹²³



¹²² Techcrunch, Unsealed docs in Facebook privacy suit offer glimpse of missing app audit , 16 September 2022, URL: <https://techcrunch.com/2022/09/16/unsealed-docs-in-facebook-privacy-suit-offer-glimpse-of-missing-app-audit/>.

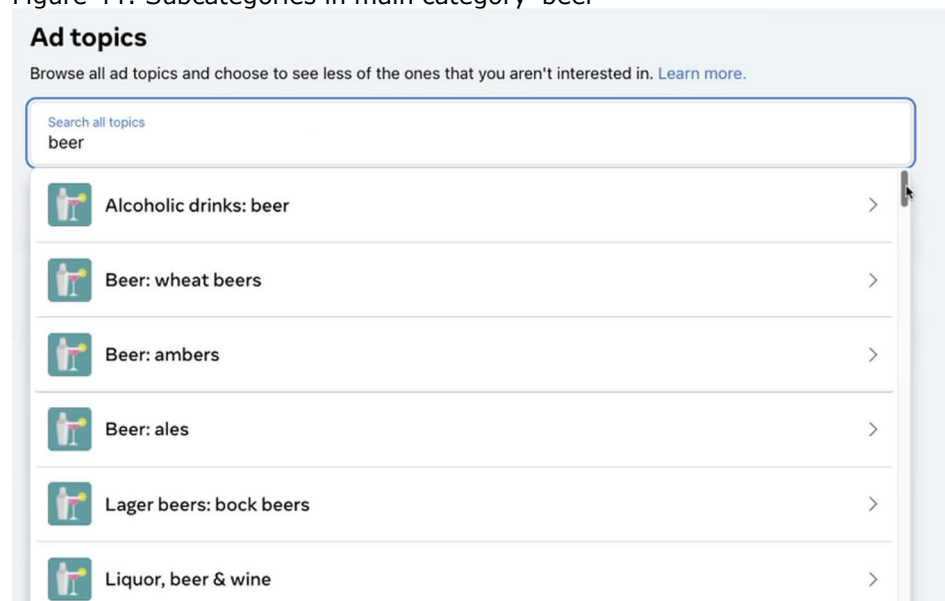
¹²³ Menu last viewed 22 July 2022.

Figure 43: Pull down menu with Ad topics a user may be interested in¹²⁴



Apparently, all of these categories now apply to a user, unless the user opts-out.

Figure 44: Subcategories in main category 'beer'¹²⁵



If a user selects a category such as 'Beer' to opt-out from advertisements, the user needs to opt-out from a long list of related or subcategories, such as different types of beer (wheat, ambers, ales, etc), and related categories such as 'liquor', with a lot of subcategories. See [Figure 44](#) above.

2.5.4 Custom audience or 'look-a-like' lists

Facebook does not show what advertisers uploaded information to Facebook relating to the user to target an advertisement (for custom audiences or 'look-a-like' lists provided by third parties). This data processing is out of scope of this DPIA.

¹²⁴ Idem.

¹²⁵ Idem.

2.5.5 *Explanation Facebook*

In an e-mail to Privacy Company and the Dutch Ministry of the Interior Facebook added that it strikes a fair balance between the competing interest of a user to obtain access to his or her personal data, and the burden for data controllers to produce these data.

"Finally, we would note that the right of access is not absolute. It is subject to various exceptions in both the GDPR and national law. For example, Article 15(4) makes clear the right to obtain a copy of the personal data undergoing processing shall not, "adversely affect the rights and freedoms of others". Article 12(5) states that a controller may refuse to act on an access request which is "manifestly unfounded or excessive, in particular because of their repetitive nature".

More generally, "proportionality" is a general principle of EU law that must inform the scope of a controller's response to a data subject request. This means data subject rights such as the right of access need to be applied in a proportionate fashion. In cases where the right to data protection runs up against other fundamental rights, the CJEU has held that it is necessary to strike a "fair balance" between the various competing interests. In other words, the right of access is not absolute and does not require the imposition of an "excessive burden" on the data controller. When engaging in this balancing exercise, the court will seek to strike fair balance between "on the one hand, the interest of the data subject in protecting his privacy, in particular through his right to have the data communicated to him in an intelligible form, so that he is able, if necessary, to exercise his rights to rectification, erasure and blocking of the data (in the event that the processing of the data does not comply with the directive) and his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to communicate such data represents for the controller.

A balanced and reasonable approach must be adopted with respect to assessing the data that is to be produced in response to a subject access request, having regard, in particular, to whether or not the data is readily accessible, and the costs incurred by the controller in retrieving certain information. The burden on Meta cannot go beyond what is necessary to achieve the objective. Given the potentially excessive burden of retrieving "all data" and the nominal value of technical data (which is meaningless to the average person) to users, we are of the view that providing users with production data, as made easily accessible through our various tools, is the best way to provide the information Meta processes about users in an intelligible and user friendly form."¹²⁶

The validity of this reply will be assessed in Section 15 of this DPIA, with reference to relevant Dutch and CJEU jurisprudence about the scope of the right of access, in relation to the scope of this DPIA, the processing of data related to interactions with the government Page, and the recommended content on the Page.

Facebook has given a more detailed explanation of the missing information in its responses to data subject access requests in the ongoing Californian court case about consumer privacy rights. The judge identified three categories of "discoverable user data" (that Facebook should provide in reply to a data subject access request):

1. data collected from a user's on-platform activity,

¹²⁶ E-mail Facebook Netherlands to Privacy Company and BZK, 5 July 2022.

2. data obtained from third parties regarding a user's off-platform activities, and
3. data inferred from a user's on or off platform activity.

Facebook explained to the court that it indeed does not provide all data belonging to the second category: the off platform activity. In this statement to the court, Facebook does not explain why it does not provide access to the third category of data: the inferred data about user behaviour on the platform.

"Plaintiffs repeatedly have asserted that DYI contains only data in category (1), citing a statement by Facebook's counsel during a status conference before Judge Corley.¹²⁷"

In fact, the full exchange with Judge Corley makes clear that Facebook's counsel was explaining that the DYI tool does not contain all data in categories (1), (2) and (3), (...) To be sure, the DYI file does not include all data related to users, but that does not mean that production of that data is consistent with Rule 26. For example, as explained above, DYI includes data received from third parties regarding a user's off-platform activity on apps and websites, such as viewing content and adding an item to a shopping cart, but does not include data identifying the specific content that was viewed or the item that was added to a cart for reasons that engineers will be prepared to explain at the hearing."

In sum, the results of the technical inspection show that Facebook processes personal data about Facebook users that visit a government Page. Based on Facebook's real name policy users are directly identifiable. Facebook is technically able to link its three different pseudonymous user IDs to the three categories of data Facebook processes: data actively provided by users, observed by Facebook and inferred by Facebook. Even if Facebook does not separately store the IP addresses and cookie identifiers that it uses to generate Insights, the statistics are pseudonymous data for Facebook, as long as Facebook retains the unique userID (as long as the person does not actively delete the account, plus 30 days, see Section 10 of this report).

Additionally, with regard to non-users that visit a government Page, Facebook is capable of singling out individual non-users based on information read from their device and browser. To this end, Facebook used at least five different kinds of tracking cookies (including the datr cookie). It appears Facebook has changed its use of cookies early in July 2022. As last tested on 15 July 2022, Facebook only sets and reads the datr tracking cookie.

2.6 Data subjects

This subsection provides an overview of the possible data subjects affected by the processing when a government organisation decides to create a Facebook Page.

This DPIA cannot provide a limitative overview of the different kinds of data subjects affected by this data processing, because this depends on the target audiences of the different government organisations.

Nonetheless, this subsection does provide some assistance to government organisations about possible visitors, to help them inventory the risks for different types of visitors.

¹²⁷ In the document, Facebook refers to Pls' Sept. 28, 2020 Mot. Compel at 7, Dkt. 526; Pls' Oct. 18, 2021 Mot. Compel Production of Named Pls' Content And Information at 3.

2.6.1 *Categories of personal data*

As described in more detail in Section 1.2.1, 1.2.3 and 1.2.4 Facebook processes two kinds of data about visits to government Facebook Pages: observed data about interactions with the Page through server logs and cookies (for users and non-users), and inferred data about advertising preferences (for users).

Personal data of a sensitive nature

Some 'normal' personal data have to be processed with extra care, due to their sensitive nature. Examples of such sensitive data are financial data, traffic and location data.¹²⁸ The metadata about who communicates with whom (in this case, with what government Pages) are of a sensitive nature, as they reveal many personal characteristics about an individual. Additionally, Facebook describes that it processes the times a user interacts with Facebook¹²⁹, time of 'hovering' over a Page¹³⁰, as well as responses to content presented on a Page or shown as posting from that Page in the personal News Feed.¹³¹

The sensitivity of the data is related to the level of risk for the data subjects in case Facebook uses the information to profile and target users. Both users and non-users may experience a *chilling effect* as a result of the monitoring of their visits to a government Page by Facebook, as these observations and inferences are used to rank the contents in the News Feed and to show targeted advertising. Nor Page administrators nor the visitors of a government Page are informed how Facebook processes the information about their visits, for what purposes, if they visit the Page, and/or interact through likes or follows.

¹²⁸ See for financial and location data the WP29 guidelines adopted by the EDPB on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, URL: [file:///C:/Users/Sjoera/Downloads/20171013_wp248_rev_01_en_D7D5A266-FAE9-3CA1-65B7371E82EE1891_47711%20\(1\).pdf](file:///C:/Users/Sjoera/Downloads/20171013_wp248_rev_01_en_D7D5A266-FAE9-3CA1-65B7371E82EE1891_47711%20(1).pdf). P. 9-10: "*Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). (...) This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.*" For the sensitivity of traffic data, see the CJEU rulings rejecting laws introducing general mandatory data retention by ISPs and telecom providers, in particular the combined ruling in cases C-511/18, C-512/18 and C-520/18, 6 October 2020, La Quadrature du Net and Others, paragraph 117 and more recently, Case C-140/20 (Irish government), 5 April 2022, paragraph 44-46.

¹²⁹ Facebook Insights Addendum, last viewed on 15 July 2022. Facebook's overview of information it collects is quoted in Section 1.2.1.

¹³⁰ Statement Facebook to the Californian Court, quoted in Section 1.2.1 as *time spent watching from a Page*.

¹³¹ Facebook Insights Addendum: *Viewing a Page, post, video, story or other content associated with a Page*.

Page visitors may experience embarrassment (if Facebook were to profile a user as a 'fan' of a politician with extremist views) or shame (if Facebook for example would infer from Page visits that a user is interested in a particular sexual disease). The chilling effect may prevent users from accessing government content that is only shown on Facebook, and not on other publicly accessible media.

Special categories of personal data

Special categories of personal data are especially protected by the GDPR. According to Article 9 (1) of the GDPR, personal information falling into special categories of data is any:

"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

With special categories of data, the principle is one of prohibition: these data may *not* be processed. The law contains specific exceptions to this rule, however, for instance when the data subject has explicitly consented to the processing, or when data have explicitly been made public by the data subject, or when processing is necessary for the data subject to exercise legal claims.¹³²

Government organisations may publish special categories of data on their Facebook Page, or the information on the page may be dedicated to visitors with sensitive characteristics. Facebook can also infer special categories of data about individual users and non-users when they visit such a government Page, for example if the information relates to specific health conditions or sexual orientation. Whether Facebook and the government organisation can successfully invoke an exception to the prohibition of the processing of special categories of data, will be discussed in Section 11 of this DPIA.

Even if Facebook has changed its advertising options, and since 19 January 2022 no longer shows detailed targeting categories to advertisers that point to sensitive categories such as political affiliation, religion, race or sexual orientation¹³³, Facebook does not exclude the use of such inferences of sensitive characteristics in the recommendations it shows to users on a government Page, and in the ranking of content in the *News Feed*.

2.6.2 *Categories of data subjects*

Generally speaking, the different kinds of data subjects that may be affected by the data processing as a result of the use of a government Page can be distinguished in three groups, namely: (i) signed in Facebook users, (ii) non-users, or users not signed into their Facebook account and (iii) the administrator of the government Page.

Facebook users

Facebook users that visit a government Page may include children younger than 16 years. From age 13 onward children are allowed to create a Facebook account. Based

¹³² These specific exceptions lifting the ban on the processing are listed in Article 9(2) under a, e, and f of the GDPR.

¹³³ Source: Euractiv, Meta to prevent ad targeting based on sensitive information, 10 November 2021, URL: <https://www.euractiv.com/section/digital/news/meta-to-prevent-ad-targeting-based-on-sensitive-information/>

on the Dutch implementation of the GDPR, below the age of 16 parental consent is required. How Facebook implements this rule, is out of scope of this DPIA.

Non-Facebook users

Though Facebook has added a permanent banner for non-users to Pages since mid-July 2022, non-users can still see the content on the Page, and scroll through the different sections. This may include visitors that have wilfully deleted their Facebook cookies, or not created a Facebook account. Facebook collects personal data about these non-users through the visits and the use of the datr tracking cookie described in Section 2.4.1.

Page administrators

As described in the previous Section 2.5, a Page administrator must use a personal Facebook account to create a Page. Once the Page is created, the page has an 'owner' that can separately sign in. The activities of the administrator on the Page are recorded by Facebook. Some of these personal data are accessible through the Page Activity Log.

3. Privacy controls

This section discusses the different privacy controls for end-users and Page administrators to minimise the processing of data about their visits to the (government) Page.

3.1 Privacy controls Page administrators

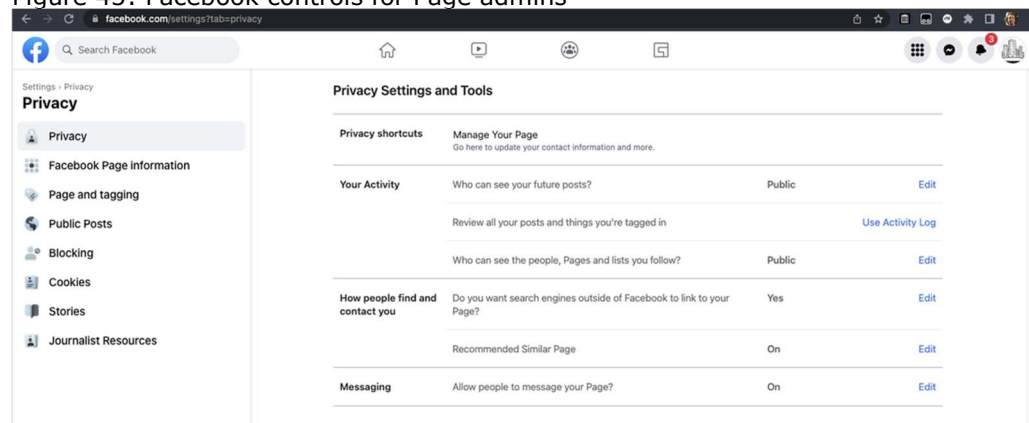
This section describes the different privacy controls Page administrators can exercise to influence the data processing. These controls do not limit the data processing by Facebook: the controls only influence the data processing by other individuals and organisations. Facebook does not allow advertisers to advertise on Pages.¹³⁴ However, sometimes advertisers can select the 'fans' of a specific Page or group of Pages, as part of the 'interest' category.¹³⁵ When briefly tested for this DPIA, the 'Ministry of Privacy' page did not appear in this category, but other specific ministries for health and for education in South America did appear.¹³⁶

¹³⁴ Facebook, About Meta Ads Placements, URL:

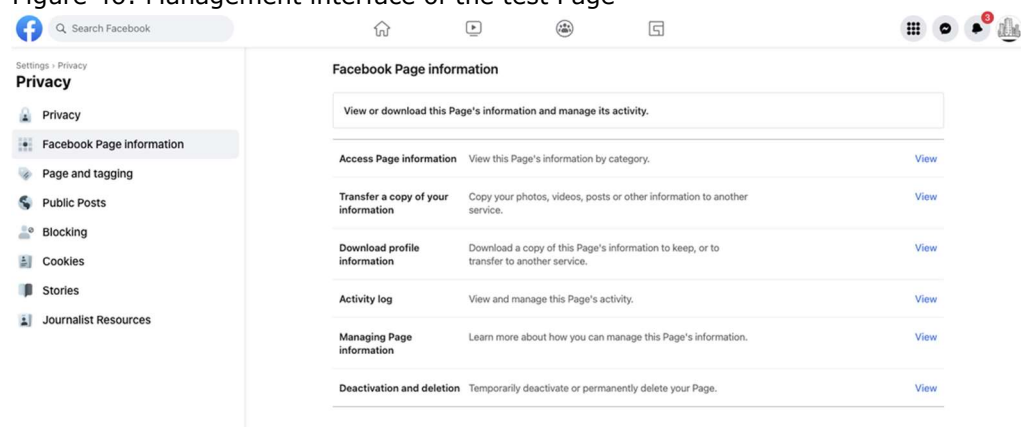
<https://www.facebook.com/business/help/407108559393196?id=369787570424415> (last viewed 24 August 2022). The page provides an exhaustive list of places where ads can be shown; Pages are not included.

¹³⁵ Techjunkie, How To Target Fans of Other Pages with Facebook Ads, 22 March 2019, URL: <https://social.techjunkie.com/target-fans-other-pages-with-facebook-ads/> (last viewed 24 August 2022)

¹³⁶ The query 'Ministry' and 'Ministerie' were entered in the 'interests' section of Facebook's advertising interface, on 24 August 2022.

Figure 45: Facebook controls for Page admins¹³⁷

As shown in [Figure 45](#), admins can opt-out from 'public' visibility of their Page to all or specific Facebook users, and they can opt-out from having their Page found through search engines. They can also opt-out from having Facebook show a banner with Recommended Similar Pages to their visitors. Admins can also block access for specific apps: for example if a user uses a gaming app that automatically posts results on Facebook as posting on a (government) Page. These options do not diminish the scope and contents of the personal data processed by Facebook.

Figure 46: Management interface of the test Page¹³⁸

Admins can also temporarily pause the Page, or export the data. See [Figure 46](#) above.

Admins cannot influence the analytics shown by Facebook. They cannot disable the analytics. They cannot ask for a shorter retention period than the default period of 3 years and 1 month (See [Section 10](#) for an overview of retention periods). Facebook does not offer an exclusive EU based data processing for Pages from EU customers (See [Section 7.2](#)). Admins cannot prohibit Facebook from using the information about interactions with the Page to infer advertising and content interests.

3.2 Privacy controls Facebook users

This section describes some of the (highly dynamic) privacy controls Facebook users can exercise to influence the data processing, only to the extent relevant for this DPIA, related to the information processed about their visits to a government Page.

¹³⁷ Page last viewed on 22 July 2022.

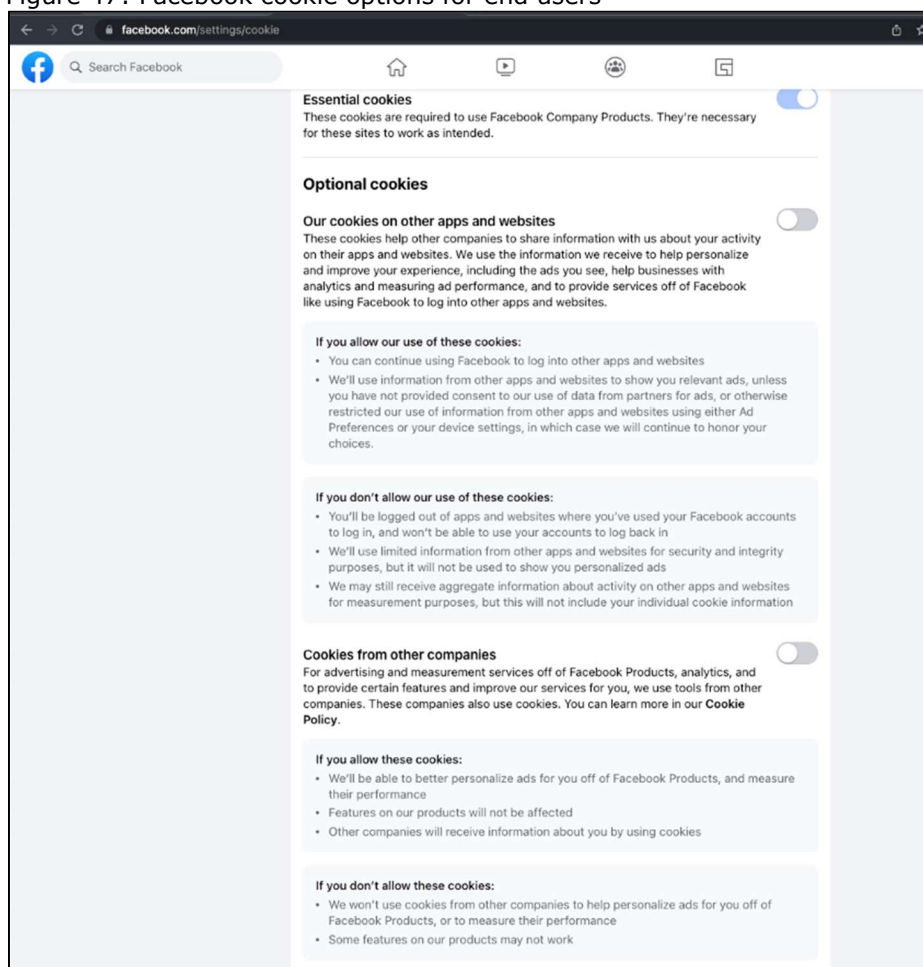
¹³⁸ Idem.

Facebook users have choices with regard to cookies, and to their advertising preferences. Users can individually choose to only select 'essential' cookies, instead of the recommended setting that enables 'optional' and 'third party' cookies. However, as explained in [Section 2.4.1](#), when Facebook sets 'essential' cookies, this includes six tracking cookies, including the datr tracking cookie. Facebook does not explain that the essential cookies include tracking cookies, as shown in [Figure 47](#) below.

Facebook users can log-out. However, this does not prevent Facebook from tracking their behaviour on and off Facebook through device recognition. Facebook distinguishes in the table in its Privacy Policy with the legal bases between users and persons that cannot be recognised based on unique device identifiers: *"If you are using a device we cannot associate with a registered user of the Meta Products."*¹³⁹

Non-users of Facebook that visit a government Page can choose between essential and optional cookies. As described in [Section 2.4.2](#) they cannot prevent the setting and reading of the datr tracking cookies, as this is included in the 'essential' level.

