Tracking the Evolution of Cookie-based Tracking on Facebook

Yana Dimova*
imec-DistriNet, KU Leuven
Leuven, Belgium
yana.dimova@kuleuven.be

Gertjan Franken*
imec-DistriNet, KU Leuven
Leuven, Belgium
gertjan.franken@kuleuven.be

Victor Le Pochat*
imec-DistriNet, KU Leuven
Leuven, Belgium
victor.lepochat@kuleuven.be

Wouter Joosen
imec-DistriNet, KU Leuven
Leuven, Belgium
wouter.joosen@kuleuven.be

Lieven Desmet
imec-DistriNet, KU Leuven
Leuven, Belgium
lieven.desmet@kuleuven.be

ABSTRACT

We analyze in depth and longitudinally how Facebook's cookie-based tracking behavior and its communication about tracking have evolved from 2015 to 2022. More stringent (enforcement of) regulation appears to have been effective at causing a reduction in identifier cookies for non-users and a more prominent cookie banner. However, several technical measures to reduce Facebook's tracking potential are not implemented, communication through the cookie banner and cookie policies remains incomplete and may be deceptive, and opt-out mechanisms seem to have no effect.

CCS CONCEPTS

• **Security and privacy → Social network security and privacy**; **Human and societal aspects of security and privacy**.

KEYWORDS

web tracking; cookies; social network; online privacy

ACM Reference Format:
Yana Dimova, Gertjan Franken, Victor Le Pochat, Wouter Joosen, and Lieven Desmet. 2022. Tracking the Evolution of Cookie-based Tracking on Facebook. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society (WPES '22), November 7, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3559613.3563200

1 INTRODUCTION

Facebook[1] has been one of the most scrutinized technology companies with regard to user privacy. One aspect is its perceived ability to track both users and non-users[2] online, primarily through the presence on third-party websites of embedded Facebook resources, such as its pixel and social plugins. People have specifically identified Facebook and its tracking ability across the web as causing them discomfort [21].

Cookies are the main technical vector of concern, as they could allow linking website visits to a specific person. Initially, Facebook stated that it "do[es]n't use [cookies] for tracking and they're not intended for tracking" [35], and provided transparency on its cookie usage [89]. Facebook contributed detailed insights on its cookies to the 2011 [70, 76] and 2012 [71, 77] audits by the Irish Data Protection Commissioner. In 2011, after an independent researcher found that cookies persisted even after a user logged out, Facebook further explained the cookies it used and clarified that they were not intended nor used for tracking [23, 25].

Since then, with a shift to interest-based advertising, first in 2014 for its users [62] and later in 2016 also non-users [13], Facebook seemingly pivoted to tracking and profiling people across the web [89]. Data protection authorities (DPAs) took note, and continued investigating how Facebook uses cookies for potential tracking. In 2015, the Belgian DPA singled out the `datr` cookie as a tracking vector in its recommendations and court cases, and demanded that Facebook stopped setting this cookie for non-users [1, 2, 85]. Facebook responded that this cookie was used only for security purposes and not tracking [90], but complied with the Belgian DPA's order by disabling the `datr` cookie in Belgium [91], until the order was reversed in appeals [74]. The French DPA fined Facebook in 2017 for "engag[ing] in unlawful tracking, via the *datr* cookie" [18], and again in 2022 for not allowing users to refuse cookies as easily as accepting them [20]. Since then, new privacy legislation, such as the General Data Protection Regulation in Europe, imposed further restrictions on how Facebook can treat personal data, such as requiring consent for storing and collecting cookies.

In this paper, we longitudinally measure the evolution of Facebook's cookie-based tracking from the Belgian DPA order in 2015 until July 2022. We observe how Facebook responded to the DPA investigations and new privacy legislation, by analyzing when Facebook implemented changes to its cookie setting practices. We study in depth how both users and non-users may receive Facebook's cookies, and subsequently become susceptible to tracking across the websites that incorporate Facebook's third-party resources.