Figure 47: Facebook cookie options for end users¹⁴⁰



¹³⁹ Facebook Privacy Policy, last updated 26 July 2022, URL: https://www.facebook.com/privacy/policy?section_id=18.4-LegitimateInterestsWeRely

¹⁴⁰ Last viewed on 22 July 2022.

4. Purposes of the processing

Government organisations can use a Facebook Page to communicate with people on the platform where they already spend time. There is a national government policy for social media. The government interests and contents of this policy are described in Section 6.1 of this report.

Taking a bird-eye perspective, two different groups of purposes can be distinguished for which Facebook processes personal data about the visits to a government Page: (i) to produce performance results and visitor analytics for the Page owner, and (ii) to use the information observed and inferred from the visits to the government Page for Facebook's own business purposes. These two main purposes are discussed in more detail below.

4.1 Purposes Insights

Based on the Insights (joint controller) Addendum, Facebook processes personal data for the following purpose:

*"to provide analytics services called Insights to Page admins to help them understand how people interact with their Pages and the content associated with them."*¹⁴¹

The addendum does not include a limitative list what personal data Facebook processes for this purpose. However, the addendum specifies that this purpose limitation only applies to specific events used to create Insights, and their subsequent aggregation into analytics.

*"Where an interaction of people with your Page and the content associated with it triggers the creation of an event for Insights which includes personal data (...) you and Facebook Ireland Limited (...) acknowledge and agree to be joint controllers in accordance with Article 26 GDPR for the processing of such personal data in events for Insights ("Insights Data"). The joint controllership covers the creation of those events and their aggregation into Insights that are provided to Page admins."*¹⁴²

4.2 Purposes observed and inferred personal data about Page interactions

The joint controller addendum specifies that Facebook may process the personal data it obtains through interactions with the Page for other self-determined purposes.

Facebook writes: *"The Parties agree that for any other processing of personal data in connection with a Page and/or the content associated with it for which there is no joint determination of the purposes and means, Facebook Ireland and, as the case may be, you, remain separate and independent controllers."*¹⁴³

The 'other' purposes of the processing are described in several layers in Facebook's new Privacy Policy (effective 26 July 2022). Additionally, Facebook mentions other purposes for the processing of observed data through cookies in its Cookie Policy.

¹⁴¹ Facebook, Information about Insights, undated, last viewed 15 July 2022, URL: https://www.facebook.com/legal/terms/Page_controller_addendum.

¹⁴² Facebook, Insights Controller Addendum.

¹⁴³ Idem.

These texts can be summarised and objectively worded in 15 main purposes, with sub purposes. They are listed in [Table 6](#) below. The only purpose not mentioned in the Privacy Policy is the execution of privacy controls. This purpose has been added for the sake of clarity.

Table 6: Facebook purposes and sub-purposes

No.	Main purpose	Sub purpose
1.	Technically provide a personalized service	Authenticate / verify account, keep users logged-in with cookies
		Cookies to improve technical performance
2.	Serve personalised ads and other sponsored / commercial content	Help deliver ads with cookies to people who have previously visited a business's website, purchased its products or used its apps and to recommend products and services based on that activity.
		To decide what to show, use information including: profile information, the user's activity on and off our Products, things Facebook infers about a user and information about friends, including their activity and interests.
		Limit the number of times an ad is shown with the fr cookie
		Serve and measure ads across different browsers and devices used by the same person with cookies
		Use cookies to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote
		Use of cookies to make suggestions to users, and to customise content on third-party sites that integrate the social plugins
3.	Rank the contents shown in the <i>News Feed</i> based on a profile	
4.	Improve the Meta Products (including Instagram and WhatsApp)	See if a product is working correctly
		Troubleshoot and fix it when it's not
		Test out new products and features to see if they work

		Get feedback on ideas for products or features
		Conduct surveys and other research about what users like about the Meta Products and brands and what Meta can do better ¹⁴⁴
5.	To develop and provide features and integrations with other Meta products	
6.	To understand how people use and interact with (other) Meta products	
7.	Process according to user and Page administrator privacy settings	
8.	Further processing for unspecified purposes after de-identification and aggregation, or anonymisation	
9.	Manual and technical review of content information, <i>'to train our algorithms'</i>	
10.	Promote safety, security and integrity, including	Verify accounts and activity
		Prevent unauthorised access with cookies
		Account recovery with cookies
		Find and address violations of the terms or policies.
		Investigate suspicious activity
		Detect, prevent and combat harmful or unlawful behaviour and activity such as spam and phishing attacks, also with cookies
		Detect and prevent spam and other bad experiences
		Detect when somebody needs help and provide support
		Detect and stop threats to personnel and property
		Maintain the integrity of the Meta Products

¹⁴⁴ Purposes 5 to 9 are mentioned in a pop-up relating to the word improve.
<https://www.facebook.com/privacy/policy/?subpage=2.subpage.4-HowWeUseInformation>

11.	Analytics and research for Meta's own purposes	Use of cookies to better understand how people use the Meta Products to improve them
12.	Providing measurement, analytics and business services for Partners, including	How many people see and interact with their content, including posts, videos, Facebook Pages, listings, Shops and ads (including those shown through apps using Meta Audience Network)
		How people interact with the content, websites, apps and services of (business) customers, also with cookies to help businesses understand the kinds of people who like their Facebook Page or use their apps so that they can provide more relevant content and develop features that are likely to be interesting to their customers.
		What types of people interact with their content or use their services
13.	To communicate with the user, including:	Send messages about the Products Meta knows are used, using the email registered to the user account
		Depending on the user settings, send marketing communications about Products the user might like
		Ask to participate in research based on things like how the user uses our Products
		Inform about policies and terms of service
		Send replies to email
		Facilitate customer support communications in reply to questions or concerns about the Meta Products, either directly or through a third party
		Send messages about the used Products via the email registered to the account

14.	To research and innovate for social good. This includes:	Contributing to social good and areas of public interest
		Advancing technology
		Improving safety, health and well-being
15.	Share information with Partners (advertisers), vendors (measurement and marketing vendors), service providers and third parties (external researchers, law and copyright enforcement (<i>in response to legal requests, to comply with applicable law or to prevent harm.</i>))	

5. Processor or (joint) controller

5.1 Definitions

Article 4 of the GDPR contains definitions of the different roles of parties involved in the processing of data: (joint) controller, processor and subprocessor.

Article 4(7) of the GDPR defines the (joint) controller as:

"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

The GDPR stipulates in Article 26 that joint controllers must determine their roles and responsibilities, especially towards data subjects, in a transparent agreement.

The GDPR stipulates in Article 4(8) that a processor may only process data on behalf of a data controller. *'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

Article 28 GDPR determines that the obligations of processors towards the controllers for whom they process data. Article 28 GDPR contains 8 specific obligations for the processor, such as that it may only process personal data in accordance with documented instructions from the controller, and that it must, for example, cooperate with audits. It follows from Article 28(4) GDPR that a processor may use subprocessors to perform specific tasks for the data controller.

5.2 Data processor

Facebook does not offer a data processor agreement to its business and government users of Pages, and does not factually behave as a data processor for the government organisation with a Page.

5.3 Data controller

In the joint controller agreement for Insights, Facebook qualifies itself as an independent data controller for the processing of all personal data related to the use of a Facebook Page, except for the data specifically created and aggregated for Insights.¹⁴⁵ Facebook writes: *“With the exception of the processing for Insights, Meta does not have any other contractual relationship or other cooperation that entails joint control over processing of personal data for Facebook Pages. Meta and Page admins are **hence** separate controllers for their own processing of personal data.”*¹⁴⁶

As independent data controller Facebook permits itself to process the personal data relating to the interactions with a (government) Page for 15 broad purposes, with sub purposes (as described in Section 4.2 above). These purposes include many types of processing related to profiling and targeted advertising.

Due to Facebook’s non limitative descriptions, it is not clear what personal data are processed by Facebook in an independent role, and what personal data in a role as ‘joint controller’. This makes it very difficult for government Page owners to assess their own role and responsibilities, and to adequately inform visitors to their website about the scope and impact of the data processing.

When Facebook acts as an independent controller, a government organisation that creates a Page needs to have a legal ground for the transfer of personal data about visits and visitors to its Page to an independent third party (Facebook). This will be assessed in Section 11 of this DPIA.

5.3.1 Disclosure to law enforcement and secret services

One of the purposes for which Facebook processes personal data as independent data controller is respond to legal requests. Facebook must comply with legal obligations imposed under US American law.

Based on the Schrems-II ruling, an expert legal analysis for the Dutch government, the analysis made by US law professor Stephen I. Vladeck (for the conference of the German State DPAs¹⁴⁷), the report from Ian Brown and Douwe Korff for the LIBE committee of the European Parliament¹⁴⁸ and input provided to SLM Rijk and SURF by multiple cloud providers in 2021, an overview was created of US laws that may be

¹⁴⁵ Facebook, Information about Insights, undated, last viewed 15 July 2022, URL: https://www.facebook.com/legal/terms/Page_controller_addendum.

¹⁴⁶ Law firm Schjodt, June 2022, Memo on the Norwegian DPA’s assessment of Facebook pages.

¹⁴⁷ Prof. Stephen I. Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, 15 November 2021, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladeck_Rechtsgutachten_DSK_en.pdf. Professor Vladeck previously acted as expert (together with Peter Swire) on behalf of Facebook in the Schrems-II case at the European Court of Justice, where he defended US intelligence gathering as offering ‘essentially equivalent’ protections, similar to the essential data protection guarantees in the EU. See for a summary of his points, IAPP, Understanding ‘Schrems 2.0’, URL: <https://iapp.org/news/a/understanding-schrems-2-0/>.

¹⁴⁸ Ian Brown and Douwe Korff, Study for the LIBE committee, Exchanges of Personal Data After the Schrems II Judgment, July 2021, URL: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU\(2021\)69467_8_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)69467_8_EN.pdf)

applied to compel US cloud services providers to disclose personal data from EU customers.

Facebook qualifies as electronic communications service provider as defined in Title 50 of the United States Code (USC) § 1881(b)(4). The definition is as follows.

The term "electronic communication service provider" means—

- a) a telecommunications carrier, as that term is defined in section 153 of title 47;*
- b) a provider of electronic communication service, as that term is defined in section 2510 of title 18;*
- c) a provider of a remote computing service, as that term is defined in section 2711 of title 18;*
- d) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or*
- e) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).¹⁴⁹*

This report assumes Facebook also qualifies as "remote computing services" or "electronic communication services" (applicability of US Stored Communications Act and US CLOUD Act).¹⁵⁰ The table below does not include legal obligations related to other US companies in other industries, such as banks or telecommunications carriers.

Table 7: Overview of US law to obtain personal data from EU Customers

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
Non-Disclosure orders can be issued up to one year ¹⁵¹ and have become		Non-disclosure orders or general secrecy requirements. Transparency	

¹⁴⁹ See the official law website of the US government: <https://uscode.house.gov/>

¹⁵⁰ "Remote Computing Service[s]" ("RCS") and "Electronic Communication Service[s]" ("ECS") are defined in 18 U.S.C. § 2510(15): "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications"; and 18 U.S.C. § 2711(2) ("remote computing service" means the provision to the public of computer storage and processing services by means of an electronic communications system"). As Facebook does not offer separate EU storage, the US CLOUD Act is less relevant for Facebook. However, there may be Support Data that are primarily processed by the Irish establishment that may fall under the reach of the US CLOUD Act.

¹⁵¹ A judge can issue a protective order for all SCA and CLOUD Act orders "when the independent judge determines that there is reason to believe that notification of the existence of the court order may create the adverse result of (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial." US Department of Justice, The purpose and impact of the CLOUD Act,

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
'commonplace'. ¹⁵² No principled restrictions on transparency reporting		reporting is only permitted in ranges. ¹⁵³	
US Stored Communications Act, also allows for preservation orders for specific records/evidence ¹⁵⁴	Content Data: warrant signed by a judge. Requires <i>probable cause</i> .	Executive Order of the President (E.O.) 12333 as amended (limited) by Presidential Policy Directive (PPD) 28. ¹⁵⁵ Since January 2021 Specified in NSA SIGINT Annex ¹⁵⁶	Does not give direct authority to NSA to order cloud providers to hand-over data, but allows for bulk interception of transatlantic cables
	Non-Content Account Data (for example names and IP-addresses) ¹⁵⁷ subpoena from court, prosecutor or agency (judge not required)		
	Other Non-Content (for example device information) ¹⁵⁸ : court order or search warrant signed by a		

Q&A 28, URL: <https://www.justice.gov/dag/Page/file/1153466/download> The gagging orders are based on 18 U.S.C. § 2705. The maximum period of one year is mentioned in a memorandum from the Deputy Attorney General, 19 October 2017, URL: <https://www.justice.gov/criminal-ccips/Page/file/1005791/download>.

¹⁵² According to testimony of Microsoft VP Tom Burt for the House Committee on the Judiciary, 30 June 2021, URL: <https://blogs.microsoft.com/on-the-issues/2021/06/30/the-need-for-legislative-reform-on-secrecy-orders/>.

¹⁵³ The secrecy requirements are defined in 18 U.S.C. § 1874, but the USA Freedom Act of 2015 authorizes four different options for companies to publish numerical information about the NSLs and FISA orders they receive.

¹⁵⁴ Clause 2703(f) of the US Stored Communications Act.

¹⁵⁵ Presidential Policy Directive 28 does not authorize intelligence gathering. It imposes limitations on how signals intelligence is gathered through other authorized means when targeting non-U.S. persons (e.g., the why, whether, when and how the intelligence community targets foreign communications). Those means are articulated in the FISA 702 legal framework.

¹⁵⁶ NSA Sigint Annex, Procedures governing the conduct of DoD intelligence activities: Annex governing signals intelligence information and data collected pursuant to section 1.7(c) of E.O. 12333, URL: <https://assets.documentcloud.org/documents/20454757/redacted-annex-dodm-524001-a.pdf>

¹⁵⁷ The full list of 'Basic Subscriber Information' is defined in Title 18 of the United States Code (about Crimes and Criminal Procedure), U.S.C 2703(c)(2), *Required disclosure of customer communications or records*.

¹⁵⁸ 18 USC 2703(c)(1) and 18 U.S.C. 2703(d), Record[s] or other information pertaining to a subscriber to or customer of such service.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
	judge, lower standard of proof than for Content Data		
	Emergency requests: voluntary hand-over by providers (in case of imminent danger/death/serious physical injury) ¹⁵⁹		
US CLOUD Act (Clarifying Lawful Overseas Use of Data Act)	Expands the scope of the US Stored Communications Act to data stored outside of the EU, same authority requirements as above	Foreign Intelligence Surveillance Act (FISA) Section 702, limited to queries about non-U.S. persons located abroad. Section 702 no longer allows for the use of keywords. Sunset of FISA Section 702 by the end of 2023	Annual authorisation by the FISA Court (FISC). ¹⁶⁰ FISC has authorized the collection of both metadata and content of communications
Electronic Communications Privacy Act (ECPA), created amendments on the Stored Communications Act and the	Information relating to subscribers of <i>"wire or electronic communication service providers."</i> ¹⁶¹ Signed by a judge <u>or</u>	National Security Letters (FBI) based on ECPA	No prior approval from a judge, when relevant to authorized national security investigations.

¹⁵⁹ 18 U.S.C. 2702(c)(4).

¹⁶⁰ According to the U.S. Department of Commerce most U.S. organizations do not handle data that U.S. intelligence agencies are interested in and therefore do not engage in data transfers that present the type of privacy risks that appear to concern the CJEU. The Annual Statistical Transparency Report for 2020, published by the Office of the Director National Intelligence identifies the following number of Section 702 court orders: 1 in 2018, 2 in 2019 and 1 in 2020, and notes the following estimated number of targets relating to such orders as 164,770 for 2018, 204,968 for 2019 and 202.723 for 2020. Published April 2021, URL: <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020>.

¹⁶¹ 18 U.S.C. 2709, et seq.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
Wiretap Act and created the Pen Register Act.	customer notice of such requests		Can only order access to Basic Subscriber Information, no content or diagnostic data.
Administrative subpoenas or demands (335 U.S. federal agencies)*	Based on the SCA, subject to the requirements described above	Title 1 (traditional) FISA warrant type a: existing account and metadata of U.S. Persons ¹⁶²	Applications to be approved by FISC
Search warrants to search and confiscate evidence, signed by judges based on state or local criminal laws (at least 57 distinct sets of laws ¹⁶³)*	Based on the SCA, subject to the requirements described above	FISA warrant b: future metadata & content (tap) of U.S. Persons.	Applications to be approved by FISC
Judicially issued subpoenas and Grand Jury subpoenas for EU individuals to appear before a US court*	Based on the SCA, subject to the requirements described above	FISA business records order (Section 501, scope limited since 2020, no more 'any tangible thing'), for non-Content Data (Diagnostic Data)	Applications to be approved by FISC

¹⁶² US Congressional Research Service, Foreign Intelligence Surveillance Act (FISA): An Overview, 6 April 2021, URL: <https://crsreports.congress.gov/product/pdf/IF/IF11451>. Applications for 'regular' FISA warrants must include the following: (1) the applicant's identity; (2) information regarding the target's identity if known; (3) why the target may be searched or surveilled; (4) a statement establishing a sufficient relationship between the target and the search location; (5) a description of what will be searched or surveilled; (6) a description of the nature of the information sought or of the foreign intelligence sought; (7) proposed minimization procedures; (8) a discussion of how the search or surveillance will be carried out; and (9) a discussion of prior applications. If electronic surveillance is sought, applications must also discuss the duration of the surveillance. Traditional FISA warrants are issued for US persons, but may lead to the incidental data collection of non-U.S. persons when the U.S. person is the target of the FISA collection because they are suspected to be "a foreign power" or "an agent of a foreign power."

¹⁶³ As mentioned by Professor Vladeck in his expert paper for the German DPAs, p. 10.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
Incoming Mutual Legal Assistance requests filed by EU law enforcement to US Department of Justice Office of the International Affairs		FISA pen registers and trap and trace devices (as expanded by US Patriot ACT from 2015 to internet communications) ¹⁶⁴	Applications to be approved by FISC, no probable cause required

* Some of these law enforcement powers may not apply to data stored outside the United States, both in general and because of the strong presumption U.S. courts apply against the extraterritorial application of statutes.¹⁶⁵

According to its bi-annual reports about government requests for user data, in 2021 Facebook received 123.653 requests from US government authorities for 214.782 accounts (users).¹⁶⁶ Facebook does not specify the location of the users: only the location of the requesting authority. Hence, these statistics do not provide insights how frequently access to personal data from EU or Dutch users was ordered and complied with, or if US authorities have demanded access to raw data relating to visits to a (Dutch government) Page.

Facebook additionally provides statistics about the amount of FISA requests, specifically aimed at non-US citizens. See [Figure 48](#). It appears these statistics are separate from the law enforcement statistics quoted above.

¹⁶⁴ Applications do not require the identity of a suspect, only (1) the identity of the federal officer seeking to use a PR/TT device; (2) the applicant's certification that the information likely to be obtained is foreign intelligence information; and (3) a specific selection term to be used as the basis of the PR/TT device.

¹⁶⁵ As mentioned by Professor Vladeck, with a reference to Supreme Court jurisprudence from 2016, *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2099–100 (2016).

¹⁶⁶ Facebook, Government Requests for User Data, undated, last viewed 15 July 2022, URL: <https://transparency.fb.com/data/government-data-requests/>

Figure 48: Facebook statistics about FISA orders¹⁶⁷**Foreign Intelligence Surveillance Act (FISA)**

The chart below reflects the ranges for FISA requests received during this reporting period. By law we must report this data in ranges and delay the release of data on these requests.

Period	Request type	Total requests	Accounts specified
Jul - Dec 2021	Data subject to 6 month reporting delay	-	-
Jan - Jun 2021	Content Requests	0-499	125,000-125,499
Jan - Jun 2021	Non-Content Requests	0-499	0-499

US Providers are legally prohibited from disclosing the exact amount of orders: they can only report in ranges.

Facebook explains that non-content data are data such as “*name, length of service, credit card information, email address(es), and a recent login/logout IP addresses and other transactional information, not including the contents of communications (for example, message headers and IP addresses).*”

5.4 Joint controllers

According to three judgments of the European Court of Justice¹⁶⁸ parties can factually become joint controllers, even if the roles are unevenly distributed, and also if the party that is the customer does not have access to the personal data processed by the party that supplies a service.¹⁶⁹

Joint controllership needs to be established on a factual basis, and cannot be excluded if there is no contractual arrangement. A supplier cannot legally fix its role by offering unilateral contract terms that specify that it is an independent data controller for all data processing not mentioned in the contract terms.

According to the EDPB guidelines on joint controllership, parties may be considered “joint controllers” when they take a common decision or when they take converging decisions about the purposes and essential means of the processing. The term “converging decisions” is defined as decisions that “*complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing*”. According to the EDPB, an important factor in determining whether there are converging

¹⁶⁷ Idem, bottom of the page, ‘National Security Requests’.

¹⁶⁸ European Court of Justice, C-40/17, 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, C210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. See in particular par. 38-43. Also see: C-25/17, 10 July 2018, Tietosuojaalututettu versus Jehovah’s Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.

¹⁶⁹ See par. 39 of the Schleswig Holstein Fan Page case and par. 69 of the Jehovah’s Witnesses case: it is not necessary that the community had access to the personal data, or to establish that the community had given its members written guidelines or instructions in relation to the data processing.

decisions is whether the two entities' processing activities are "inextricably linked", in the sense that the processing in question *"would not have been possible without both parties' participation" in the processing operations.*"

According to Facebook, it follows from this explanation from the EDPB that joint controllership only applies to the creation of Insights, not to any other data processing by Facebook.

This seems a rather limited interpretation of the joint controller concept in the GDPR. Every visit to a government Page generates a lot of data in Facebook's systems, be it from a user or a non-user (through cookies).

If a government organisation does not create a Page, Facebook would not be able to collect any personal data about the interactions of its users and non-users with this specific government organisation. Facebook's collection of personal data about the individual visitors to the page is inextricably linked to the creation of a Page by a government organisation, even if Facebook only processes some of these observed data as analytics for the Page admin. It is plausible that the government organisation is in fact also a joint controller with Facebook for the invisible and undefined processing of the observed behaviour data about interactions with the Page, and the inferred data, such as an interest in the content shown on the Government Page.