Based on four technical reports of Facebook's cookie usage, we see how Facebook has restricted its cookies for non-users over time. Whereas in 2015, Facebook automatically set cookies (including `datr`) whenever a non-user visited their website, by 2018, interaction was required. In 2022, a cookie banner forces non-users to explicitly consent to cookies. This has a cascading effect on tracking on third-party websites: whereas in the past, there had been

*These authors contributed equally to this research.
[1]In October 2021, the parent company of the Facebook social network renamed itself from Facebook, Inc. to Meta Platforms, Inc., or Meta for short. Throughout this paper, we use the term Facebook to refer interchangeably to the website and the company that operates it.
[2]We use the term 'users' for people who have registered a Facebook account, and 'non-users' for people without a Facebook account (Section 2.2.1).

WPES '22, November 7, 2022, Los Angeles, CA, USA

scenarios in which Facebook would set and afterwards collect cookies that could uniquely identify a non-user, this is no longer the case. Facebook users received the `fr` cookie – used for targeted advertising – automatically in 2015, but can now reject this cookie if they decline 'optional' cookies.

Despite this progress, certain aspects of Facebook's cookie setting practices remain inadequate to guarantee privacy. The cookie banner only offers choices that will result in uniquely identifiable cookies being stored in the browser, including the `datr` cookie, which Facebook considers essential. This banner also appears to deploy dark patterns to favor a more privacy-invasive choice. Moreover, despite the technical means to do so, Facebook does not restrict its identifier cookies to the `facebook.com` domain only. If a (non-)user accepted cookies from Facebook, these are therefore sent to Facebook on every visit to a third-party website with a Facebook resource. Finally, opting out of targeted ads does not appear to impact identifier cookies and the associated tracking capabilities for both non-users and users.

Our work is designed as a case study of the dynamic nature of online tracking practices, and the effects of external pressure on user privacy, with Facebook only being one example of a major online platform that could engage in tracking. With our in-depth case study of Facebook's cookie-based tracking over time, we complement the prior work that broadly analyzed tracking prevalence across the web [4, 36, 58, 78]. Our detailed and longitudinal analysis provides a unique view into how actions by legislators and regulators concretely impact tracking behavior. Moreover, our study serves as a historical documentation of Facebook's cookie policies and behavior; as we show, these change frequently and may therefore be difficult to observe retroactively.

Our paper is structured as follows. We start with background (Section 2) and a description of our methods (Section 3). We then analyze tracking for non-users of Facebook (Section 4), studying which behavior causes cookies to be set, and how non-users are informed through a cookie banner and additional policy documents. Afterwards, we compare with tracking for Facebook users (Section 5), studying cookie setting as well as how users can (re)configure their cookie settings. We conclude with a discussion on how Facebook's cookie-based tracking evolved over time as a response to legal developments (Section 6), and an overview of related work (Section 7).

2 BACKGROUND

2.1 Technical context: cookie-based tracking

2.1.1 HTTP cookies. Cookies add stateful information to the stateless HTTP protocol [99], e.g., for session management. A cookie is a small unit of (textual) data that is typically sent by a website to be stored inside a user's web browser. Cookies can either be set through the `Set-Cookie` response header, or through JavaScript by modifying the `document.cookie` property. As a result, all cookies set by a website will be automatically included in the `Cookie` request header for every subsequent request to that website, until the cookie expires.

2.1.2 First-party and third-party cookies. A web page hosted on a certain domain will typically embed resources hosted on other domains. For example, a page may include images or scripts hosted on a CDN. As mentioned before, the requests for those resources will contain the cookies set for the domain on which they are hosted. If the domain of the currently visited website (i.e., the domain in the browser's address bar) and the domain of the loaded resource are the same, the request is said to be in a *first-party* context, and the cookies of that domain are referred to as *first-party* cookies [68]. In a first-party context, a website (such as Facebook) can store cookies in the visitor's browser and then collect them back on visits to a web page within that website's domain (e.g., `www.facebook.com`). If the domains of the visited website and loaded resource differ, the request is said to be in a *third-party* context, and the cookies of the domain from which the resource is loaded are referred to as *third-party* cookies. Note that this third party is still unable to access the cookies of the first party, since cookies are restricted to a specific root domain.