This inextricable link between the creation of a Page and the processing of personal data by Facebook for personalisation purposes, including advertising, is particularly visible in the use of cookies. Facebook sets five tracking cookies in the web browser of visitors that are Facebook users. With regard to non-users, Facebook appears to have recently limited its cookie operations to the setting and reading of a single, data tracking cookie (instead of 5 tracking cookies).

Visitors cannot consent nor opt-out from this data processing when they visit the government Page. Facebook calls these cookies 'essential' cookies, but this does not correlate with the legal exception in the ePrivacy Directive for necessary cookies (See Section 9 of this DPIA). In fact, these cookies enable Facebook to collect information about visits to websites outside of Facebook, even if the user does not have a Facebook account, and does not click on any interaction with a Facebook icon. As described in Section 2.4.1, Facebook was able to correlate visits to the test Page with visits to a large employment agency and an online shop / ecommerce platform by one of the test users. Facebook's commercial raison d'être is the processing of personal data to generate advertising revenue. With the information about visits to the government Page, Facebook is able to enrich the profile of users, and hence improve its targeting algorithms. Facebook would not be able to process these personal data for its own commercial purposes without the initiative from a government organisation to open a Page on the network.

In its reply to the DPIA from the Norwegian DPA, Facebook emphasises that the Schleswig-Holstein court case only qualified Facebook and the Wirtschaftsakademie as a joint controller for the cookies set by the Page, and for the creation of the Page specific statistics. Facebook argues that the court held it is **not** a joint controller for any other data processing resulting from visits to a (government) Page. This looks like a *contrario* reasoning, as the ruling is limited to the facts and the questions raised by the referring court. The case centred around the lack of information provided to the Page visitors about the data processing with cookies. The court did not discuss the other personal data automatically generated and observed by Facebook about visits to a Page.

*"According to the documents before the Court, the data processing at issue in the main proceedings is essentially carried out by Facebook placing cookies on the computer or other device of persons visiting the fan page, whose purpose is to store information on the browsers, those cookies remaining active for two years if not deleted."*¹⁷⁰

(...)

*"While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account."*¹⁷¹

The CJEU explicitly ruled that *"the fact that an administrator of a fan page uses the platform provided by Facebook in order to benefit from the associated services cannot exempt it from compliance with its obligations concerning the protection of personal data."*¹⁷²

In the Fashion ID case, the CJEU nuanced its earlier stance, and ruled that a company or person cannot be qualified as joint controller for subsequent operations for which it does not determine either the purposes or the means. The CJEU found that the use of a Like button on an (external) website enables Facebook *"to obtain personal data of visitors to its website and that such a possibility is triggered as soon as the visitor consults that website, regardless of whether or not the visitor is a member of the social network Facebook, has clicked on the Facebook 'Like' button or is aware of such an operation."*¹⁷³ According to the ruling it is clear that the website operator is joint controller for the collection and disclosure by transmission of the personal data of visitors to its website. However, the website operator with a Like button cannot be qualified as controller for the 'further' processing by Facebook, as it cannot determine the purposes and means of these subsequent operations.¹⁷⁴

In November 2021 the appellate administrative court of Schleswig-Holstein (to whom the 2011 Page case was referred back by the CJEU) issued its ruling. It concluded that the school indeed had to close its Facebook Page, due to violations of cookie and data protection law. The court concluded that the data processing of user data by Facebook as a result of visiting a Page was not based on any legal ground, nor could it be based on consent from the users. In particular, because the data subjects were not sufficiently informed about the data collection and processing purposes that result from the visit to a Page.¹⁷⁵ The court explicitly ruled that Facebook and the Page

¹⁷⁰ CJEU, C-210/16, par. 33

¹⁷¹ Idem, par. 35

¹⁷² Idem, par. 40.

¹⁷³ CJEU, Fashion ID, par. 75

¹⁷⁴ Idem, par. 76.

¹⁷⁵ The title of the press release from the appellate administrative court of Schleswig-Holstein is: *Wirtschaftsakademie ist wegen datenschutzrechtlicher Verstöße verpflichtet, Facebook-Fanpage zu deaktivieren*. 27 November 2021, URL: https://www.schleswig-holstein.de/DE/justiz/gerichte-und-justizbehoerden/OVG/Presse/PI_OVG/2021_10_27_Ausbaubeitrag_hat_Bestand_kopie.html. Text of ruling: Schleswig-Holsteinisches OVG, Urteil vom 25.11.2021 - 4 LB 20/13, URL: <https://openjur.de/u/2383902.html>.

owner were joint controllers for the Page Insights and for the lack of adequate information.

In response to this ruling, the German State DPAs formed a Taskforce Facebook-Fanpages. They concluded on 18 March 2022 that Facebook and Page owners share responsibility to obtain consent from Page visitors for three tracking cookies: *datr*, *c_user* and *fr* from users, and *datr* from non-users. The German DPAs substantiate why Facebook does not obtain this consent. The German DPAs also insist on joint controllership for the collection and further processing by Facebook of Page visitor data, contrary to the ruling of the appellate administrative court that the Page operators would not have an interest in the processing by Facebook for other purposes than showing website analytics.

The German DPAs do identify a commercial interest from organisations in opening a 'free' Page, and reason that Facebook is only able to offer these services for free thanks to advertising, and that this business model is successful thanks to Facebook's massive scale, achieved by network effects. The operators of the Pages benefit from this scale to reach all kinds of specific audiences. The German DPAs conclude: *Thus, both Facebook and the operators of Fan Pages pursue related, complementary purposes of displaying the content of the operators to as many interested parties as possible, as this processing results in a mutual benefit for both.*¹⁷⁶

The German DPAs conclude: *"Even if the OVG's [appellate court] findings on joint controllership fall short of the case law of the ECJ and the German Constitutional Court as outlined above, it is still possible to establish joint controllership for large parts of the data processing by Facebook between the Fanpage operators and the Meta company."*¹⁷⁷ They point out that the appellate court did not assess the position of non-users that have to accept the *datr*-cookie for which consent is required when they visit Pages, without any option to provide or refuse that consent.

As concluded in Section 5.3, if a government organisation cannot legitimately conclude a joint controller agreement with Facebook for the processing of all personal data related to visits to a government Page, (only for the data processing resulting in analytics), the government organisation must have a legal ground for the transfer of all other personal data to Facebook as independent third party. This will be assessed in Section 11 of this DPIA. This assessment included the risk of transfer of personal data to Facebook's headquarters in the USA, and the realistic possibility of disclosure of personal data relating to Page visits to US law enforcement and secret services.

6. Interests in the data processing

This section outlines the different interests of Facebook and government organisations in offering the Page service, and communicating via a government Page. This section does not mention the fundamental data protection rights and interests of data subjects. How their rights relate to the interests of Facebook and the Dutch government is analysed in part B of this DPIA.

¹⁷⁶ Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook - Fanpages, 18 March 2022, translated by Privacy Company, p. 16.

¹⁷⁷ Ibidem.

6.1 Interests of Dutch government organisations

Dutch government organisations have public interest and legal compliance reasons to use a Facebook Page. Citizens have a right to information from the government. Government organisations must actively provide information based on the Open Government Act (WOO).¹⁷⁸ There are 11 principles for government communication, including active awareness raising, interactive policy preparation, available and responsive communication, accessible, comprehensive and adequate information.¹⁷⁹

Following these principles, the government has a strong interest to be present where citizens are, especially online. In view of Facebook's unrivalled reach of almost every Dutch citizen aged 13 years and above, there is also a financial/economic interest to communicate through a 'free' Facebook Page, as opposed to having to reach the same mass audience with expensive public awareness raising campaigns on traditional media such as radio, tv and newspapers.

On the other hand the Dutch government has a legal obligation, a moral interest, and an exemplary role as legislator, to comply with the GDPR and only work with privacy proof third parties.

6.2 Interests of Facebook

Facebook has a strong financial monetisation/economic interest in offering 'free' Pages to professional organisations. The content on these Pages helps to expand the potential audience for Facebook, and the daily interaction time with the network. Facebook does not have altruistic motives, but uses the interactions with the content presented on these pages, in combination with information learned from websites outside of Facebook through cookies, to sell targeted advertisements.

Facebook similarly has a business interest in operating as an independent data controller, to be able to process large amounts of data in flexible systems to develop new services and features.

Facebook has a legal and economic interest to comply with the GDPR and ePrivacy rules. In its financial report over 2021, Facebook dedicates many lines of concern about future business obstacles in the EU.¹⁸⁰ Facebook mentions the word 'transfer' 51 times and GDPR 21 times, in sentences such as: "*The GDPR is still a relatively new law, its interpretation is still evolving, and draft decisions in investigations by the IDPC are subject to review by other European privacy regulators as part of the GDPR's consistency mechanism, which may lead to significant changes in the final outcome of such investigations.*"¹⁸¹

Facebook also describes its financial concerns about the transfer of personal data from the EU to the USA: "*If a new transatlantic data transfer framework is not adopted and we are unable to continue to rely on SCCs or rely upon other alternative means of*

¹⁷⁸ Dutch text of the Wet Open Overheid, URL:

<https://wetten.overheid.nl/BWBR0045754/2022-05-01>, entered into force on 1 May 2022.

¹⁷⁹ Mentioned in guidelines for privacy proof and effective campaigning from the *Dienst Publiek en Communicatie* from the Dutch ministry of general affairs, dated 25 May 2018, p. 6.

¹⁸⁰ Meta Platforms Inc, Form 10-K filed with the United States Securities And Exchange Commission, 3 February 2022, URL: <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf>.

¹⁸¹ Idem, p. 9.

data transfers from Europe to the United States, we will likely be unable to offer a number of our most significant products and services, including Facebook and Instagram, in Europe, which would materially and adversely affect our business, financial condition, and results of operations.”¹⁸² With 307 million users in Europe in the first quarter of 2022, with an annual value of 20 US dollars per users, a withdrawal from Europe would cost Facebook well over 6 billion US dollars annually.

See Section 7 below for more information about data transfers.

7. Transfer of personal data outside of the EU

7.1 Facebook’s factual transfers of personal data to the USA

Facebook systematically transfers personal data from its EU customers to the USA. Facebook explains in its Privacy Policy:

“We share the information that we collect globally, both internally across our offices and data centres, and externally with our partners, vendors, service providers and third parties. Because Meta is global, with users, partners and employees around the world, transfers are necessary for a variety of reasons, including:

- So we can operate and provide the services stated in the terms of the Meta Product you’re using and this Policy. This includes allowing you to share information and connect with your family and friends around the globe.*
- So we can fix, analyse and improve our products.”*

Facebook explains that the personal data can be transferred to any location where Facebook has infrastructure or data centres, where Meta Company Products are available, and other countries where *“partners, vendors, service providers and third parties are located outside of the country where you live, for purposes as described in this Policy.”¹⁸³*

In March 2021, Facebook published a press release why it doesn’t create a European cloud, and what measures it takes to securely transfer the data from EU users to the USA.¹⁸⁴

According to Facebook it cannot split the processing between EU and US silos: *“Our services are designed to be global and are supported by a cutting-edge global infrastructure that’s taken us over a decade to build. Seamless global data transfers are therefore a necessary ingredient for our services to work.”¹⁸⁵*

Contractually, in its role as controller/joint controller for the Pages, Facebook relies on the SCC for the transfer. These SCC, between Facebook [Meta] Ireland as data controller and Facebook [Meta Platforms] Inc in the USA are not publicly available and no copy was requested for this DPIA.¹⁸⁶

¹⁸² Idem, p. 36.

¹⁸³ Facebook Privacy Policy, effective 26 July 2022.

¹⁸⁴ Facebook Press release, ‘Steps We Take to Transfer Data Securely’, 11 March 2021, URL: <https://about.fb.com/news/2021/03/steps-we-take-to-transfer-data-securely/>

¹⁸⁵ Idem.

¹⁸⁶ Facebook, What are Standard Contractual Clauses? URL:

<https://www.facebook.com/help/566994660333381> . Facebook explains that people need to contact Facebook to request a copy of the SCC.

In the March 2021 press release Facebook describes it applies the following supplementary measures to the transfers:

- Encryption of data in transit
- Dynamic security measures to keep ahead of evolving risks and security threats
- No “back door” for any government with direct access or encryption “back doors.”
- Comprehensive policies governing how to evaluate and respond to government requests for user data. “We review each request and only provide information in response to requests that we determine are valid, producing only information that is narrowly tailored to respond to that request.”¹⁸⁷
- Defend users’ rights: “Where necessary, we will challenge or reject unlawful government requests. We would also challenge any order seeking to require us to redesign our systems in a way that would undermine the security we provide to protect people’s data, or that attempted to gag us from disclosing the existence of such an order and our efforts to fight it.”¹⁸⁸
- Publication of bi-annual transparency reports about government requests “it is our policy to notify users of requests for their information prior to any disclosure, unless we are prohibited by law from doing so or in exceptional circumstances when notice would be counterproductive such as when a child is at risk of harm.”¹⁸⁹

7.2 GDPR rules for transfers of personal data

The GDPR contains specific rules for the transfer of personal data to countries outside the European Economic Area (EEA). In principle, personal data may only be transferred to countries outside the EEA if the country has an adequate level of protection. That level can be determined in a number of ways: a multinational may adopt Binding Corporate Rules, apply the (revised) EU Standard Contractual Clauses (SCC) or only transfer to countries for which the European Commission has taken a so-called adequacy decision.

Facebook does not have BCR. Additionally, Facebook cannot rely on Article 49 of the GDPR for its transfers to the USA. This article lists several grounds for transfers to third countries such as consent, or necessity to perform a contract, but these grounds can only be used for incidental transfers, not for structural data transfers. Therefore only the SCC and the adequacy decision are discussed in more detail below.

7.2.1 Standard Contractual Clauses (SCC)

Personal data may be transferred from the EEA to third countries outside of the EEA using SCC (also known as EU model clauses) adopted by the European Commission.¹⁹⁰ The SCC contractually ensure a high level of protection. The European Commission

¹⁸⁷ Facebook Press release, ‘Steps We Take to Transfer Data Securely’.

¹⁸⁸ *Idem*.

¹⁸⁹ *Ibid*.

¹⁹⁰ Based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6794 June 2021, URL:

https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

adopted new SCC in June 2021, as a result of the Schrems-II decision from the Court of Justice of the European Union (See 7.3 below).¹⁹¹

Although the European Court of Justice recognizes the validity of the decision of the European Commission with which it adopted the SCC, and data transfers on the basis of the SCC are therefore still permitted in principle, this validity cannot be assumed for systematic transfers of personal data to the United States.

The fact is that transfers via the SCC also require that the recipient country provides an adequate level of data protection as defined in EU law. Article 46(1) of the GDPR explains that this means that data subjects must have adequate safeguards, enforceable rights and effective legal remedies at their disposal. Whether this is the case, according to the Court, must be determined by the data controllers and cloud providers themselves.

The CJEU writes: *"The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation."*¹⁹²

The EDPB explains that there are four guarantees that make limitations to the data protection and privacy rights as recognised by the Charter justifiable.¹⁹³

These four guarantees are:

1. Processing should be based on clear, precise, and accessible rules
2. Necessity and proportionality concerning the legitimate objectives pursued need to be demonstrated
3. An independent oversight mechanism should exist
4. Effective remedies need to be available to the individual

These criteria are essential guarantees, the EDPB adds, but not sufficient by itself to determine whether the legal regime of the third country offers an essentially equivalent level of protection.

It follows from the Schrems II ruling that the legal regime in the USA, in particular FISA legislation, did not meet these four criteria, for the following reasons:

¹⁹¹ European Commission, Standard Contractual Clauses, URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

¹⁹² European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximilian Schrems (Schrems-II), 16 July 2020, par 104.

¹⁹³ EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020, URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_european_essentialguaranteessurveillance_en.pdf

1. FISA Section 702 and E.O. 12333 do not indicate limitations on the powers they confer to implement surveillance programmes for the purposes of foreign intelligence.

The protection of the Fourth Amendment of the US Constitution, which prohibits “unreasonable searches and seizures” and requires that a warrant must be based upon “probable cause” extends only to US nationals and citizens of any nation residing within the US. According to the US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment.¹⁹⁴

2. US laws permit public authorities to have access on a generalised basis to the content of electronic communications. This must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.
3. The scope of the supervisory role of the oversight mechanism by the US Ombudsman does not cover the individual surveillance measures. It is doubtful whether the US Ombudsman meets the other elements for independence defined by the European Court of Human Rights in its jurisprudence about surveillance measures, such as independence from the executive, being vested with sufficient powers and competence and whether its activities are open to public scrutiny.
4. Closely related to the third guarantee, data subjects from the EU whose data are transferred to the USA cannot bring legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data.

While FISA Section 702 orders can theoretically be challenged by non-US persons through civil actions under the Administrative Procedure Act, it is very unlikely that such individuals are informed that their data have been accessed. Without such a notice, individuals don't know, and cannot seek redress.¹⁹⁵ Additionally, in order to obtain ‘standing’ in a US court, a data subject must provide ‘injury in fact’, a high hurdle when it comes to secret surveillance.¹⁹⁶

7.2.2 *European Commission Adequacy decision*

An adequacy decision means that the country in question has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea,

¹⁹⁴ Quote from the Ad-Hoc-EU-US Working Group on Data Protection, quoted by Ian Brown and Douwe Korff in their study about transfers for the LIBE committee of the EP.

¹⁹⁵ *Idem*.

¹⁹⁶ See for example JD Supra, US Supreme Court Clarifies Injury-in-Fact Plaintiffs Must Show To Have Standing To Assert Statutory Privacy Rights in Federal Court, 14 July 2021, URL: <https://www.jdsupra.com/legalnews/us-supreme-court-clarifies-injury-in-9824522/>

Switzerland, the UK and Uruguay.¹⁹⁷ The adequacy decision for (some transfers under the Privacy Shield to) the USA is no longer valid since the summer of 2020. There is a possibility a new third transatlantic data agreement will be signed between the EU and the USA in 2023. This is discussed in more detail below, in Section 7.3.

7.3 Legal obstacles data transfers to the USA

Facebook's data transfers to the USA are the root cause of ongoing legal debate about the differences in the legal guarantees for privacy protection between the EU and the USA. Due to court cases instigated by the Austrian lawyer Max Schrems against the Irish Data Protection Commissioner, the European Court of Justice has twice invalidated adequacy decisions from the European Commission determining that the level of data protection in the USA was adequate for data imported from the EU.

In the first case, in 2015, the Safe Harbor agreement between the EU and the USA was invalidated. On 16 July 2020, the CJEU ruled that its successor, Privacy Shield, was no longer valid either, with immediate effect.¹⁹⁸ As quoted above, the court cited as the main reasons that the restrictions on privacy arising from the U.S. regulations were insufficiently defined and disproportionate and therefore constituted too great an invasion of privacy.

In both procedures, Facebook legally objected against any attempt to limit the transfers.

On 25 March 2022, President Joe Biden and European Commission President Ursula von der Leyen signed an agreement 'in principle' to work out legal measures to ensure adequate protection of the data in the USA. On 7 October 2022, Biden signed a new Executive Order implementing this agreement with new binding safeguards for the data collection by US intelligence agencies, and introducing a new redress procedure.¹⁹⁹ Following this EOP, the European Commission will prepare a new draft adequacy decision.²⁰⁰ The Commission must ask the EDPB for an Opinion, obtain a green light from a committee with representatives of the EU Member States, and process the input from the European Parliament. A possible new adequacy decision is not expected before March 2023.

In the meantime, Facebook will have to rely on SCCs to legitimise the transfer from the EU to third countries. In its annual financial report over the fiscal year 2021, Facebook provides a summary of its battle with the Irish DPC (the lead data protection

¹⁹⁷ European Commission, Adequacy decisions, URL last visited 28 January 2022: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

¹⁹⁸ European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximillian Schrems (Schrems-II), 16 July 2020.

¹⁹⁹ Executive Order of the President, Enhancing Safeguards for United States Signals Intelligence Activities, URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>.

²⁰⁰ Press release European Commission, Questions & Answers: EU-U.S. Data Privacy Framework, 7 October 2022, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

authority for Facebook in the EU) about the validity of the Standard Contractual Clauses (SCC) after the 2020 CJEU ruling.²⁰¹

Facebook writes:

*"For example, the CJEU considered the validity of SCCs as a basis to transfer user data from the European Union to the United States following a challenge brought by the Irish Data Protection Commission (IDPC). Although the CJEU upheld the validity of SCCs in July 2020, our continued reliance on SCCs will be the subject of future regulatory consideration. In particular, in August 2020, we received a preliminary draft decision from the IDPC that preliminarily concluded that Meta Platforms Ireland's reliance on SCCs in respect of European user data does not achieve compliance with the GDPR and preliminarily proposed that such transfers of user data from the European Union to the United States should therefore be suspended. Meta Platforms Ireland challenged procedural aspects of this IDPC inquiry in a judicial review commenced in the Irish High Court in September 2020. In May 2021, the court rejected Meta Platforms Ireland's procedural challenges and the inquiry subsequently recommenced. We believe a final decision in this inquiry may issue as early as the first half of 2022."*²⁰²

In February 2022 the Irish DPC sent a (renewed) draft decision to Facebook. According to media publications, the DPC once again decided that the SCCs were not valid, and Facebook was allegedly ordered to suspend the data transfer to the USA.²⁰³

On 7 July 2022 the DPC presented its final decision about Facebook's transfer to the other concerned data protection authorities in the EU. According to the US news source Politico the DPC formally prohibits Facebook from transferring personal data from EU citizens from Ireland to the USA.²⁰⁴ Depending on the response from the other data protection authorities in the EU, it may take up to 6 months before this decision becomes final. This estimate is based on the process and timeline previously followed by the EDPB after the DPC proposed a decision about WhatsApp, and many authorities objected that the decision did not sufficiently address all GDPR infringements. The EDPB decided to increase the proposed fine from 30-50 million euro to 225 million euro.²⁰⁵

²⁰¹ Meta Platforms Inc, Form 10-K filed with the United States Securities And Exchange Commission, 3 February 2022, URL: <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf>.

²⁰² Idem, p. 36.

²⁰³ TechCrunch, Meta sent a new draft decision on its EU-US data transfers, 21 February 2022, URL: <https://techcrunch.com/2022/02/21/dpc-meta-draft-data-transfers-decision/>

²⁰⁴ Politico, Europe faces Facebook blackout, 7 July 2022, URL: <https://www.politico.eu/article/europe-faces-facebook-blackout-instagram-meta-data-protection/>

²⁰⁵ The Irish DPC shared its draft decision with other concerned supervisory authorities on 24 December 2020; the EDPB took a binding decision on 28 July 2021. See: press release EDPB, EDPB adopts Art. 65 decision regarding WhatsApp Ireland, 28 July 2021, URL: https://edpb.europa.eu/news/news/2021/edpb-adopts-art-65-decision-regarding-whatsapp-ireland_en. Binding decision EDPB: https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf. Final decision Irish DPC 2 September 2021: <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>.

This development could lead to a possible ban in the EU on the use of Facebook and/or a withdrawal from Facebook from Europe. Additionally, the EDPB is working on guidelines for social media use by public sector institutions.²⁰⁶ These guidelines may advocate suspension of the use of Pages by public sector institutions as long as visitor data are transferred to the USA. The French DPA CNIL has already suspended its own Facebook Page.

As the negative transfer assessment of the Irish DPC is not yet publicly available, this DPIA does not contain a separate DTIA. Based on the currently available information, the risk of the ongoing structural transfer of personal data of Page visitors has to be qualified as high. Though the visitor data are encrypted in transit, and Facebook uses pseudonymous identifiers, both as user identifiers and in tracking cookies, Facebook stores the personal data in readable format. Facebook is able to use the personal data to rank the contents in each individual News Feed and show targeted advertising. Hence Facebook is technically able to comply with an order from government authorities to disclose the transferred personal data in plain text. As described in Section 5.3.1, Facebook receives a high amount of US government orders for personal data from its users, 123.653 requests from US government authorities for 214.782 accounts (users) in 2021, plus FISA orders for approximately 125.000 non US users in the first half of 2021.

As outlined in Section 2.6.2 Facebook can infer special categories of data about individual visitors (users and non-users) to a government Page, for example if the information relates to specific health conditions or sexual orientation, and if the visitor shares information by liking a post with such information. Even if Facebook no longer allows advertisers to select target audiences based on such special categories of data, Facebook does not exclude its own use of such inferences to produce recommendations and in the ranking of content in the News Feed. If Facebook were obliged to disclose any such sensitive or special categories of data to US government authorities, there are obvious high data protection risks for the data subjects.

As a result of the CJEU ruling, and the assessment that the US legal regime does not meet the four essential guarantees, even the mandatory disclosure of 'regular' account data of users that visited a government Page has to be treated as high risk data processing. A theoretical example: if US authorities demand a file of all visitors to a specific government Page, and one of the visitors is flagged as suspect of terrorist activities (based on for example interest in military targets), without being informed, and without adequate legal means to properly defend themselves in possible US legal proceedings, the impact on the visitor can be very high.

8. Techniques and methods of the data processing

As explained in Section 2 of this report, Facebook collects and generates personal data about visits to government Pages in three ways. First, if users interact with content on the Page, through direct visits to the Page, or through posts shown in their News Feed. Second, through observation of their interactions with the Page, and third, by inferring interests based on a combination of the first two categories of data. Facebook applies machine learning to rank the contents of the News Feed and infer advertising interests. Section 8.1 provides a summary of the technology used by Facebook to rank and profile users. Section 8.2 describes the nature of big data

²⁰⁶ The Dutch DPA told a journalist about these upcoming guidelines, not yet mentioned on the EDPB website. Source: <https://www.agconnect.nl/artikel/gemeenten-hebben-geen-benul-van-data-doorgifte-aan-vs>.

processing by Facebook, to better understand Facebook's challenges when retrieving all personal data in reply to a data subject access request.

8.1 Machine learning

In a presentation for the OCP Summit 2019, Facebook engineer Whitney Zhao explained how Facebook uses Machine Learning, or Artificial Intelligence, to generate the contents of users' home Pages.²⁰⁷

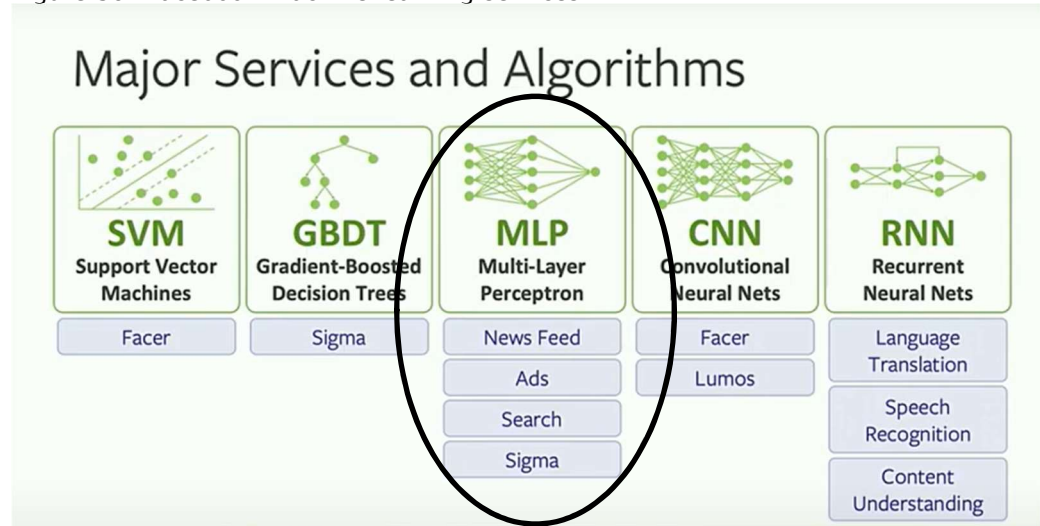
In the presentation Mrs. Zhao explained how the interests of users are inferred based on machine learning. Interactions of users with content through likes, shares and clicks are put into a model to generate predictions of their interests, to show them the content and ads they are most likely to be interested in. This is an iterative process: the performance of the model is tested, the results evaluated and fed back into the system to train the system.

Figure 49: Slide from Facebook engineer Zhao about Machine Learning



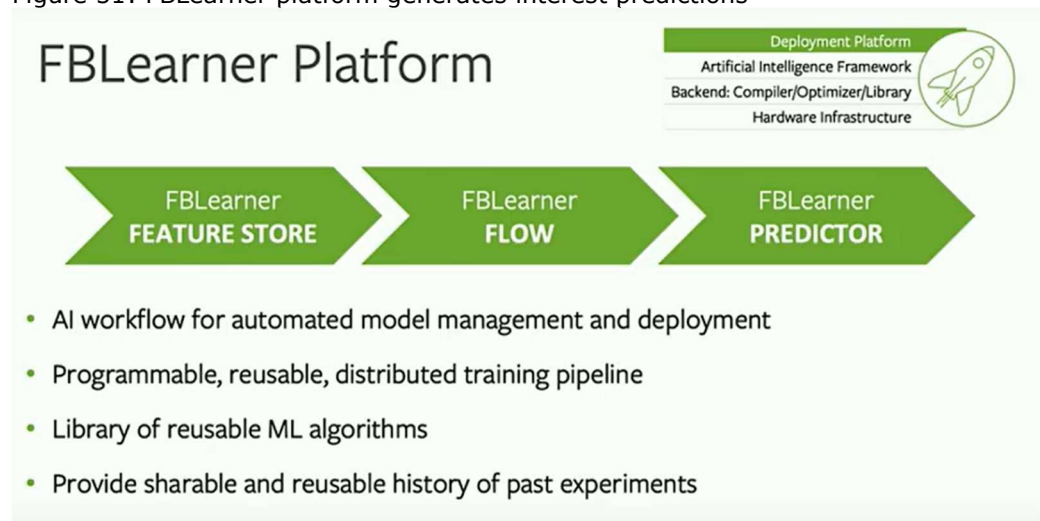
To show contents in the *News Feed*, to select the ads, rank the search results and detect spam and malware with a system called Sigma, Facebook uses Multi-layer Perceptron (MLP). See [Figure 50](#) below. This is an artificial neural network that is used to predict data points. MLP is based on deep learning, also called Deep Neural Networks.

²⁰⁷ Video of presentation Whitney Zhao at OCP Summit 2019 at YouTube, URL: <https://www.youtube.com/watch?v=MYICesArTWk>

Figure 50: Facebook machine learning services²⁰⁸

The MLP is part of Facebook's AI ecosystem. Mrs. Zhao explained how Facebook engineers without in-depth AI knowledge can access the MLP, through a platform called FBLeaer that generates the content of the *News Feed* and ads.

Figure 51: FBLeaer platform generates interest predictions



8.2 Big Data Processing

With data about 2.85 billion monthly active users, Facebook is at the forefront of Big Data processing.

To manage the Big Data, Facebook uses all kinds of open and closed source database tools to manage the different components and microservices. Such as MySQL, Apache Hadoop, HBase, Hive, Apache Thrift and PrestoDB. All these are used for data

²⁰⁸ Idem.

ingestion, warehousing and running analytics.²⁰⁹ The Hive/Hadoop cluster at Facebook stores more than 2 petabyte of uncompressed data and routinely loads 15 terabyte of data daily.²¹⁰

In the ongoing Californian consumer privacy court case, the plaintiffs are trying to get full information about, and access to, all personal data processed about them for advertising purposes. According to a news article in Tech Crunch, this information was *"extracted like blood from a stone via a tortuous, multi-year process of litigation-triggered legal discovery."*²¹¹

In this context, Facebook has explained how it currently technically collects and processes personal data to show targeted advertisements.

Facebook has two main data pipeline systems for data analysts to access the Diagnostic Data: Dataswarm and FBLeaRner. These two pipeline systems access large datasets made accessible in Hive. FBLeaRner is a *deep learning* neural network. Facebook calls this its *AI backbone*.²¹²

Facebook writes: *"The majority of batch data processing of Hive data at Meta is handled by a system called Dataswarm, which is described below. The remaining minority of batch data processing is coordinated by FBLeaRner, which is a similar system derived from Dataswarm."*²¹³

Facebook explains to the court why it cannot reproduce how specific ads were shown to the plaintiffs, because tasks are performed automatically in Dataswarm on a very big scale. On a given day in February 2022, 5 million tasks were performed. Facebook writes it requires a time intensive manual process to find out how inputs (user actions) are translated into outputs (ads and ranking of content in the *News Feed*). That is why Facebook could only produce a sample of 10 tasks in a given timeframe.

Facebook writes: *"Dataswarm works by having employees (1) define atoms of computation called tasks and then having employees (2) explicitly state the dependency relationships between these tasks so that the system can initiate a task's computations after the preceding tasks have completed their execution. These tasks are treated as black boxes: the system knows nothing about what the task does beyond the rough type of computation performed. For any given task, Dataswarm does not know what data is used as inputs to the computations it orchestrates or what data is produced as outputs by these computations. Facebook's current approach for identifying what data is consumed as inputs by a job and is generated as outputs by*

²⁰⁹ Blog post Shivang, Facebook Database [Updated] – A Thorough Insight Into The Databases Used @Facebook, URL: <https://www.scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/>

²¹⁰ <https://www.facebook.com/notes/10158790010637200/>

²¹¹ Techcrunch, Unsealed docs in Facebook privacy suit offer glimpse of missing app audit , 16 September 2022, URL: <https://techcrunch.com/2022/09/16/unsealed-docs-in-facebook-privacy-suit-offer-glimpse-of-missing-app-audit/>

²¹² Facebook blog post, Introducing FBLeaRner Flow: Facebook's AI backbone, 9 May 2016, URL: <https://engineering.fb.com/2016/05/09/core-data/introducing-fblearner-flow-facebook-s-ai-backbone/>

²¹³ Facebook Inc Consumer Privacy User Profile litigation at the United States District Court Northern District of California, Case no. 3-18-MD-02843-VC, Document 913, Exhibit 41.

*that job is a time-consuming manual process. Because Dataswarm performs millions of tasks each day, it is not possible to complete this manual process for all Dataswarm tasks. To respond to the Special Master's request, Facebook completed this manual process for a sample of 10 tasks run in Dataswarm on February 15, 2022. This sample is attached Exhibit D. Approximately five million Dataswarm tasks were run on February 15."*²¹⁴

Facebook not only uses direct user actions, such as liking a post, but also relies on the social graph to predict interests. The social graph is stored in a distributed data store called TAO (abbreviation of *The Associations and Objects*).

Objects are friendships between users, while the relationship between users is an *association*. Each object in the database has an id and type. Each association contains the object IDs, as well as the type of association (such as friendship). Each association has a timestamp that can be used for querying.

Facebook explains: "TAO (*The Associations and Objects*) (...) is the primary source from which Graph API pulls data (including user data). TAO is a high performance service for storing, caching, and querying the graph for nodes and associations, by providing a clean interface for internal and external developers to integrate into the social graph, abstracting away many of the complexities of developing and maintaining a data storage at scale (...)." ²¹⁵

"MySQL: MySQL is TAO's backbone. It provides transactional and availability properties to columnar data. For example, a user's comment can be stored in a MySQL database as a row in a table, where the comment id is the primary key and the comment is a text field. As another example, the fact that someone liked a comment can be represented by an association with the type like from the comment id and the user id, this could be represented as 3 columns in the table, with comment id, user id, and type of reaction." ²¹⁶

While MySQL-databases normally function with explicitly-defined data models (tables with well-defined columns and indexes and constraints), TAO consists of an abstraction on top of the MySQL data. This allows for efficient processing of less well-defined data if they fit in the model. The design of both the Dataswarm and TAO is aimed at flexibility instead of using a well-defined structure of data as common in more conventional databases.

The scale and complexity of Facebook's data processing cause at least two obstacles when providing access to an individual's personal data: a lack of overview of the data due to the scale, and the difficulty to query complex systems.

The amount of data is the most obvious obstacle. To search through a database table without a proper index to find all occurrences of personal data of a specific data subject requires searching through all the rows in the table. The computational effort to perform such a search grows proportionally to the size of the database. Meaning: twice as much data will take twice the amount of computational effort to search through given the same infrastructure to perform the search. Often organisations that

²¹⁴ Idem.

²¹⁵ Ibid.

²¹⁶ Ibid.

are used to process large volumes of data have infrastructure in place to increase the processing capabilities.

The second factor is complexity. Large organisations can work with a large collection of different data models where some might be changed over time. In practice organisations can lose track of what data is being processed where. According to a publication in the US American news source Motherboard (by Vice), Facebook engineers are quoted saying *"We do not have an adequate level of control and explainability over how our systems use data"*.²¹⁷ Vice quotes from an alleged internal Facebook memo.²¹⁸ Privacy Company was not able to verify this statement, as Facebook did not provide access or more information about the raw data it processed relating to the use of the Ministry of Privacy test page.

However, in the Californian class action, two Facebook engineers more or less confirmed this lack of control. *"I don't believe there's a single person that exists who could answer that question," replied Eugene Zarashaw, a Facebook engineering director. "It would take a significant team effort to even be able to answer that question."* When asked about how Facebook might track down every bit of data associated with a given user account, Zarashaw was stumped again: *"It would take multiple teams on the ad side to track down exactly the — where the data flows. I would be surprised if there's even a single person that can answer that narrow question conclusively."*²¹⁹

When complexity is an issue when responding to a data subject access request, a compromise can often be found if the data controller is willing to provide an overview of the available data and systems and allows to the data subject to further specify the request. As described in [Section 2.5](#), Facebook was not willing to provide such an overview.

9. Additional legal obligations: e-Privacy Directive

This section only describes the additional obligations arising from the current ePrivacy Directive and (possible) future e-Privacy Regulation. In view of the limited scope of this DPIA, other legal obligations or frameworks (for example in the area of information security, such as BIO, or in the area of platform regulation, such as the new European Digital Services Act) are not included in this report.

Article 5(3) of the current ePrivacy Directive contains a consent requirement for cookies (information set and read on an end users' device). This provision was transposed in Article 11.7a of the Dutch Telecommunications Act. Consent is required prior to the reading from or placing of information on the devices of end-users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or the necessity for the technical transmission of information. The Dutch implementation

²¹⁷ Vice, Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document, 26 April 2022, URL: <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>.

²¹⁸ Facebook internal document, ABP Privacy Infra, Long Range Investments [A/C Priv], URL: <https://www.documentcloud.org/documents/21716382-facebook-data-lineage-internal-document>.

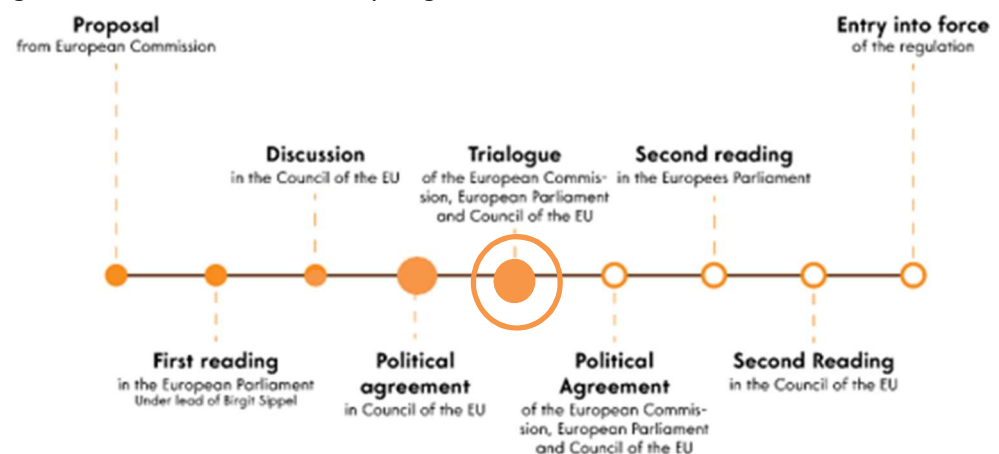
²¹⁹ Paragraph quoted from The Intercept, Facebook engineers: We Have No Idea Where We Keep All Your Personal Data, 7 September 2022, URL: <https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/>.

contains a legal assumption that *tracking cookies* (used across multiple services of the information society) involve the processing of personal data, and hence, the GDPR applies. As analysed in Section 2.4 of this report, Facebook places and retrieves unique identifiers in five different tracking cookies in the browsers of users, and at least one tracking cookie (the datr cookie) in the browser of non-users when they visit a government test Page. These cookies are also set and read by external websites, even if the users do not click on any Facebook icon on such an external website. Facebook requires all government Page visitors to accept these 'Essential' cookies without an option to refuse (users and non-users).

The consent requirement for tracking cookies will likely continue to exist in the future ePrivacy Regulation. As illustrated in [Figure 52](#), the process started with a proposal published by the European Commission in January 2017.²²⁰

This was followed by an intense political debate the last five and a half years. The European Parliament responded quickly and positively, but it has taken the representatives of the EU Member States three years to draft a compromise about the proposed ePrivacy Regulation. The Council sent its agreed position to COREPER to start the trialogue on 10 February 2021.²²¹ The trialogue is ongoing since. The last publicly available update from the Council dates from 28 March 2022, in which the proposed compromises are all blacked out.²²²

Figure 52: Process new ePrivacy Regulation



The points of view of the European Parliament and the European Council are widely diverging. Therefore, it is not likely that the ePrivacy Regulation will enter into force anytime soon. Hence Facebook will have to comply with the current ePrivacy rules in the next few years.

²²⁰ European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017 COM(2017) 10 final, URL: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>.

²²¹ Council of the European Union, Interinstitutional File 2017/0003(COD), Brussels, 10 February 2021 (OR. en) 6087/21, URL: <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>.

²²² French presidency, preparation for trialogue, 7458/22, 28 March 2022, URL: <https://data.consilium.europa.eu/doc/document/ST-7458-2022-INIT/x/pdf>.

10. Retention periods

Facebook's Privacy Policy does not mention specific retention periods. Facebook informs users that it *"keep(s) information as long as we need it to provide our Products, comply with legal obligations or protect our or other's interests. We decide how long we need information on a case-by-case basis."*²²³

Facebook mentions factors that help determine the different (unspecified) retention periods, such as the feature the retained data are used for, or a legal obligation, or when necessary for other legitimate purposes, or when individual data are preserved for a longer period of time, in case of investigations/complaints and litigation.

Facebook has explained to the Californian court that Diagnostic Data in the Hive database system are retained indefinitely. They cannot be deleted, though the unique user ID is deleted after 90 days, to be replaced with a unique Replacement ID (RID).

As quoted in Section 2.1.2 Facebook writes: *"In data systems that do not support deletion (e.g. Hive), any user data retained for more than 90 days can only be retained with an RID."*²²⁴

Facebook also described in this court case that it retains data about the ads shown to each individual user since the log was created in 2007, hence, currently already for a period of 15 years (See Section 2.5.2).

Facebook also explained that such RIDs are deleted after a user has deleted his or her account. *"When a user deletes her account, Facebook deletes the record connecting the UserID to the RID so that data stored with that RID can no longer be connected to that user."*²²⁵ Facebook can be used by any user worldwide since September 2006. That means the oldest identifiable data with RID may cover a period of almost 16 years. Facebook does not appear to have an active data retention policy for inactive account. Facebook writes it may disable or delete unused accounts, if they remain inactive for an unspecified 'extended' or 'long' period of time.²²⁶

Factually, deletion of a user account takes 30 days. Facebook calls this the 'grace period', for users to change their mind and cancel their request.²²⁷

²²³ Facebook Privacy Policy, effective 26 July 2022.

²²⁴ Facebook Inc Consumer Privacy User Profile litigation at the United States District Court Northern District of California, Case no. 3-18-MD-02843-VC, Document 913, Exhibit 41.