A third-party cookie can be used to track user visits across multiple first-party websites, when those first-party websites all embed resources from the same third party [31]. If such a cookie contains a unique identifier for a user, that cookie and identifier will be sent along with all third-party requests, regardless of the first party that embeds the third party's resource. The third party can therefore perform cross-site tracking to create a user profile, especially when the third-party request contains the URL of the first party's web page, e.g., in the `Referer` header, or in a parameter of the request.

2.1.3 Security and privacy-related cookie attributes. Due to security and privacy issues where cookies in cross-site requests enable session hijacking or the leaking of information across websites, certain cookie attributes can restrict the type of requests that cookies are sent along with [83]. The `Secure` attribute causes cookies to only be sent with requests made over a secure HTTPS connection. This prevents them from being intercepted by an intermediate party on the connection ('manipulator in the middle', MitM). If the cookie contains a unique user identifier, this would enable that party to track all requests by the user or act on their behalf.

The `SameSite` attribute indicates in which contexts the cookie will be added to a (cross-site) request. When the value is `Strict`, cookies are only sent along with requests in a first-party context. Note that this means that cookies are not sent along with the first request to a site when navigating to that site through a link from another domain. When the value is `Lax`, cookies are sent along with requests in a first-party context and with top-level navigations to a website. If no `SameSite` attribute is set, modern browsers default to this `Lax` value. When the value is `None`, the cookies can be sent in a third-party context, i.e., also with requests for resources embedded on another website. In order to enable third-party tracking through cookies, a third-party domain must explicitly set this `None` value for its cookies [31].

2.2 Facebook context

2.2.1 Users versus non-users. We distinguish between Facebook *users* and *non-users*. Facebook users are Internet users who have explicitly registered an account on Facebook. These users can therefore access the full functionality of the Facebook website. Non-users have not gone through such a registration process, therefore do not have a Facebook account, and as such cannot log in to Facebook.

2.2.2 Embedded Facebook resources. Facebook provides resources to website developers that these can embed on their website to add functionality. Facebook subsequently operates in a third-party context on those websites, and could use third-party cookies to track visitors. In our analysis, we consider the following resources:

The *Facebook pixel/Meta pixel*[3] allows to "track visitor activity on a website". The website can call pixel functions to track events such as page visits, searches, or product purchases. In the remainder of the paper, we refer to this unambiguously as the Facebook pixel.

Social plugins[4] are a variety of buttons and plugins that enable social interactions from within a website. These include the 'Like' and 'Share' buttons to share a web page on Facebook, and the 'Page' plugin to embed a frame with page information.

2.3 Legal context

GDPR and cookies. In 2016, the European Union passed the General Data Protection Regulation (GDPR) [75], one of the strictest privacy legislations worldwide. The GDPR requires processing of personal data to have a specific legal basis, of which consent is the only appropriate basis for the purpose of online tracking and user profiling [6, 41, 102]. On top of this, the ePrivacy directive [32], a *lex specialis* from 2002 that remains in force next to the GDPR, requires consent specifically for placing cookies that are not necessary or essential for providing a service. Therefore, consent must be obtained from the user, prior to the use of tracking cookies. The user must also be informed about the specifics of the data processing and their rights. In short, essential cookies (e.g., session cookies) do not require user consent, while explicit consent is required for cookies used for online tracking, profiling and advertising.

Conditions for valid consent under the GDPR are strict. One requirement for consent is that it must be freely given, i.e., with a clear and affirmative action. For instance, presenting consent under the form of a pre-ticked checkbox, does not meet this requirement [38]. Moreover, consent must be unambiguous and provided in an intelligible and easily accessible form, and it must be as easy for someone to withdraw their consent as it is to give it. Consent may not be bundled together for different cookie types as a take-it-or-leave-it choice, but rather the user should be able to decide for which cookie types they want to opt in [40].

The GDPR applies to all processing of personal data of European citizens, whether or not the company is based in the European Union. Therefore, all businesses which provide a service in Europe, including Facebook, need to comply with the regulation.