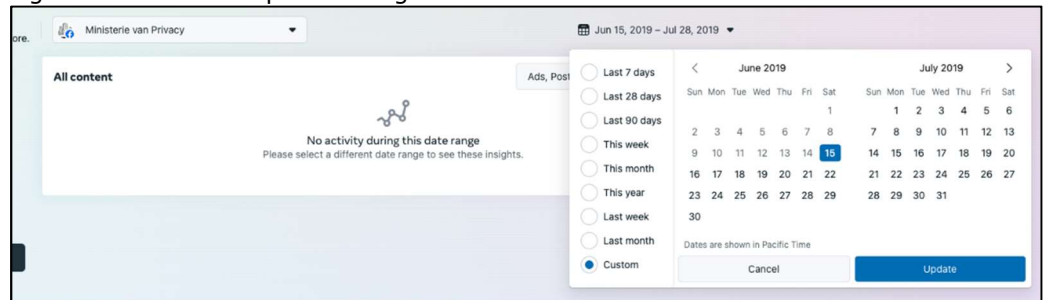
²²⁵ Ibid.

²²⁶ Facebook writes it **may** disable or delete an account (...) *"if the account is unused and remains inactive for **an extended period of time**".* In a further explanation in a drop down menu Facebook explains: *"We may disable and delete accounts that are unused and remain inactive for a **long period of time**. We look at several signals to understand whether your account is unused, including whether you've recently logged in to your account or into another service using your Facebook account. We also take into consideration prior activity on your account such as whether you've added any photos or friends, or followed any Pages."* Source: Facebook, 'Facebook's policies on disabling or deleting hacked, unused or unconfirmed accounts', URL: <https://www.facebook.com/help/3434203120011796>.

²²⁷ Wersm, Facebook Extends Its Account Deletion Grace Period To 30 Days, 7 October 2018, URL: <https://wersm.com/facebook-extends-its-account-deletion-grace-period-to-30-days/>.

As shown in [Figure 53](#) below, Facebook’s default retention period for Insights is 3 years and 1 month. As the test page was not yet active 3 years ago, there is no activity at the earliest date that could be selected.

Figure 53: Retention period Insights²²⁸



[Table 2](#) in page 60 shows the intended retention period of Facebook cookies in the browser of a Page visitor. These retention periods are dynamic: every time a Page is visited, the cookie is updated, and the retention period refreshed. As described above, Facebook retains the pseudonymised user identifiers in its own databases for an indefinite period of time.

²²⁸ Data accessed on 15 July 2022.

Part B. Lawfulness of the data processing

The second part of the DPIA assesses the lawfulness of the data processing. This part contains a discussion of the legal grounds, an assessment of the necessity and proportionality of the processing, and of the compatibility of the processing in relation to the purposes.

11. Legal Grounds

To be permissible under the GDPR, the processing of personal data must be based on one of the grounds mentioned in Article 6 (1) GDPR. Essentially, for processing to be lawful, this article demands that the data controller bases the processing on the consent of the user, or on a legally defined necessity to process the personal data.

The appropriate legal ground depends on Facebook's role as (joint) controller, or as processor.

As described in Section 1.2, Facebook processes four categories of personal data

1. Data collected from user activity on a government Page
2. Data collected from user activity outside of Facebook
3. Data inferred from user activity related to content on a government Page (including cookies from third parties)
4. Data collected from non-users when visiting a (public) government Page.

The second category of personal data is not relevant for this DPIA about the processing of data related to the visits to a government Page.

As described in Section 4.2, Facebook permits itself to process collected and inferred personal data for 15 different purposes. Facebook additionally aggregates some of these personal data to provide Insights to the government Page administrators.

In its privacy policy, Facebook mentions all six available legal grounds for different purposes of the processing. Facebook explains: *"We rely on different legal bases to process your information for the purposes described in this Privacy Policy. Depending on the circumstances, we rely on different legal bases when processing your same information for different purposes."*²²⁹ Per legal ground, Facebook offers a long table with purposes, and types of personal data to achieve the purpose. These purposes often overlap. For example, Facebook invokes contract, consent and legitimate interest for the purpose of personalising its products/services. The differences between the three legal grounds are very subtle: consent is invoked for the processing of *'information with special protections'*. According to Facebook this concerns information actively provided by users as part of their profile, as well as information from Partners, vendors and third parties about activities off Facebook, also from non-users. Facebook invoked the legal ground of contract to use any other information to personalise the content, including browser and device information, as well as information from Partners, vendors and third parties about activities off Facebook, with the exception of identifying data provided by these third parties. The legitimate interest ground is invoked with regard to minors *who have a limited ability to enter*

²²⁹ Meta Privacy Policy, What is our legal basis, URL:

<https://www.facebook.com/privacy/policy/?subpage=7.subpage.1-WhatIsOurLegal>

into an enforceable contract for all data, for all types of personalisation and advertisements.²³⁰

Facebook also invokes consent, contract and legitimate interest (in relation to minors) to “undertake analytics” as well as a legitimate interest in relation to all people including minors, to “provide aggregated user analytics and insights reports to businesses, advertisers and other Partners”.

The assessment of available legal grounds is tied closely to the principle of purpose limitation. The EDPB notes that “*The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation. [...] When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes.*”²³¹

Thus, in order to determine whether a legal ground is available for a specific processing operation, it is necessary to determine for what purpose, or what purposes, the data was or is collected and will be (further) processed. There must be a legal ground for each of these purposes.

To better understand the possible legal grounds, this analysis describes four possible legal grounds for the personal data directly observed and indirectly inferred as a result of visits to a government Page. Additionally, a second paragraph describes the legal ground for the data processing for Insights, for which Facebook offers a joint controller agreement.

Two of the six available legal grounds (vital interest and legal obligation) do not appear to be relevant for this DPIA.

Facebook states it can rely on the legal ground of the protection of the vital interests of data subjects, including to detect, remove, and report illegal content.²³² This legal ground is not relevant in view of the type of content published by government organisations on Facebook Pages. In 2023 the Digital Services Act²³³ will create a

²³⁰ Idem, pop-up Information from Partners, vendors and third parties, URL:

<https://www.facebook.com/privacy/policy/?subpage=1.subpage.4-InformationFromPartnersVendors>

²³¹ EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

²³² This is dubious, as use of this legal ground should be limited to life-or-death situations. See recital 46 GDPR: “*Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis.*” Scanning content data to remove and report alleged illegal content involves high data protection risks for data subjects, and is prohibited by law under the ePrivacy Directive. The EU has created a specific legal exception for this type of data processing (Regulation (EU) 2021/1232 of 14 July 2021) and is in the process of creating a dedicated Act to regulate specific types of illegal content detection and reporting, in addition to the rules for illegal content detection and removal described in the DSA.

²³³ Digital Service Act, provisional version adopted after Trialogue, Dossier interinstitutionnel:

legal obligation for very large online platforms such as Facebook to analyse systemic risks, remove illegal content, and enable access to personal data to vetted researchers. However, Facebook cannot anticipate on these future legal obligations to allow itself to process personal data for research purposes.²³⁴

With regard to other possible legal obligations, Facebook may be subjected to legislation in third countries (notably the USA) to disclose observed and inferred data to government authorities. Absent a mutual legal assistance treaty between the EU and such a third country (notably the USA where all of Facebook's personal data are ultimately processed), Facebook contravenes the GDPR when it complies with an order to disclose personal data relating to Dutch visitors of a government Page.

The analysis below of the four remaining legal grounds is informed by the reasoning in the recent Opinion from the Advocate General of the Court of Justice of the European Union in the case of Meta Platforms against the German competition authority.²³⁵ It is also informed by the November 2021 ruling from the German appellate court in the famous Schleswig-Holstein Fan Page court case that Facebook cannot invoke any legal ground for its current data processing, in particular as a result of the use of cookies for which consent is required.

11.1 Data observed and inferred from visits to a government Page

As data controller for the processing of personal data collected directly and indirectly when persons with a Facebook account visit a government Page, Facebook mostly relies on the legal ground of contract to personalise the *News Feed* and show icons from 'similar pages' on a government Page. This includes data inferred from user activity on and outside of Facebook, based on interactions with the content of a government Page (including processing as a result of the mandatory acceptance of tracking cookies).

11.1.1 Consent

As quoted in the introduction of this Section 11, Facebook relies on explicit consent for the processing of special categories of data, such as data about health, sexual preferences or religious beliefs.

Dutch government Pages may contain information that may reveal sensitive information about the visitor, ranging from health information to political views, and from sexual orientation to ethnic background. Facebook users are not asked to provide explicit consent to Facebook for profiling and personalisation based on these data (including the use of cookies to show personalised content outside of Facebook), since Facebook only asks for explicit consent for data a user actively provides as visible content in his or her profile.

2020/0361(COD), 15 June 2022, URL: <https://data.consilium.europa.eu/doc/document/ST-9342-2022-INIT/x/pdf>. See in particular articles 26 and 31.

²³⁴ The exception made by the European Commission in July 2021 on the ePrivacy Directive for webmail and messenger services to scan for child sexual abuse material lifts the generic prohibition on the scanning of content data, but does not create a legal obligation. Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1232>

²³⁵ Opinion AG CJEU, Meta Platforms Inc., formerly Facebook Inc., v Bundeskartellamt, C-252/21, 20 September 2022, ECLI:EU:C:2022:704.

It follows from the AG Opinion for the CJEU that Facebook's definition of special categories of data is too limited, and should include information that *emerges* from liking or sharing content from government Pages, when such information is linked to the Facebook account data, and **can** be used for profiling.

The AG writes: "(...) *I doubt whether it is relevant (or always possible) to distinguish between the data subject merely being interested in certain information and the data subject belonging to one of the categories covered by the provision in question. Although the parties to the main proceedings have opposing views in that regard, I believe the answer to that question must be sought on a case-by-case basis and with regard to each of the activities comprising the practice at issue.*

Although, as the German Government points out, simply collecting sensitive personal data about the visit to a website or an app is not, in itself, necessarily the same as processing sensitive personal data within the meaning of that provision, linking the data to the relevant user's Facebook account or using the data could, on the other hand, both easily amount to such processing. The decisive factor for the purpose of applying Article 9(1) of the GDPR is, in my view, whether the data processed allow user profiling based on the categories that emerge from the types of sensitive personal data mentioned in that article."²³⁶

The AG concludes: "Article 9(1) of the GDPR must be interpreted as meaning that the prohibition on processing sensitive personal data may include the processing of data carried out by an operator of an online social network consisting in the collection of a user's data when he or she visits other websites or apps or enters such data into them, the linking of such data to the user account on the social network and the use of such data, provided that the information processed, considered in isolation or aggregated, make it possible to profile users on the basis of the categories that emerge from the listing in that provision of types of sensitive personal data."²³⁷

The AG also refutes the argument from Facebook that users would make such sensitive information **manifestly public** (Art. 9 (2) sub e GDPR), as they only want to share this information with a self-chosen specific audience, not with the general public.

Additionally, though Facebook users that visit a government Page are asked to provide consent for tracking cookies, this consent is invalid. As described in Section 2.4.1. Facebook sets and reads tracking cookies when a user chooses to reject tracking cookies, and selects 'essential cookies'. In using the datr cookie, Facebook manifestly acts against the expressed intent of the Page visitors. Additionally, Facebook sets unique device identifiers in the device of the Facebook user. Even if the Facebook user logs out (for example, if he or she wants to visit a government Page with information that might reveal sensitive characteristics), Facebook does not remove these unique identifiers, and continues to collect information.

Last but not least, as shown in [Figure 30](#) and [Figure 31](#), if external websites ask for consent for tracking cookies, they do not ask for *explicit* consent to allow Facebook to process sensitive data from these websites for advertisements on those and other external apps and websites.

²³⁶ Idem, par. 37-39.

²³⁷ Opinion AG CJEU, C-252/21, par 38.

In sum, Facebook is legally required to obtain explicit consent for the processing of special categories of data, as these characteristics can be inferred from surfing and social engagement behaviour. Facebook is legally required to obtain consent for the use of tracking cookies, both with regard to users and non-users. Facebook does not ask for consent for tracking cookies, and does not ask for explicit consent, though it cannot rely on one of the other legal exceptions in Article 9 GDPR for the processing of special categories of data.

11.1.2 Contract

Article 6 (1) (b) GDPR reads: “processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.”

Facebook relies on a contract for the use of the services. Users accept Facebook’s terms of service when they click on the ‘Sign up’ button. These terms describe that Facebook also collects data from third-party websites and apps via integrated interfaces or via cookies placed on the user’s computer or mobile device.

As the AG notes, when a controller invokes the necessity to perform a contract, and does not obtain the consent of the data subject, or even processes data for purposes directly against the will of the data subject, this “calls for a strict interpretation of the grounds in question, particularly in order to avoid any circumvention of the requirement for consent.”²³⁸

The AG argues that Facebook does not meet the requirements of the necessity test for each of the separate services or elements of a service that can be performed independently of one another.

The AG writes: “the applicability of Article 6(1)(b) of the GDPR should be assessed in the context of each of those services separately. (...) As far as the personalised content is concerned, it seems to me that, although that activity may, to some extent, be in the user’s interest, since it makes it possible to display content, particularly in the ‘News Feed’, which, on the basis of an automated evaluation, matches the user’s interests, it is not apparent that it is also necessary in order to provide the service of the social network at issue, such that the processing of personal data to that end does not require the user’s consent. For the purpose of that examination, consideration should also be given to the fact that the practice at issue concerns the processing not of data relating to the user’s activities on the Facebook site or app, but data originating from external and therefore potentially unlimited sources. Therefore, I am curious as to what extent the processing might correspond to the expectations of an average user and, more generally, what ‘degree of personalisation’ the user can expect from the service he or she signs up for.”²³⁹

The AG does not discuss all 15 identified purposes for the processing of observed and inferred data about visits to a government Page (as identified in Section 4.2 of this DPIA). However, with regard to the sharing of data within all Meta companies, the AG notes: “I doubt that the processing of personal data from other group services (including Instagram) is necessary to provide Facebook services.”²⁴⁰

²³⁸ Opinion AG CJEU, C-252/21, par 51.

²³⁹ Idem, par. 56.

²⁴⁰ Idem, par. 57.

However, as the use of contract as a legal ground (instead of freely given informed consent) needs to be strictly interpreted, the remaining 13 purposes for the processing of personal data related to the visits to government Pages, only 2 purposes seem to be able to pass the test of necessity to perform a contract in relation to each individual visitor:

- Technically provide a personalized service, with the two sub purposes (i) authenticate / verify account, keep users logged-in with cookies and (ii) cookies to improve technical performance
- Process according to user and Page administrator privacy settings

The 'contract' ground can only apply to people that have signed up for a Facebook account. This legal ground cannot be invoked for visitors of government Pages without a Facebook account, or visitors that have logged-out of Facebook.

However, Facebook uses cookies to keep users signed in, and serves the data tracking cookie to non-users. Facebook does not obtain the required consent for these cookies, as described in [Section 11.1.1](#) above, nor the required explicit consent to infer special characteristics of visitors to government Pages. Facebook cannot invoke the legal ground of necessity for a contract to compensate for the lack of – legally required – explicit consent.

The second purpose, execution of privacy settings, is not mentioned in Facebook's Privacy Policy, but was added for the sake of clarity.

Hence, Facebook can only rely on the legal ground of necessity to perform a contract for one purpose not mentioned in its Privacy Policy (to execute privacy settings), and only with regard to Facebook users.

11.1.3 *Public interest and legitimate interest*

Article 6 (1) (e) GDPR reads: "*processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.*"

Article 6 (1) (f) GDPR reads: "*processing is **necessary for the purposes of the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

The last sentence of Article 6(1) of the GDPR adds: "*Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.*"

The last sentence of Article 6(1) of the GDPR excludes the application of the legitimate interest ground for processing carried out by public authorities in the performance of their tasks. However, the choice to use Facebook Pages to communicate with the general public is secondary to the performance of public tasks by public authorities, and can therefore also be considered as a task primarily exercised under private law.

As explained in Recital 47 of the GDPR, the legal ground of necessity for the legitimate interest (Article 6(1) f) is more likely to exist "*where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.*" When a

government Facebook Page is used to communicate with a general audience, government organisations may also want to rely on the legal ground of necessity for the performance of their public tasks.

Both legal grounds require an assessment of the necessity of the personal data processing, of the proportionality and availability of alternative, less infringing means to achieve the same legitimate purposes (subsidiarity).

Even though Facebook is not a public sector organisation, it claims it can rely on legal provisions about research in the Treaty of the Functioning of the European Union to undertake 'research for social good' based on the legal ground of public interest. This is not plausible. Even if those articles were to provide a public interest ground, the scope of Facebook's purpose 'research for social good' is only described with an example ("*such as sharing relevant research data with*" [third parties]), and defined as "*research and other tasks in the public interest*". Because of this lack of purpose specification Facebook cannot rely on this legal ground for any data processing related to unknown types of research about the use and users of a government Page.

The AG addresses three purposes of the data processing in which Facebook relies on the legitimate interest ground: advertising, network security and product improvement. The AG focusses on the use of external data for these purposes. In all three cases the AG concludes that there is no obvious necessity to process personal data for these purposes, while "*it is necessary therefore for a close link to exist between the processing and the interest pursued, in the absence of alternatives that are more data-protection friendly, since it is not enough for the processing merely to be of use to the controller.*"²⁴¹

Though Facebook does not show advertisements on government Pages, Facebook does show recommended commercial content, as shown in **Fout! Verwijzingsbron niet gevonden.** and **Fout! Verwijzingsbron niet gevonden..** These recommendations can also be qualified as advertisements, in the literal sense, to draw attention to a third party organisation. Facebook does not explain to users or admins why it has selected these Pages. Facebook does however offer a more privacy-friendly alternative: Page admins can opt-out from having Facebook show a banner with Recommended Similar Pages to their visitors. If Facebook did not use the personal data about government Pages for other purposes (but it does, see below), the privacy friendly settings could help government Page admins to rely on the necessity for their public interest to use a Page to communicate with a general public.

However, admins do not have a control to prevent Facebook from using information derived (observed or inferred) from visits to government Pages, or interactions with postings from such government organisations to feed the algorithm to show personalised content. Nor government organisations, nor Facebook can rely on the legal ground of necessity for a public interest for these purposes of the processing of the personal data related to government Page visits.

Facebook invokes the legal ground of necessity for its legitimate interest for many purposes of the processing of the personal data of Page visitors. According to Facebook's Privacy Policy it distinguishes between legitimate interest as an alternative to contract with regard to minors, as a separate legal ground for other purposes (including minors), and as general legal ground for the processing of personal data

²⁴¹ Idem, par. 61.

about non-users and unknown devices. The list of legitimate interest purposes is specified below, in [Table 8](#) below.

Only one purpose, of showing targeted advertisements based on information provided by external organisations (custom or look-a-like audiences), is excluded from this table, as it is out of scope of this DPIA. For each of the remaining purposes, Facebook also describes what personal data it may process. This is generally the case for **all** personal data, as in: (i) activity and information users provide, (ii) friends, followers and other connections (iii) App, browser and device information (including location data), (iv) Information from partners, vendors and third parties.

Table 8: Specific purposes mentioned by Facebook, with legitimate interest

No.	Main purpose	Legitimate interest
For minors, if Facebook cannot rely on contractual necessity		
1.	Provide and improve (including research and testing) a personalised service, including personalised ads and sponsored / commercial content	To create, provide, support and maintain innovative products and features that enable people under the age of majority to express themselves, communicate, discover and engage with information and communities relevant to their interests, build community and utilise tools and features that promote their well-being.
		To share meaningful updates with our users under the age of majority about our products and promoting our products and services.
		To provide, personalize and improve the Meta Products in a consistent manner while ensuring additional safeguards for those under their Member State's age of consent.
		The legitimate interest of our users in being able to access the Meta Products and those Products being personalised to each user.
2.	Improve the Meta Products (including Instagram and WhatsApp)	To create, provide, support and maintain innovative products and features that enable people under the age of majority to express themselves, communicate, discover and engage with information and communities relevant to their interests, build community and utilise tools and features that promote their well-being.
		To enable people under the age of majority to use and connect to the Meta Products in an easy and intuitive manner.
		To provide, personalize and improve the Meta Products in a consistent manner while ensuring additional safeguards for those under their Member State's age of consent.
		The legitimate interest of our users in being able to access the Meta Products and those Products being personalised to each user.

		To create, provide, support and maintain innovative products and features that enable people under the age of majority to express themselves, communicate, discover and engage with information and communities relevant to their interests, build community and utilise tools and features that promote their well-being.
3.	Promoting safety, integrity and security on and across the Meta Products	<p>To secure our platform and network, to verify accounts and activity, to combat harmful conduct, to detect, prevent, and address spam and other bad experiences, to keep the Meta Products free of harmful or inappropriate content, to investigate suspicious activity or breaches of our terms or policies, and to protect the safety of people under the age of majority, including to prevent exploitation or other harms to which such individuals may be particularly vulnerable.</p> <p>In the interests of our users and the public at large, to prevent bad experiences and promote safety, integrity and security.</p>
4.	No purpose mentioned by Facebook (!)	To share meaningful updates with our users under the age of majority about our products and promoting our products and services.
For all people, including minors		
1.	Providing measurement, analytics and other business services to businesses, advertisers and other partners	<p>To provide accurate and reliable reporting to our advertisers, developers and other Partners, to ensure accurate pricing and statistics on performance and to demonstrate the value that our Partners realise using Meta Company Products</p> <p>In the interests of advertisers, developers and other Partners to help them understand their customers and improve their businesses, validate our pricing models and to evaluate the effectiveness of their online content and advertising on and off the Meta Company Products.</p>
2.	Communicating, engaging and sharing across the Meta Company Products	<ul style="list-style-type: none"> To provide seamless, consistent and richer, innovative communication, engagement and sharing experiences across Meta Company Products.
3.	Business intelligence and analytics	In our interest to measure the use of our Products and services and count the people who interact with our Products and services in order to inform and improve product direction and development and to enable provision of accurate and reliable reporting.
4.	Identifying you as a Meta Product user and personalising the ads we show you through	In our interest to fund our provision of the Meta Products and provide quality personalised advertising to users who visit the websites, apps and devices that use our advertising services;

	Meta Audience Network when you visit other apps/websites	In our interest to promote the Meta Products to people who are not registered users of the Meta products; and In the interests of advertisers who wish to reach people who may be interested in their information, products or services.
5.	Providing marketing communications to you	In our interest to promote Meta Company Products and send our direct marketing.
6.	To research and innovate for social good (incl. research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being).	In our interest and those of the general public to further the state-of-the-art or academic understanding on important social issues that affect our society and world in a positive way.
7.	Anonymising your information	In our interest to fund our provision of the Meta Products, provide relevant advertising to users, and improve ads delivery and Meta Products; In the interests of advertisers to help them to reach relevant audiences who may be interested in their information, products or services; In the interests of users that Meta practice data minimisation and privacy by design in respect of their information
8.	Share information with others including law enforcement and to respond to legal requests.	In our interest and the interest of the general public to prevent and address fraud, unauthorised use of the Meta Company Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, Meta personnel and property or Meta Products), our users or others, including as part of investigations or regulatory enquiries; or to prevent death or imminent bodily harm.
9.	Promote safety, integrity and security in limited circumstances outside of the performance of our contracts with you	In our interest to secure our platform and network, to verify accounts and activity, to combat harmful conduct, to detect, prevent, and address spam and other bad experiences, to keep the Meta Company Products free of harmful or inappropriate content, and to investigate and take action in respect of suspicious activity or breaches of our terms or policies; and In the interests of our users and the public at large, to prevent bad experiences and promote safety, integrity and security.
Visitors with unknown devices		
1.	Promote safety, integrity and security	In our interest to secure our platform and network, to verify accounts and activity, to combat harmful conduct, to detect, prevent, and address spam and other bad experiences, to keep the Meta Company Products free of harmful or inappropriate content, and to investigate and take action in respect of suspicious activity or breaches of our terms or policies; and

		In the interests of our users generally and the public at large, to prevent bad experiences and promote safety, integrity and security.
2.	Providing marketing communications to you (!, to unknown visitors)	In our interest to promote Meta Company Products and send our direct marketing.
3.	Research and innovate for social good (incl. research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being).	In our interest and in the interest of the general public to further the state-of-the-art or academic understanding on important social issues that affect our society and world in a positive way.
4.	Share information with others including law enforcement and to respond to .	In our interest and the interest of the general public to prevent and address fraud, unauthorised use of the Meta Company Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, Meta personnel and property or Meta Products), our users or others, including as part of investigations or regulatory enquiries; or to prevent death or imminent bodily harm.
5.	Product improvement, including (i) See if a product is working correctly, (ii) Troubleshoot and fix it when it's not, (iii) Test out new products and features to see if they work, (iv) Get feedback on our ideas for products or features and (v) Conduct surveys and other research about what you like about our Products and brands and what we can do better	To improve the Meta Company Products in a consistent manner, to correct technical glitches, and to optimise functionality.

As quoted in [Table 8](#) above, Facebook provides a brief description of the legitimate interest, of itself, of third parties, or of the users. As noted by the AG, a justification should be in the interest of the data controller, not in the interest of the user. If data processing mainly benefits the user, the data controller should ask for consent. *"From that perspective, it is unclear to what extent it could constitute a legitimate interest of the controller, thus avoiding the need for the user's consent."*²⁴²

It is up to Facebook to provide a convincing analysis why it would be necessary to process specific personal data, including sensitive personal data, resulting from a visit

²⁴² Idem, par. 66.

to a government Page, for its own commercial advertising, profiling and research purposes.

Facebook does not offer any hyperlinks to more extensive documentation how it has calculated the strict necessity for the processing of all listed personal data for each of the sub purposes.

In view of the sensitivity of data relating to surfing behaviour, it appears unlikely that purposes such as 'research to advance technology', or 'research to improve health', without any further limitation or exclusion of inferred sensitive data can be qualified as strictly necessary for Facebook to provide the service of access to a government Page. The same logic applies to purposes such as 'training our algorithms' or improving the Meta Products (including Instagram and WhatsApp). Though such training and sharing may very well be useful for Meta, it is not in the interest of the government Page visitor, nor is this data processing necessary to provide the Page service to government organisations.

Finally, Facebook requires all government Page visitors to accept 'Essential' cookies, without an option to refuse (users and non-users). This results in several tracking cookies and reading of device information in relation to users, and at least one tracking cookie in the browser of non-users. With the help of the unique device identifiers, Facebook is able to continue to track the surfing behaviour of users, even if they log out.

In earlier procedures against EU data protection authorities, Facebook claimed it had a legitimate interest to use the datr tracking cookie to identify non-users, for undefined security purposes.²⁴³ Facebook still does not provide an explanation about the purposes of its datr cookie. See Table 2 in Section 2.4.4. As explained in Section 9, in the Netherlands consent is required for the use of tracking cookies. As demonstrated in Sections 2.4.1 and 2.4.2 these cookies are also set and read by external websites, even if the users do not click on any Facebook icon on such an external website. Facebook cannot rely on its legitimate interest, and currently does not have any other legal ground for the processing of personal data resulting from the use of these cookies.

Users and Page administrators cannot opt-out from the data processing for any of these purposes. Because of this *take it or leave it* character of the processing, Facebook should provide a clear justification of the strict necessity of the processing of all listed personal data, including sensitive data about surfing behaviour, for all purposes. This is not the case. Facebook does not provide a clear explanation to users that it will continue to track them, even if they log out. Facebook does not delete the cookies and stop reading the unique device information when users log out.

Facebook also relies on the legal ground of necessity for its legitimate interest when it is compelled to disclose personal data to law enforcement authorities. This particular purpose of the data processing is discussed below, in Section 11.2 about Insights.

Absent transparency for users why they are shown specific recommendations, absent opt-outs for users for purposes / categories of personal data in which their fundamental rights prevail over the legitimate interests of Facebook, and absent opt-

²⁴³ See the Facebook file at the website of the Belgian Data Protection Authority, URL: <https://www.gegevensbeschermingsautoriteit.be/burger/facebook-zaak-het-hvi-eu-heeft-uitspraak-gedaan>.

outs for the admins of government Pages, to exclude all interactions with a government Page except for following the users instruction, such as 'I want to receive posts from this Page), nor Facebook nor the government organisations can appeal to the ground of necessity for a legitimate interest for the analysed data processing.

11.2 Facebook Insights

In case of joint controllership, each joint controller must have a legal basis for the processing. This should preferably be the same legal ground.²⁴⁴

For the creation of Facebook Insights, Facebook and government organisations can only use the necessity for their legitimate interest as a legal ground. Public law does not require government organisations to collect analytical data about Page visits and visitors. Therefore, the legal ground of necessity for the public interest cannot be successfully invoked, neither by government organisations, nor by Facebook.

Even though Facebook mentions consent and contract as legal grounds to "*Undertake analytics*", this purpose apparently differs from analytics provided as insights to Page owners, as the latter is mentioned separately, with the legal ground of necessity for the legitimate interest of Facebook, and the legitimate interest of others such as Page owners.

In order to rely on the last ground of legitimate interest, the interests of the organisations and the Page visitors must be carefully weighed. The analytics shown by Facebook do not allow for individual identification of visitors. As shown in [Figure 22](#), Facebook uses a threshold of at least 100 page visits or follows.

However, as described in [Section 5.4](#), the statistical data presented to the Page admin are only the tip of the iceberg of the data collected by Facebook as a result of visits to a government Page. Under water, and invisible to users and Page admins, Facebook processes observed behaviour data about interactions with the Page, and inferred data, such as an interest in the content shown on the government Page. Since Facebook retains these identifiable data for an indefinite period of time (with a pseudonymised RID after 90 days), the statistics presented to the Page admins are not anonymous, but pseudonymous personal data. Facebook is able to reidentify each of those visitors, based on its collection of diagnostic data.

There is an inextricable link between the creation of a Page by a Dutch government organisation and the processing of personal data about visitors of that Page by Facebook (for personalisation purposes, including advertising). This is particularly visible in the use of tracking cookies. With the information about visits to the government Page, Facebook is able to enrich the profile of users, and hence improve its targeting algorithms. Facebook would not be able to process these personal data for its own commercial purposes without the initiative from a government organisation to open a Page on the network.

In view of these circumstances, on the foot of the expert opinion of the German DPAs, and against the opinion of Facebook, this DPIA maintains the conclusion that Facebook and the government organisation factually are joint controllers. This means both need

²⁴⁴ EDPB Guidelines Controller-Processor v2.0, 7 July 2021, p. 4. The EDPB also mentions in footnote 73: "*Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose.*"

to be able to rely on a legal ground. As concluded in [Section 5.3](#), government organisations currently cannot conclude a joint controller agreement with Facebook for the processing of all personal data related to visits to a government Page. Such an agreement is only available for a small percentage of the relevant data processing: the Insights statistics.

If Facebook and the Page owners cannot be considered joint controllers for all processing related to Pages, a government organisation with a Page must have a legal ground for the transfer of all personal data to Facebook as independent third party. The processing of the visitor data for Facebook's own purposes is a form of 'further' processing of data. Such 'further' processing is only allowed if this is compatible with the initial purposes of the data collection. For government organisations, there are only two purposes for the data collection from visitors to a Page, namely to technically provide a communication facility to Facebook users and non-users, and to create website analytics.

To assess the legitimacy of this further processing for different purposes (Facebook's own commercial purposes), 5 criteria need to be taken into account (based on Article 6(4) of the GDPR):

- a) *any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;*
- b) *the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;*
- c) *the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;*
- d) *the possible consequences of the intended further processing for data subjects;*
- e) *the existence of appropriate safeguards, which may include encryption or pseudonymisation.*

These five criteria are assessed below.

11.2.1 *Link between purposes*

With regard to the *link between the purposes* Facebook users may expect that their interactions with a government Page result in a higher priority for such content in their News Feed. However, it is nearly impossible to understand the link with other users' preferences (friends of friends), or content from other, unknown, organisations suggested in the News Feed. As the AG writes: "*Consideration should also be given to the fact that the practice at issue concerns the processing not of data relating to the user's activities on the Facebook site or app, but data originating from external and therefore potentially unlimited sources. Therefore, I am curious as to what extent the processing might correspond to the expectations of an average user and, more generally, what 'degree of personalisation' the user can expect from the service he or she signs up for.*"²⁴⁵ As shown **Fout! Verwijzingsbron niet gevonden.**, there is no intuitive link between following political parties and being served extremist anti-government content. As the HRIA explains, this is a result of several biases in Facebook's algorithms.

²⁴⁵ Idem, par. 56.

11.2.2 Context

The *context* in which the data are collected is particularly non evident for non-users, as they may accidentally end-up on a Facebook Page if they search for government information. If they refuse tracking cookies, they are still being served with the Facebook data tracking cookie.

11.2.3 Nature of the data

Facebook processes three categories of personal data: (i) special categories of data, (ii) data of a sensitive nature and (iii) personal data related to tracking cookies and device identifiers.

Special categories of data may be *revealed* from visits to government Pages, as explained in [Section 11.1.1](#). Facebook collects/generates these data for its own purposes, and uses some of these data to create Facebook Insights.

The personal data processed for Insights may also include personal data of a sensitive nature, as explained in [Section 2.6.1](#) such as data about surfing behaviour and location data. As quoted in [Section 1.2.1](#) Facebook accesses both the user-provided location data, and the observed user location data when a user visits a government Page in order to geotarget advertisements on and off Facebook.

Thirdly, Facebook processes personal data related to tracking cookies and device identifiers, also outside of Facebook.

Since Facebook is capable of using these three categories of personal data to profile users for its own commercial purposes, including showing paid postings and advertisements in visitors' *News Feed*, the nature of the data entails significant risks to the fundamental rights and freedoms of the Page visitors.

As the AG notes, "*the decisive factor for the purpose of applying Article 9(1) of the GDPR is, in my view, whether the data processed allow user profiling based on the categories that emerge from the types of sensitive personal data mentioned in that article.*"²⁴⁶ It is not relevant if Facebook actually intends to profile users, but only if Facebook links these characteristics to the Facebook user account (or to the profile related to the tracking cookie in the browser of a non-user). "*the controller is not required to process those data knowing and intending to derive particular categories of information directly from them. The aim of the provision in question is, in essence, objectively to prevent significant risks to the fundamental rights and freedoms of data subjects arising from the processing of sensitive personal data, irrespective of any subjective element such as the controller's intention.*"²⁴⁷

11.2.4 Possible consequences for Page visitors

Facebook transfers all personal data relating to a government Page visit to the USA, including sensitive data and special categories of data that emerge from interactions with specific content from government Pages. As described in [Section 10](#) Facebook retains these personal data for an indefinite period of time.

²⁴⁶ Idem, par. 38.

²⁴⁷ Idem, par. 41.

As shown in [Table 7](#) in [Section 5.3.1](#) Facebook is subjected to a long list of US American legal obligations to disclose personal data from its users, including data about visitors of a Dutch government Page. In 2021 Facebook received 123.653 requests from US government authorities for 214.782 accounts (users).²⁴⁸ Facebook does not specify the location of the users: only the location of the requesting authority. Additionally, in 2021 Facebook was ordered to disclose data about 125.000 to 125.499 Facebook accounts under FISA legislation, from non US persons.

These large amounts of disclosures, combined with the indefinite retention period of behavioural data linked to pseudonymous user identifiers indicate that there is a significant chance that personal data from visitors of a Dutch government Page may be disclosed to US authorities. As summarised in [Section 7.2.1](#) it follows from the Schrems II ruling from the CJEU that the current legal regime in the USA, in particular FISA legislation, does not meet the four essential data protection guarantees. Currently (pending negotiations about a new transatlantic data agreement) there is no independent oversight mechanism in the USA, legislation does not meet proportionality requirements, and non US persons lack legal status under US law to have effective remedies. In practice this means non US persons are not informed when their data are accessed by law enforcement or secret services, and may end up in Kafkaesque situations when they are for example being refused entry to the United States, or worse, are being held in custody.

As described in [Section 7.3](#), the Irish Data Protection Commission has issued a provisional ban on the transfer of personal data to the USA, following the Schrems-II jurisprudence from the CJEU. This suspension has not yet entered into force, but provides a clear indication of the possible negative consequences for Page visitors.

11.2.5 *Appropriate safeguards*

Facebook uses pseudonymous identifiers in its Big Data processing, and replaces the unique User ID after 90 days with a different unique replacement ID. This is not a relevant safeguard. In fact, the use of unique computer readable identifiers has enabled Facebook to apply machine learning on an unprecedented scale. As described in [Section 8.2](#) the resulting logic of the personalised content (how inputs related to outputs) has become impenetrable, even for Facebook.

In sum, as joint controllers nor the Dutch government organisations nor Facebook have a legal ground for the processing of personal data relating to Page visits. Though government organisations can generally rely on the necessity for a legitimate interest to collect statistics about visits to their webpage, this is not the case when they publish on a Facebook Page. Facebook's further processing of the website data for its own commercial purposes is not compatible with the purpose for which the Dutch government allows Facebook to collect the data: provide the Page functionality and create web analytics. The *further* processing involves sensitive data with possibly very high data protection risks for Page visitors, if their data are disclosed to government authorities in third countries without an adequate data protection regime.

12. Special categories of data

Special categories of data are “*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a*

²⁴⁸ Facebook, Government Requests for User Data, undated, last viewed 15 July 2022, URL: <https://transparency.fb.com/data/government-data-requests/>

natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Article 9 GDPR). In addition, Article 10 of the GDPR prohibits the processing of *"personal data relating to criminal convictions and offences or related security measures."*

As explained in Section 2.6.1 of this DPIA, government organisations can enable Facebook to collect or infer personal data of a sensitive nature as a result of interactions with the content published on the Page or shared as posts. Facebook may also collect or infer special categories of data from interactions with government content.

With special categories of data, the principle is one of prohibition: these data may *not* be processed. The law contains specific exceptions to this rule, however, for instance when the data subject has explicitly consented to the processing, or when data have explicitly been made public by the data subject. As explained in [Section 11.1.1](#), Facebook cannot rely on these two exceptions, and does not have a legal ground for the processing of special categories of data.

Even though Facebook has changed its advertising options, and since 19 January 2022 no longer shows detailed targeting categories to advertisers that point to sensitive categories such as political affiliation, religion, race or sexual orientation²⁴⁹, Facebook does not exclude the use of such inferences of sensitive characteristics in the recommendations it shows to users on a government Page, and in the ranking of content in the *News Feed*. Government admins have no way of preventing such inferences and further processing by Facebook, as described in [Section 3.1](#).

In sum, as joint controllers nor the Dutch government organisations nor Facebook have a legal ground for the processing of special categories of personal data relating to Page visits, but government organisations cannot prevent Facebook from further processing these data for its own commercial purposes.

13. Purpose limitation

The principle of purpose limitation is that data may only be *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes"* (Article 5 (1) (b) GDPR). Essentially, this means that the controller must have a specified purpose for which he collects personal data, and can only process these data for purposes compatible with that original purpose.

Data controllers must be able to prove, based on Article 5(2) of the GDPR, that they comply with this principle (accountability). As explained in [Section 5.4](#) of this report Facebook and the Dutch government organisation that decides to use a Facebook Page are joint controllers, not only for Insights, but for all personal data processing related to visits to a government Page.

²⁴⁹ Source: Euractiv, Meta to prevent ad targeting based on sensitive information, 10 November 2021, URL: <https://www.euractiv.com/section/digital/news/meta-to-prevent-ad-targeting-based-on-sensitive-information/>

As detailed in [Section 11.2](#) Facebook processes the observed and inferred data for (at least) 15 purposes, with sub-purposes. These purposes are not specific, nor limited to specific personal data. Generally, Facebook permits itself to process all personal data for all purposes. Nor Page visitors, nor Page admins can effectively determine the scope and impact of visiting a government Page or interacting with government content.

Because Facebook does not offer a joint controller agreement to the government organisations outside of the creation of Insights, all purposes for which Facebook processes the personal data relating to a government Page visit are a form of 'further' processing.

As analysed in [Section 11.2](#), Facebook's further processing of the website data for its own commercial purposes is *not compatible* with the purpose for which the Dutch government allows Facebook to collect the data: provide the Page functionality and create web analytics. The further processing involves sensitive data with a possibly very high data protection risks for Page visitors, if their data are disclosed to US government authorities.

14. Necessity and proportionality

14.1 The principle of proportionality

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which are processed must be necessary for the purpose pursued by the processing activity. [Proportionality](#) means the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. [Subsidiarity](#) means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the controller needs to decrease the amount of personal data to what is necessary.

Therefore, essentially, the data controller may only process the personal data that are necessary to achieve the legitimate purpose, but may not process personal data he or she may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

14.2 Assessment of the proportionality

The key questions are: are the interests properly balanced? And does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.

Data must be '*processed lawfully, fairly and in a transparent manner in relation to the data subject*' (Article 5 (1) (a) GDPR). This means that data subjects must be informed

about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected.

Facebook's business model is based on offering personalised content, with a key role for paid advertising. How Facebook determines what content to show to a user, is however completely intransparent. Facebook only publishes a generic information Page about its approach to ranking.²⁵⁰ Facebook explains that it makes a personalised prediction about each post of how likely it is of interest to the user, but does not reveal the individual logic it applies to select the content for a specific user. Facebook does not offer an interface for users to see why a certain post ended up in their News Feed, or why other Pages from commercial organisations were recommended to them.²⁵¹ Facebook also does not explain the logic behind the (assumed) preferences and the interface for ads preferences does not reveal this logic either. Therefore users cannot understand why certain content is recommended to them on the government Page, why contents from government Pages they follow are shown or not shown in their *News Feed*, or how their interactions with the government Page translate in content from other persons/Pages in their News Feed.

Facebook does not provide meaningful information, nor in advance, nor in retrospect in reply to a data subject access request. As explained in [Section 8](#), the way in which Facebook has organised the data processing, with tasks that are performed automatically in Dataswarm on a very big scale, makes it virtually impossible for Facebook to retrieve in retrospect why each piece of content was shown to a user.

In a recent article in *The Intercept* about the revelations in the Californian class action court case, the lack of transparency was summarised as follows: *"In the March 2022 hearing, Zarashaw and Steven Elia, a software engineering manager, described Facebook as a data-processing apparatus so complex that it defies understanding from within. The hearing amounted to two high-ranking engineers at one of the most powerful and resource-flush engineering outfits in history describing their product as an unknowable machine."*²⁵²

Facebook's data processing can thus be characterised as '*obscurity by design*'.

Facebook does not publish detailed or limitative documentation about the specific behavioural and device data it collects relating to government Page visits. Similarly, Facebook does not provide an exhaustive list of the cookies it uses. In its Privacy and in its Cookie Policy Facebook provides generic purpose descriptions and often uses examples, (words as 'such as'/'like' or 'See examples'). In its Privacy Policy Facebook lists 8 types of device information, and provides hyperlinks to examples. Facebook also describes a category of Page visitors that cannot be recognised based on unique

²⁵⁰ Meta Transparency Center, Our approach to ranking, last updated 17 June 2022, URL: <https://transparency.fb.com/en-gb/features/ranking-and-content/>

²⁵¹ Apparently Facebook was able to show such information per content item in 2019, but this option has since been removed. See: <https://about.fb.com/news/2019/03/why-am-i-seeing-this/>.

²⁵² The intercept, Facebook engineers: We Have No Idea Where We Keep All Your Personal Data, 7 September 2022, URL: https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/?utm_medium=social&utm_source=twitter&utm_campaign=theintercept.

device identifiers: *"If you are using a device we cannot associate with a registered user of the Meta Products."*²⁵³

As described in [Section 3.2](#) Facebook users can log-out. However, this does not prevent Facebook from recognising their unique device identifiers, and track their behaviour on and off Facebook. Facebook does not provide any clear explanation or warning to Page visitors that logging-out does not stop this surveillance. Recently, Facebook was even accused in a new class action case in the USA of tracking users on their iOS devices after they had explicitly disabled the mobile advertising ID, through the embedded browser in the Facebook app.²⁵⁴ This points to a pattern where Facebook commercially benefits from a lack of transparency.

In sum, Facebook does not meet the required transparency standard. The lack of transparency makes the data processing inherently unfair.

The [principles of data minimisation and privacy by design](#) require that the processing of personal data be limited to what is necessary. The data must be *'adequate, relevant and limited to what is necessary for the purposes for which they are processed'* (Article 5(1)(c) of the GDPR). This means that the controller may not collect and store data that are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings.

Facebook does offer some controls to users and Page admins (described in [Section 3](#)), but these controls do not minimise Facebook's data processing. As shown in [Figure 32](#), admins can opt-out from having their Page found through search engines. They can also opt-out from having Facebook show a banner with Recommended Similar Pages to their visitors. However, nor user nor Page admins can protect the personal data relating to their interactions with government content against further processing by Facebook. Page admins cannot minimise the retention period of the observed and inferred personal data relating to visits to a government Page. The available cookie choice for 'essential' cookies suggests an option for data minimisation, but does not prevent Facebook from setting and reading tracking cookies. Last but not least, users cannot stop the surveillance by logging out, as Facebook will continue to recognise them based on the unique identifiers in their devices.

As shown in [Figure 18](#) Facebook has graphically designed its cookie choice in such a way to give clear preference to the button to accept optional cookies. The light grey 'only allow essential cookies' button attracts less attention than the blue button. This type of interface design leads to 'deception by design', according to the Norwegian Consumer Council.²⁵⁵ It is a clear example of a *dark pattern*. It is also misleading, because the word 'essential' is commonly understood to exclude tracking cookies, while Facebook still sets/reads the data tracking cookie for which consent is required.

²⁵³ Facebook Privacy Policy, last updated 26 July 2022, URL:

https://www.facebook.com/privacy/policy?section_id=18.4-LegitimateInterestsWeRely

²⁵⁴ Techcrunch, Facebook users sue Meta, accusing the company of tracking on iOS through a loophole, 22 September 2022, URL: <https://techcrunch.com/2022/09/22/meta-lawsuit-ios-privacy/>.

²⁵⁵ Norwegian Consumer Council (Forbrukerradet), Deceived by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy, 27 June 2018, URL: <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>

As described in a report from the Norwegian Consumer Council, *"User interfaces can be employed to steer consumers into prioritising certain choices over others, to hide or omit relevant information, or to otherwise trick, confuse or frustrate users. These practices can be collectively referred to as dark patterns or manipulative/deceptive design. Dark patterns can be summed up as features of interface design that push or nudge people into making choices for the benefit of the service provider, often at the cost of the individual's money, time and/or privacy."*²⁵⁶

In sum, Facebook does not enable government organisations to effectively minimise Facebook's data processing. Facebook actively misleads users with dark pattern design. This also makes the data processing inherently unfair.

The principle of storage limitation requires that personal data should only be kept for as long as necessary for the purpose for which the data are processed. Data must *'not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed'* (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that *'personal data may be kept longer in so far as the personal data are processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'* (Article 5(1)(e), second sentence, GDPR).

It follows from the Californian class action court case that Facebook retains identifiable behavioural data for an indefinite period of time (with a pseudonymised RID after 90 days). Facebook is able to reidentify each of those visitors, based on its ongoing collection of diagnostic data. Facebook does not inform users or Page administrators about this retention period. Instead, Facebook only mentions it keeps information as long as necessary. None of the examples and purposes mentioned by Facebook explain that this means an indefinite retention period for behavioural data linked to pseudonymous identifiers, or why this would be necessary.

Similarly, Facebook is unwilling to explain why it would be necessary to have a life time of 2 years for the datr-cookie in the browsers of users and non-users for the purpose of protecting the social network.²⁵⁷

Facebook does not provide information about the Insights retention periods either, but it appears from the user interface the default retention period for Insights is 3 years and 1 month. This does not seem excessive, as Facebook's aggregation above 100 users is adequate to prevent reidentification. However, this retention period does not influence Facebook's own retention of the underlying raw personal data.

²⁵⁶ Norwegian Consumer Council, You can log out, but you can never leave, How Amazon manipulates consumers to keep them subscribed to Amazon Prime, 14 January 2021, URL: <https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf>

²⁵⁷ As established by the German appellate administrative court in November 2021 and the conference of German DPAs in their expert opinion of March 2022.

An indefinite retention period is by its very nature disproportionate, and not in line with the requirement of Article 5(e) GDPR.

In sum, Facebook's current data processing of personal data observed or inferred by visits to a government Page is not transparent, and does not comply with the legal privacy by design and data retention requirements. Therefore, the data processing is not proportionate to the interest pursued by the Dutch government to distribute content to a mass audience.

14.3 Assessment of the subsidiarity

The key question is whether the same goals can be reached with less intrusive means.

In view of Facebook's market share in the social media market, and the government's desire to communicate where people already spend time, there is no ready alternative for Facebook as a social medium. The Dutch government has already adopted a policy not to advertise on Facebook, due to the privacy risks. The Dutch government is not required to use Facebook, but can also use other communication media.

Alternative social media such as Twitter, TikTok and LinkedIn do not reach the same audiences. More importantly, absent DPIAs government organisations cannot assume these platforms are GDPR and ePrivacy directive compliant. In fact, the German DPAs warn that the problems with joint controllership most likely apply to all other social media.²⁵⁸

One relevant alternative in the making is 'Pubhubs', an initiative from two Dutch professors to encourage the development of an alternative social network for public sector organisations.²⁵⁹

PubHubs introduces itself as a *"new Dutch community network, based on public values. PubHubs stands for Public Hubs. It is open and transparent and protects data of the network's participants. PubHubs aims to connect people, in different hubs, such as your family, sports club, school class, museum, local library, neighborhood, or municipality."*²⁶⁰

Use of this communication tool may present less data protection risks, as it will be offered by a Dutch organisation without a subsidiary in the USA, and it will be developed based on the principles of security and privacy by design and by default. As open-source tool, its compliance with the GDPR can be more easily assessed.

²⁵⁸ DSK, FAQ zu Facebook-Fanpages, Stand: 22. Juni 2022, URL:

https://www.datenschutzkonferenz-online.de/media/oh/20220622_oh_10_FAQ_Facebook_Fanpages.pdf. Q&A 4: "Bestehen die gleichen Probleme auch bei anderen Social-Media-Diensten (z. B. Instagram, Twitter, TikTok usw.)? In der Tat dürften viele der Erkenntnisse auch auf andere Social-Media-Auftritte übertragbar sein. Die Umstände sind häufig sehr ähnlich, sodass die rechtliche Bewertung sinngemäß übertragbar ist."

²⁵⁹ PubHubs, URL: <https://pubhubs.net/en/index.html>

²⁶⁰ Idem.

The DPA of Schleswig-Holstein mentions another privacy friendly alternative in its press communication about the final ruling in the Fan Page case: Mastodon as alternative for Twitter.²⁶¹

15. Data Subject Rights

The GDPR grants data subjects a number of privacy rights. In this section, only two of these rights are discussed, as relevant for the data processing related to government Pages. These are (i) the right to information and (ii) the right to access.

Right to information

Data subjects have a right to information. This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.

As assessed in Section 14.2 above, the information Facebook provides about the processing of behavioural data, and the logic of content selection, is incomplete. Without this information, nor admins nor end users can fully understand what personal data are processed and for what purposes as a result of visits to government Pages.

Right to access

Secondly, data subjects have a (fundamental) right to access personal data concerning them. Upon request, data controllers must inform data subjects whether they are processing personal data about them (directly, or through a data processor). If this is the case, they must provide data subjects with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

In reply to the data subject access requests, Facebook referred to its Do It Yourself download tool. Though this tool did provide plenty of data, it did not provide access to the most relevant data for this DPIA, what data Facebook uses for its algorithmic decisions, or the logic behind the ranking of content, suggested friends and recommended posts and Pages, including the underlying profile on which the specific personalised content was based. As quoted in Section 2.5.2 the judge in the Californian court case identified three categories of “discoverable user data” (that Facebook should provide in reply to a data subject access request):

1. data collected from a user’s on-platform activity,
2. data obtained from third parties regarding a user’s off-platform activities, and
3. data inferred from a user’s on or off platform activity.

²⁶¹ ULD Schleswig Holstein, press release 11 April 2022, URL: <https://www.datenschutzzentrum.de/artikel/1397-Gutachten-zu-Facebook-Fanpages-Betrieb-noch-immer-nicht-datenschutzkonform-der-oeffentliche-Bereich-muss-handeln.html#extended>. ULD mentions [https://social.bund.de/@dsk\[Extern\]](https://social.bund.de/@dsk[Extern])) and notes that the instance of this decentralised open source platform is offered by the federal German IT supplier.

The court case has provided irrefutable evidence, based on Facebook's own testimony, that Facebook does generate and store these data, and is technically capable of reproducing these data.

To explain the missing data, as quoted in [Section 2.5.5](#) Facebook explained that it strikes a fair balance between the competing interest of a user to obtain access to his or her personal data, and the burden for data controllers to produce these data. Facebook claims producing more data would impose a disproportionate burden. Facebook writes that the GDPR allows the controller to take into account *whether or not the data is readily accessible, and the costs incurred by the controller in retrieving certain information*. Facebook argues that it would be disproportionate for Facebook to retrieve individual personal data from its large Hive datasets.

As the GDPR does not explicitly mention any proportionality considerations with regard to the right to data subject access, Facebook probably leans on the CJEU reasoning in the case of *Rijkeboer*.²⁶² In this case (based on the Data Protection Directive, DPD) the Court introduced the principle that the effort required by controllers to comply with data subject rights should be proportionate to the benefit data subjects gain from exercising their rights.

A draft thesis on data subject access rights from René Mahieu²⁶³ summarises this as follows: *"In some cases, controllers can legitimately limit the response to an access request, if responding would require "disproportionate effort". This ground for limiting access is not explicitly mentioned in the GDPR, instead, it was mentioned in some provisions of the DPD. According to the ECJ, this ground for limiting access should apply analogously to other obligations.*²⁶⁴ *Moreover, it was included in several national implementations of the DPD.*²⁶⁵ *Some scholars have questioned to what extent the limitation does still apply under the GDPR*²⁶⁶, *but controllers definitely still appeal to it, and courts and supervisory authorities do in some cases accept the legitimacy of such an appeal.*"²⁶⁷

Mahieu also writes: *"the effort that can be expected of controllers is substantial, and controllers are expected to design systems in a way that allows for the exercise of data subject rights.*²⁶⁸ *It should be noted that the complexity of the processing cannot*

²⁶² CJEU case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer*, 7 May 2009, ECLI:EU:C:2009:293, paras 61-63.

²⁶³ Draft thesis version August 2022, Chapter 2. René Mahieu is doctoral candidate at Vrije Universiteit Brussel (VUB), LSTS, Interdisciplinary Research Group on Law Science Technology & Society.

²⁶⁴ *Idem*.

²⁶⁵ For example, the Irish Data Protection Acts 1998 section 4(9) (repealed) and DPA UK 1998 section 8(2)(a) (repealed) contained provisions for limiting the right of access based on disproportionate effort.

²⁶⁶ Veale, M; Ausloos, J; (2021) *Researching with Data Rights. Technology and Regulation* pp. 136-157, Section 5.1.7 Disproportionate effort, p. 152, URL: <https://doi.org/10.26116/techreg.2020.010>.

²⁶⁷ Gegevensbeschermingsautoriteit (Belgian DPA) beslissing ten gronde 15/2021 para 2.2.2.2.

²⁶⁸ England and Wales Court of Appeal, *Dawson-Damer & Ors v Taylor Wessing LLP* [2017] EWCA Civ 74 para 78-79 (here, the court applies these principles to the question of whether the effort required to deal with an access request is proportionate); *Arbeitsgericht Düsseldorf* (German Court of first instance labor law), 9 Ca 6557/18

*be used as a reason to consider providing access too burdensome. Instead, the burden which can be expected from the controllers in complying with transparency obligations is higher when the processing is more complex. The proportionality of the required effort also depends on the situation in a specific case."*²⁶⁹

It follows from Facebook's court testimony in the Californian class action case that Facebook retains unique user identifiers, and can hence search these data for data relating to specific individuals. Relevant jurisprudence from a German appellate court indicates that proportionality needs to be assessed in relation to the size/scale of the data processing.

The German court explained: *"To the extent the defendant argues that it is economically impossible for large companies which, like the defendant, manage a large amount of data, to query and secure personal data in the data, with the resources at their disposal, this does not hold water. It is up to the defendant, when processing electronic data, to organise the data in accordance with the legal order and, in particular, to ensure that data protection and ensuing data protection rights of third parties are taken into account."*²⁷⁰

In other words, the lack of access to personal data does not mean Facebook cannot retrieve these data, only that it requires (a lot of) effort to search for these data in the datasets in reply to an individual data subject access request. In view of Facebook's global operations and technical know-how with regard to the searching of extremely big datasets, it is hard to understand how retrieving personal data would be impossible.

More importantly, the German court also refers to the privacy by design obligation in the GDPR: that companies that process electronic data on a large scale, must organise the data in such a way that they can reply to data subject access requests in a meaningful way.

Finally, if Facebook would want to rely on the exception of Article 23(1) sub i, (to protect Facebook's own interests not to spend time and money on queries) Facebook should refer to specific national implementing law, in this case, the UAVG. Article 23 does not create a generic exception on data subject rights. The implementation in the Dutch UAVG is unlawful, according to DSAR expert Mahieu, as it does not specify the restrictions.²⁷¹ Additionally, there is a relevant ruling from the Austrian Supreme Court

ECLI:DE:ARBGD:2020:0305.9CA6557.18.00 (The court ruled that a controller, which had provided access to copies of many documents to the employee who had submitted a request, did not have to search all email boxes, mobile phones and notebooks of his colleagues and superiors, because this would be disproportionate, especially since the employee did not substantiate his belief that these sources would contain more personal data).

²⁶⁹ Draft thesis, Chapter 2.

²⁷⁰ OLG Köln, Urteil vom 26.07.2019, par. 81, URL: <https://openjur.de/u/2177719.ppdf>.

Translation by Privacy Company.

²⁷¹ Mahieu, Feedback for the European Data Protection Board (EDPB) in response to the public consultation on 'Guidelines 10/2020 on restrictions under Article 23 GDPR Version 1.0 Adopted on 15 December 2020, submitted 12 February 2021, par. 8, URL: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_feedback_art23_ggf_ld_rm_mnp.pdf.

that the financial interest of a data controller cannot be claimed as a 'right of others' protected by Article 23(1) sub i.²⁷²

For the sake of completeness, in case Facebook would want to rely on an argument that its pseudonymous Replacement Identifiers would not (no longer) be personal data, or it would cost too much effort to query such non-indexed logs, Dutch jurisprudence clearly obliges organisations to provide access to such pseudonymous identifiers. The Dutch administrative law court (Raad van State) ordered the municipality of The Hague to produce the IP addresses from its webserver access logs, and IP addresses registered in one of its specific registration systems, even though the municipality initially claimed these were anonymous data.²⁷³

Another argument used by Facebook withhold full access is that the data would be *meaningless* to an average person.²⁷⁴ Privacy Company explained at the beginning of the DPIA that it is not an average person, but wanted to have full access, and is fully capable of reading technical logs. Facebook did not provide any additional information.

In sum, Facebook's generic refusal to provide full access to the personal data it evidently processes in multiple systems, is invalid. As joint controllers with Facebook, government organisations are unable to (fully) honour the rights of the data subjects that visit their Pages. As noted in the HRIA, the lack of data subject access makes that Page visitors have no effective possibility to understand the decisions made and no effective possibility to lodge a complaint. In general, this lack of transparency makes it impossible to assess what impact the personalisation of Facebook has on human rights when the government uses Pages.

²⁷² Austrian Supreme Court, OGH - 6Ob138/20t, 17 December 2022, ECLI:AT:OGH0002:2020:0060OB00138.20T.1217.000. The case is machine translated in English by GDPRhub, para 71, URL: [https://gdprhub.eu/index.php?title=OGH - 6Ob138/20t](https://gdprhub.eu/index.php?title=OGH%20-%206Ob138/20t).

²⁷³ Raad van State, case 202006125/2/A3, 24 February 2022, ECLI:NL:RVS:2022:611.

²⁷⁴ E-mail Facebook Netherlands to Privacy Company and BZK, 5 July 2022.

Part C. Discussion and Assessment of the Risks

This part of the DPIA contains a discussion and assessment of the risks for data subjects related to the processing of personal data observed and inferred from visits to government Pages, including the effects of the mandatory use of tracking cookies.

This part starts with a brief summary of possible risks in relation to the two main categories of data processing: Facebook's processing of observed and inferred data relating to Page visitors, and Facebook's processing of these data into Insights that are available for Page admins.

16. Risks

16.1 Identification of data protection risks

Data protection risks are different from security risks. They do not include business risks, such as reputation risk, or the financial risk of a fine by a supervisory authority.

Data protection risks assess the specific impact on people, related to the likelihood that a specific violation occurs. The impact does not need to be material, but can also be immaterial and/or psychological. Because data protection is a fundamental right, infractions of rights such as the right to data subject access automatically lead to a qualification as a high data protection risk, because the impact is qualified as high. Without access, data subjects are unable to assess the scope of the data processing, and cannot invoke their other rights. Additionally, even a small probability of occurrence of a risk can lead to a high risk, depending on the impact on the data subject. This is visualised in a matrix in Table 9 below.

Data protection risks can be grouped in the following categories:

- Inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage¹⁸¹

These risks have to be assessed against the likelihood of the occurrence of these risks and the severity of the impact.

The UK data protection commission ICO provides the following guidance: "*Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to*

*qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.*¹⁸²

In order to weigh the severity of the impact, and the likelihood of the harm for these generic risks, this report combines a list of specific risks with specific circumstances of the specific inspected data processing.

16.1.1 *Inability to exercise data subjects rights*

Facebook processes large amounts of observed and inferred data in complex self-learning algorithmic data systems. Though Facebook offers a Do It Yourself download tool to its users, and access to some logs to Page admins, nor users nor Page admins are able to obtain full access to the personal data relating to government Page visits. This has a particularly high impact because Facebook does not explain the logic behind its personalisation algorithms. Individual Page visitors cannot understand why they are being shown *rage bait* articles, if this is a result of following particular Pages or people, or because of indirect inferences. Because they are not informed, they cannot exercise other rights, such as asking Facebook to correct inferences.

As Facebook has admitted in the Californian court case, it does not provide access to all relevant and available personal data. Facebook's reasons to withhold access are invalid. It is plausible that Facebook itself doesn't know anymore what data it processes, in what systems. Facebook should have designed its systems with transparency and individual access in mind. Instead, Facebook's big data processing is an example of *obscurity by design*. Facebook cannot rely on the exception of Art. 23(1) sub i by pointing out that there are costs involved in redesigning its systems to comply with the law. In view of its size and profitability, the threshold for investments to become disproportional is very high.

The probability of occurrence of the risk that data subjects cannot exercise their fundamental right to access these personal data is more likely than not, while the impact is very high. That is why the data protection risks for the data subjects are high.

16.1.2 *Chilling effect on other fundamental rights*

The knowledge that Facebook processes information about interactions with government content can cause a *chilling effect* on the exercise of other fundamental rights. A *chilling effect* is the feeling of pressure someone can experience through the monitoring of his or her behavioural data, discouraging this person from exercising their rights, such as accessing certain content.²⁷⁵

Both users and non-users of Facebook may experience a *chilling effect* as a result of the monitoring of their visits to a government Page by Facebook, as these observations and inferences are used to rank the contents in the News Feed, to show other recommended content and to show targeted advertising. This risk may be exacerbated for government employees that use their personal Facebook account to manage a government Page, as their private life and their professional activities may become intertwined, even long after they switch work environment.

Nor Page administrators nor the visitors of a government Page are informed how Facebook processes the information about their visits, for what purposes, if they only visit the Page, or interact through likes or follows, and there is no opt-out.

²⁷⁵ Definition Merriam-Webster, <https://www.merriam-webster.com/legal/chilling%20effect>

The impact is related to the level of risk for the data subjects in case Facebook uses the information to profile and target users. Facebook can process two kinds of personal data with a high impact: data of a sensitive nature (such as location data and web surfing behaviour, also outside of Facebook), and special categories of data. As argued in [Sections 11.2.3 and 12](#), Facebook may infer special characteristics from interactions with government content. Government Page visitors may be prevented from replying to government content and participate in political discussions for fear of revealing sensitive characteristics. They may also fear embarrassment (if Facebook were to profile a user as a 'fan' of a politician with extremist views) or shame (if Facebook for example would infer from Page visits that a user is interested in a particular sexual disease).

As visible in the short test period, the new test account that followed the leaders of all political parties in the Netherlands soon received anti-government content. Because Facebook did not provide any information about the logic of this personalisation, but did apparently profile this test user as interested in this kind of content, there is a real probability that the user experiences the chilling effect. This profiling has a high impact on the exercise of his or her other rights. Therefore the data protection risks for the data subjects are high.

16.1.3 *Lack of transparency purposes of the processing*

Facebook does not provide a limitative list of specified and explicit purposes. It requires close reading of different policies to discern different purposes of the processing. In its Privacy Policy, Facebook uses broadly worded purposes, for which it generally permits itself to process all categories of personal data.

As detailed in [Section 11.2](#) Facebook processes the observed and inferred data about government Page visits for (at least) 15 purposes, with sub-purposes. Facebook does not describe as specific purpose that it profiles users, and that this may include inference of special characteristics of Page visitors.

Facebook and the government organisations are factually joint controllers for all personal data processing relating to government Page visits, not just for the creation of the Page Insights. Nor Page visitors, nor Page admins can effectively determine the scope and impact of visiting a government Page or interacting with government content. The scope also includes surveillance by an unknown amount of unknown third parties that may obtain access to the tracking cookies and device identifiers shared by Facebook on and off Facebook. As joint controller, government organisations are equally accountable as Facebook for the lack of transparency.

The data processing may involve sensitive data and special categories of data with possibly very high data protection risks for Page visitors, if their data are disclosed to government authorities in third countries without an adequate data protection regime.

It is a proven fact that Facebook is not transparent about essential purposes of the processing. This leads to a 100% probability of occurrence of this risk. The impact may be very high. Therefore the data protection risks for the data subjects are high.

16.1.4 *Loss of control due to further processing by Facebook*

Page administrators cannot prevent Facebook from processing personal data relating to a visit to a government Page for Facebook's own purposes. As shown in [Section 4.2](#) this involves at least 15 main purposes, with sub purposes.

Section 11.2 provides a detailed analysis why processing of the three identified categories of personal data for most of these purposes is incompatible with the purposes for which Dutch government organisations create a Page: to technically communicate with a mass audience, and to obtain insights in the effectivity of this communication through aggregate statistics. As assessed in [Section 13](#) Facebook's data processing does not comply with the principle of purpose limitation.

Facebook is capable of using these three categories of personal data to profile users for its own commercial purposes, including showing paid postings and advertisements in visitors' News Feed.

Because this further processing for incompatible purposes is a fact, the probability of occurrence of this risk is 100%, while the nature of the data entails significant risks to the fundamental rights and freedoms of the Page visitors. Therefore the data protection risks for the data subjects are high.

16.1.5 *Loss of control due to personal data sharing with third parties*

As described in Section 2.4 about cookies and device identifiers, Facebook uses tracking cookies, and reads unique identifiers from the end user devices, even if users object against tracking cookies by selecting 'essential cookies', and even if users log-out from their Facebook account. Facebook shares these personal data with third parties when government Page visitors visit outside websites that have (pixel based) interactions with Facebook, even if they do not click on any interaction option with Facebook such as a like or share button.

The amount of third parties that may gain knowledge about a government Page visitor is even larger. Research by the university of Washington has shown that by purchasing ads personal information about individuals can be extracted.²⁷⁶ This creates the risk that personal data about visits to government Pages are shared with unknown third parties, even in the absence of tracking cookies or device identifiers.

The way Facebook's data cookie work, leads to a real probability that outside companies and organisations can obtain information about government Page visits. Because the impact can be very high if such visits reveal special categories of data to such third parties, the privacy risks for the data subjects are high.

16.1.6 *Loss of control, re-identification of pseudonymised data due to disclosure to authorities in third countries*

Facebook transfers its data to data centres all over the world, including in third countries without an adequate data protection regime. In the HRIA this global accessibility is addressed as a human rights risk. In this DPIA, the risk assessment is limited to the current structural transfer of personal data to the USA. This transfer poses well known data protection risks, due the chance of undue access by US government authorities. In view of Facebook's high annual amount of data disclosures, there is a realistic chance that Facebook is compelled to disclose personal data from visitors to a government Page to US law enforcement, courts or secret services.

²⁷⁶ Paul Vines, Franziska Roesner, and Tadayoshi Kohno, Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob; Paul G. Allen School of Computer Science & Engineering, University of Washington (2017), URL: <https://adint.cs.washington.edu/ADINT.pdf>

The impact of such undue access depends on the nature of the data. The impact on data subjects in case of disclosure of their sensitive and special categories of personal data to US law enforcement or security services can be extremely high. This is due to the lack of notification and the lack of an effective means of redress for EU citizens.

It is reasonably likely that such disclosure happens, while the USA do not (currently) comply with the four essential data protection guarantees. The Irish DPC has already issued a provisional suspension of the data transfers. Hence, there is a high risk for the processing of personal data relating to a government Page that may reveal sensitive and special categories of data. This may change if the European Commission adopts a renewed (third) adequacy decision for the USA, but even if the USA release a new Executive Order of the President on 3 October 2022, it will take another 6 months for the adequacy decision to be adopted.²⁷⁷

16.1.7 *Filter bubble: missed messages*

The risk that messages posted on a (government) Facebook Page are not shown in the News Feed of Facebook users is also in scope of this DPIA. Facebook's algorithms determine which messages are shown in the News Feed of its users and the order in which they are shown. The algorithm personalises the content that is shown to the Facebook users. The algorithm filters out information that is deemed of little interest to specific users, providing them with content they are expected to consume. This is often referred to as the 'filter bubble'. If the algorithm does not show certain messages from a government organisation to individual Facebook users, this may result in the missing of possibly relevant information.

Because the workings of the algorithm are unknown, occurrence of this risk cannot be excluded. The impact on data subjects may vary, depending on the urgent nature of the missed content, but can be high. Therefore the data protection risk has to qualified as high.

16.1.8 *Chilling effect due to government access to Insights and activity log*

Page visitors could also fear recognition by Dutch government organisations, if Facebook would reveal their identity to the Page owners. This is not the case. As described in Section 2.3, the Insights presented to admins are aggregated to a sufficiently high level (at least 100 visitors) to prevent identifiability. The activity log, available for Page admins, does show identifiable data from visitors, but only if they left a publicly visible response to a posting on a Page. These visitors can know they have publicly posted, and are able to delete their comment.

Because the Insights are presented at an aggregate level, it is nearly impossible for Page admins to reidentify the individual visitors from Insights. Even though the impact of such reidentification could be very high, the data protection risk is low.

²⁷⁷ Politico, US expected to publish Privacy Shield executive order next week, 27 September 2022, URL: <https://www.politico.eu/article/us-expected-to-publish-privacy-shield-executive-order-next-week/>

16.2 Summary of risks

These circumstances and considerations as explained above lead to the following 7 high, and 1 low data protection risks for data subjects:

High risks

1. Inability to exercise data subjects rights
2. Chilling effect on other fundamental rights
3. Lack of transparency purposes of the processing
4. Loss of control due to further processing by Facebook
5. Loss of control due to personal data sharing with third parties
6. Loss of control, re-identification of pseudonymised data due to disclosure to US authorities
7. Filter bubble: missed messages

Low risk

8. Chilling effect due to government access to Insights

Table 9: Risk matrix based on the ICO model¹⁸⁴

Severity of impact	Serious harm	Low risk 8	High risk 2, 5, 6, 7	High risk 1, 3, 4
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

Part D. Description of risk mitigating measures

Following the Dutch government's DPIA model, Part D describes the proposed countermeasures against the data protection risks identified in part C.

The following section contains a table with the mitigating technical, organisational and legal measures that Facebook can take.

17. Risk mitigating measures

In section 16.2 of this report, eight data protection risks for data subjects have been identified. There are seven high risks and one low risk.

Facebook can mitigate all high risks, but it is unlikely that Facebook is willing to mitigate some of these risks, for example by drafting a joint controller agreement with Page owners for all relevant data processing, or with regard to the transfer of personal data to the USA. The most effective measure government organisations can take is to refrain from using Facebook Pages. They can take some other measures, but these measures cannot mitigate all high risks.

The German DPAs demand at least four measures if government organisations want to continue their Page:

1. the conclusion of an agreement pursuant to Art. 26 of the GDPR on joint controllership with Facebook,
2. sufficient information on the joint data processing vis-à-vis the users of the fan pages in accordance with Art. 13 of the GDPR,
3. proof of the permissibility of storing information in the user's terminal equipment and access to this information pursuant to Art. 25 TTDSG, as well as
4. proof of the permissibility of transferring personal data to the access area of authorities in third countries.²⁷⁸

The table below includes these and other measures both parties can take.

17.1 Measures against the seven high and one low risk

The table below shows the 7 high and 1 low data protection risks for data subjects, with the mitigating measures Facebook can take. Government organisations can take very few measures.

No	High risk	Measures government	Measures Facebook
1.	Inability to exercise data subject rights	Stop using Facebook Pages until Facebook provides meaningful access to the logic of its	Provide meaningful access to the logic of the personalised content, including inferences and interest predictions and enable users to remove wrong data. Create meaningful tooling to provide such access with each posting in the News Feed.

²⁷⁸ Decision from the Conference of German State and Federal DPAs, 23 March 2022 (in German), URL: https://datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf.

		data processing	
2.	Chilling effect on other fundamental rights	Make all information also available on public webpages, outside of the Facebook platform.	Provide access for vetted researchers to actual data processed by Facebook relating to popular government Pages, to investigate if following a government Page results in an increase or decrease of different views represented in the personalisation. Additionally, researchers must be able to perform A/B testing in an isolated lab, with model accounts. Currently, Facebook prohibits the use of test accounts.
		Warn Page admins to log-in with the Page Admin account after Page creation	
3.	Lack of transparency purposes of the processing	-	Amend the joint controller agreement for Insights to include all data processing related to government Page visits, from users and non-users, including inferred data and the prediction of the interests of users
			Do not force acceptance of data cookie for non-users
			Use privacy by default settings with regard to cookies for users. Do not use dark design patterns.
4.	Loss of control due to further processing by Facebook	If Facebook provides a data minimisation setting: use it	Create an opt-out for government Page admins for any further processing beyond the agreed purposes in the joint controller agreement
		If Facebook creates a control to limit data storage: minimise the retention period	Do not force acceptance of the data cookie
5.	Loss of control due to personal data sharing with third parties	Instruct visitors to empty the cookie jar in their browser after a visit to a government Page	Create a control for government Page admins to determine the retention period of the raw data relating to Page visits
			Do not force acceptance of tracking cookies
			Delete all Facebook cookies when users log out. Only read device IDs/cookies if there is an authentication cookie that signals that the user has logged in.
			Obtain <u>explicit</u> , informed consent for all tracking cookies, to take account of the sensitive nature of surfing data
6.	Loss of control, re-identification of pseudonymised data due	Stop using Facebook Pages (reconsider if	Obtain <u>explicit</u> , informed consent for all potential data transfers to third parties.
			Stop transferring personal data from Dutch government Page visitors to the USA. Reconsider the refusal to open a dedicated EU cloud

	to disclosure to US authorities	there is a new transatlantic data agreement)	Provide detailed statistics to Dutch government organisations about disclosure of personal data of visitors to Dutch government Pages
			Do not retain personal data about visits to Dutch government Pages longer than 1 week, and create weekly Insights.
7.	Filter bubble: missed messages	Invite Page visitors to subscribe to a dedicated mailing list or other non-algorithmic communication channel	Comply with Art. 29 of the DSA and offer users the option to select a non-personalised News Feed
			Enable users to opt-in to always receive messages from a government Page in the top 10 messages of the News feed.
No	Low risk	Measures government	Measures Facebook
8.	Chilling effect due to government access to Insights	No measures needed	Do not lower the aggregation level

Conclusions

The outcome of this DPIA is that there are 7 high and 1 low data protection risk when government organisations use a Facebook Page to communicate with a mass audience. This DPIA recommends a number of measures Facebook could take to mitigate these risks. Though government organisations can take some measures to partially mitigate some risks, government measures cannot mitigate all high risks. Even if the European Commission adopts a new adequacy decision for data transfers to the USA, Facebook's global data processing may still cause risks related to the accessibility of data in other third countries without adequate data protection.

This DPIA concludes that government organisations should stop using Facebook Pages if Facebook does not take measures to mitigate the high data protection risks. The Dutch government will immediately open a dialogue with Facebook.

Appendix 1

Response Meta to Dutch government DPIA on Facebook Pages²⁷⁹

According to Meta, the scope of the DPIA is too broad. The Dutch government is **only a joint controller for the Page Insights analytics**, not for any of the underlying data processing. A DPIA may only assess the data processing that is within the Dutch government's control. The DPIA incorrectly examines many processing activities that are exclusively under Meta Ireland's control. Privacy Company would ignore the differences between Facebook Pages and other cloud service providers.

According to Meta, the DPIA is of generally poor quality in terms of accuracy of legal analysis and facts. There are shortcomings in the technical analysis and **research methodology**, because Privacy Company only used 3 test accounts.

There is no **'transfer'** of personal data from the Dutch government to Meta in the USA: as the Insights analytics are directly generated by Meta Ireland, and were never in the possession of the Dutch government. Additionally, the European Commission has stated that all safeguards negotiated with the US government as part of the new Transatlantic Data Agreement are available for all transfers to the US.²⁸⁰

The assessment of the **legal grounds** in part B of the DPIA is incorrect. The DPIA incorrectly describes Meta's use of consent and other legal grounds. The DPIA incorrectly refers to an **opinion of an Advocate General of the CJEU** in a case brought by the German Federal Cartel Office against Facebook for other legal grounds without rigorous analysis. Meta claims that the statement that the legal ground of legal obligation does not appear to be relevant for this DPIA, is incorrect, without further explanation.

More importantly, according to Meta, **cookies** may not be addressed in a GDPR assessment, as they are regulated by the ePrivacy Directive, and not by the GDPR. Meta points out that the specific datr-cookie was not addressed in the CJEU ruling about the use of a Fanpage by Wirtschaftsakademie, only the general use of cookies.

The relevant data processing is **not likely to result in a high risk to the rights and freedoms of natural persons**. The DPIA mistakenly states that all data protection risks are automatically 'high' risk, because data protection is a fundamental right. Meta's criticisms of the high risks are detailed in the table below.

Table 10: Overview of Meta's responses to the high risks

High risk identified in the DPIA	Meta's response
Inability to exercise data subjects rights	Reference to access sources, including the 'Why am I seeing this Post' feature
Chilling effects on other fundamental rights	Entirely hypothetical situations, contradicts Meta's own Human Rights Impact Report

²⁷⁹ E-mail Meta to the Dutch Ministry of the Interior and Kingdom Relations, 11 November 2022.

²⁸⁰ Meta refers to European Commission, Questions & Answers: EU-U.S. Data Privacy Framework, URL: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_22_6045/QANDA_22_6045_EN.pdf.

Lack of transparency purposes of the processing	Easy to find and clearly structured in Terms of Service and Privacy Policy, and the 'Why am I seeing this' in every post and Ad, plus specific transparency about Page Insights joint controllership
Loss of control due to further processing	There is no controller-processor relationship between the Dutch government and Facebook, there is no 'further' processing because Facebook mentions all purposes of the processing in the Privacy Policy.
Loss of control due to personal data sharing with third parties	Meta only shares with third parties mentioned in the Privacy Policy
Loss of control, reidentification of pseudonymised data due to disclosure to authorities in third countries	Thanks to the signing of Executive Order of the President 14086 by President Biden on 7 October 2022, the protection of personal data is further enhanced, on top of the SCC.
Filter bubble: missed messages	Users can always switch to a chronological News Feed, or go to a specific Page to see all posts from that Page.

Response Privacy Company

Privacy Company performed a DPIA following the Dutch government DPIA model, **without any assumptions** about the role of Facebook or references to other DPIAs.

As explained in the DPIA, a data controller such as the Dutch government must perform a DPIA when the data processing is likely to result in a high risk for data subjects. By creating a specific government Page on Facebook, the government factually enables Meta to process Page visitor data for its own commercial and profiling purposes, including the tracking cookies set by Meta. Meta does not want to act as a data processor for Pages, nor as a joint controller. That means **Meta is a third party**, a recipient of the Page visitor data. The DPIA requirement is not limited to the data processing by joint controllers or by data processors, but must also address the risks for data subjects if data controllers were to give, sell, lease or otherwise provide personal data to third parties.

The GDPR makes data controllers responsible and accountable that all data processing they initiate is performed in accordance with this Regulation (Article 24), and hence, they **must also perform a DPIA for such disclosure**. Disclosure to a marketing company can lead to high data protection risks, as described in the first criterion of *evaluation or scoring* in the EDPB adopted guidelines on DPIAs.²⁸¹ This example includes: *"a company building behavioural or marketing profiles based on usage or navigation on its website."*

²⁸¹ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, URL: <https://ec.europa.eu/newsroom/article29/items/611236>.

The GDPR specifies in Article 35(1) that a DPIA is “*an assessment of the impact of the envisaged processing operations on the protection of personal data*”. It is not only possible but common that some of the impact of processing personal data is an indirect result of the processing. Assessing the impact of processing is therefore not possible without also **assessing the context** in which the processing takes place. In this case, by one of the largest advertising networks in the world.

The perceived problems with the research **methodology** are documented in the DPIA and HRIA. Due to the lack of cooperation and transparency by Meta the tests were limited to small scale black box testing. Meta also does not allow mass automated account creation. The DPIA explains that due to this restriction, it is not possible to create sufficient accounts for statistically relevant testing.

With regard to **transfers**, Meta’s arguments are without merit. First of all, Meta can only create these statistics based on the underlying personal data processing from Page visitors with and without a Meta account. As a result of both Schrems-rulings from the CJEU Meta is well aware that transfer can take place because personal data are transferred within a group with data centres and offices outside of the EEA, especially the USA. As quoted in Section 7 of the DPIA Facebook systematically transfers personal data from its EU customers to the USA. The European Commission has not yet issued a new adequacy decision for the USA: this will first have to be approved by the EDPB.

Section 11.2 of the DPIA elaborates on the **risks of further processing by a third party if Meta is not a joint controller with the Dutch government**. The DPIA assesses the legitimacy of this ‘further’ processing by analysing all the elements of the compatibility test in Article 6(4) of the GDPR, and concludes that Meta’s further processing of the website data for its own commercial purposes is not compatible with the purpose for which the Dutch government allows the network to collect the visitor data: provide the Page functionality and to create web analytics.

With regard to the reference to the **AG Opinion**, the DPA carefully explains that the analysis of the four remaining legal grounds is informed by (but not based on) the reasoning in that opinion, but also informed by the November 2021 ruling from the German appellate court in the famous Schleswig-Holstein Fan Page court case that Facebook cannot invoke any legal ground for its current data processing, in particular as a result of the use of cookies for which consent is required.

The DPIA specifically assesses Meta’s use of **cookies**, as did the CJEU in two cases, and as did the German data protection authorities in their recent advise to the German government to stop using Facebook Pages. The DPIA explains that the Dutch implementation of the ePrivacy Directive contains a legal presumption that the use of tracking cookies involves processing of personal data, and hence, the GDPR applies to the processing of personal data obtained through such tracking cookies. Facebook already applied a datr-cookie in 2011, when the DPA of Schleswig Holstein ordered an academy to stop using a Facebook page.²⁸² Even though the CJEU does not specifically mention the name of any cookies, the case was clearly about the use of the datr-cookie.²⁸³ On 10 November 2022, the German data protection authorities

²⁸² <https://www.itsagadget.com/2011/10/facebook-privacy-issues-persist-and-datr-cookie-is-back-on-track.html>

²⁸³ See for example the general letter from 3 November 2011 of the Schleswig-Holstein DPA calling on Germans organisations to stop using Facebook Pages, URL:

have expanded and updated their analysis of joint controllership between Facebook and the Page owners, based on the use of tracking cookies.²⁸⁴

Finally, the table below refutes criticisms from Meta about the high risks.

Table 11: Response Privacy Company to Meta's view on the high risks

High risk identified in the DPIA	Facebook's response	Privacy Company response
Inability to exercise data subjects rights	Reference to the same access sources quoted in the DPIA, including the 'Why am I seeing this Post' feature	All sources mentioned by Meta were already quoted in the DPIA, and assessed as insufficient. The 'Why am I seeing this?' interface does not provide access to the algorithmic logic.
Chilling effects on other fundamental rights	Entirely hypothetical situations, contradicts Meta's own Human Rights Impact Report	The HRIA provides evidence of the bias in the timeline. Because Meta does not give access to the underlying algorithmic logic or data, other likely impacts could not be proven or rejected. The HRIA outlines how this research can be done. This type of research is not present in the Human Rights Impact Reports Meta has published.
Lack of transparency purposes of the processing	Easy to find and clearly structured in Terms of Service and Privacy Policy, and the 'Why am I seeing this' in every post and Ad, plus specific transparency about Page Insights joint controllership	All purposes must be 'specified'. Hence, there must be a limitative list. This is not the case. The 'purposes of the processing are described in several layers in Facebook's new Privacy Policy. Additionally, Facebook mentions other purposes for the processing of observed data through cookies in its Cookie Policy.

<https://www.datenschutzzentrum.de/artikel/1190-Musterverfuegung-nach-38-Abs.-5-BDSG.html#extended>. The datr cookie is mentioned in the first sentence of the reasons for the ban. The DPA writes: "Der Cookie „datr“ ist für zwei Jahre aktiv, sodass auch dann eine namentliche Zuordnung über diesen Zeitraum möglich ist, wenn ein zunächst nicht angemeldeter Nutzer sich innerhalb der Aktivitätszeiträume des Cookies bei Facebook anmeldet. Facebook verarbeitet die gewonnenen Nutzungsdaten zu pseudonymen Nutzungsprofilen. Es liegt in diesem Zusammenhang ein Verstoß gegen § 15 Abs. 3 Satz 3 TMG vor, da Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen."

²⁸⁴ Taskforce Facebook Fanpages, Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages, 10 November 2022, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Kurzgutachten_Facebook-Fanpages_V1_1_clean.pdf.

Loss of control due to further processing	There is no controller-processor relationship between the Dutch government and Facebook, there is no 'further' processing because Facebook mentions all purposes of the processing in the Privacy Policy.	The Dutch government only wants to open a Page to communicate with platform users and obtain visitor analytics. Processing for Meta's own purposes is 'further' processing of these visitor data. There is no limitative list of specified purposes.
Loss of control due to personal data sharing with third parties	Meta only shares with third parties mentioned in the Privacy Policy	The Privacy Policy describes sharing of information with Partners (advertisers), vendors (measurement and marketing vendors), service providers and third parties (external researchers, law and copyright enforcement (in response to legal requests, to comply with applicable law or to prevent harm.) These are very broad categories of recipients.
Loss of control, reidentification of pseudonymised data due to disclosure to authorities in third countries	Thanks to the signing of Executive Order of the President 14086 by President Biden on 7 October 2022, the protection of personal data is further enhanced, on top of the SCC.	As the Dutch data protection authority reiterates in two recently published letters about the use of cloud providers the risks of transfer also occur when data are transferred within a group outside of the EEA or when entities outside of the EEA obtain access to these personal data. ²⁸⁵ The DPIA contains a specific risk analysis of both types of transfer.
Filter bubble: missed messages	Users can switch to a chronological News Feed, designate a certain Page as one of the "Favourites" and see a separate Favourites Feed, or go to a specific	Facebook has introduced an option for users to select a chronological news feed end of July 2022 ²⁸⁶ , while testing for the DPIA ended on 30 March 2022. The chronological setting only works for a short period of

²⁸⁵ The Dutch DPA writes in a letter about the use of cloud providers, z2022-00846, dated 10 November 2022: "*Doorgifte kan ook plaatsvinden doordat persoonsgegevens binnen een groepsonderneming, of via een leverancier, worden doorgezonden naar landen buiten de EER. Van doorgifte is tevens sprake als entiteiten uit landen buiten de EER toegang krijgen tot persoonsgegevens.*" URL:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_over_inzet_cloud_service_providers.pdf.

²⁸⁶ BuzzFeed, Facebook Is Finally Giving People A Non-Algorithmic News Feed, 21 July 2022, URL: <https://www.buzzfeednews.com/article/katienotopoulos/facebook-chronological-home-feed>

	Page to see all posts from that Page.	time. ²⁸⁷ After that, Facebook reapplies the algorithmic sorting. The main 'filter bubble' risk is not caused by information that's not accessible but by information that is selectively and structurally provided to a person by default.
--	---------------------------------------	--

²⁸⁷ Facebook, How do I see the most recent posts in my Feed on Facebook?, URL: https://www.facebook.com/help/218728138156311/?helpref=related_articles. Facebook explains: "You can sort your Feed to see recent posts, but Feed will eventually return to its default setting."