Other soft law. In 2011, the Irish Data Protection Commissioner (DPC) audited Facebook's data protection practices [76], at the time under the 1995 Data Protection Directive [33]. The DPC recommended, a.o., limiting data collection via social plugins, improving user privacy controls, and making the privacy policies simpler and more accessible. In the DPC's 2012 re-audit [77], they found that "most of the recommendations ha[d] been fully implemented".

In 2015, after a change in Facebook's cookie and privacy policy, the Belgian Privacy Commission (BPC; the predecessor of the Belgian DPA) fined Facebook, alleging that Facebook's cookie usage was in violation of Belgian privacy law. The violations consisted of tracking of users and non-users of Facebook on websites with a Facebook social plugin using cookies, without having obtained valid consent. They issued a recommendation [1], requesting Facebook to cease all tracking of non-users as well as users with deactivated or deleted accounts, unless the visitor had selected an unambiguous opt-in consent option. Facebook was also advised to offer privacy-friendlier social plugin integrations on third-party websites, which would not automatically send personal data through cookies to Facebook upon visiting the website. Facebook also had to provide more transparency about their cookies. The BPC updated their recommendation in 2017 [2], since Facebook had changed their cookie practices after 2015. This recommendation addressed roughly the same issues, in more depth. The court case is still ongoing in 2022 after a dispute over jurisdiction. We refer the interested reader to legal articles that give more context on the case proceedings [27, 28, 42, 85, 95, 101].

Table 1: Reports considered for our in-depth analysis of Facebook cookies.

	Measurement			
Year	Start	End	Country	Reference
2015	2015-03-01	2015-03-31	Belgium	[5]
2017	2016-11-29	2017-02-23	Belgium	[43]
2018	2018-06-14	2018-07-06	Belgium	[46]
2022	2022-01-11	2022-02-22	Belgium	[45]

3 METHODS

3.1 Data collection

We base our in-depth analysis of the evolution of Facebook's cookie setting practices on four technical reports (Table 1), which were written for the Belgian DPA's case. These reports give a detailed description of observations of cookies set by Facebook, and cover scenarios such as the tracking of non-users, the tracking of Facebook users who are signed in or signed out, and the functioning of the 'opt-out' mechanisms proposed by Facebook. In general, the scenarios in these reports were analyzed through manual interactions with the Facebook website, executed in contemporaneous browsers and in virtualized environments that were reset between experiments to ensure a clean profile and isolate the effects of the interactions. A number of Facebook accounts were created for the experiments that required logged-in users. Through a browser extension, every change (creation, modification, and deletion) made to the cookie jar of the `facebook.com` domain was logged. Where relevant, the network requests to the `facebook.com` domain were examined through the browser's developer tools.

3.2 Defining cookie-based tracking

Third-party web tracking, or behavioral tracking, commonly refers to practices that relate to the observation of browsing activity across multiple websites by a third party unrelated to those websites, although it is not a strictly defined term. Tracking breaks down into two major components: the *technical ability* to observe user activity, and the *intent* to actually record and use that activity. The

[3] https://developers.facebook.com/docs/meta-pixel
[4] https://developers.facebook.com/docs/plugins/

term 'tracking' can then alternatively refer to only the ability, or both the ability and intent.

The presence of the technical ability to track is relatively easy to measure: by analyzing whether third parties assign unique identifiers to users, store those identifiers in the user's browser, and collect those identifiers while users visit other websites, one can reasonably infer that those identifiers and visits *could* be collected and used to assemble a profile of one user's behavior. Yu et al. [104] develop their approach on such a model of ability. As long as a service sends *'unsafe'* data, defined as data that is only sent by a small number of users, they consider that there is a privacy risk for which mitigation is necessary. Coincidentally, they give Facebook's `datr` cookie as an example of a cookie where the intent may not be tracking, but the uniqueness still provides the ability to track users, possibly unintentionally. Mayer et al. [66] also consider tracking as the *collection* of browsing history, and develop a model of potential harms that arise from such collection. Roesner et al. [78] analyze the tracking *capabilities* of services, and state that they "do not distinguish between *"can track"* and *"does track"*". They give Facebook as an example of a 'personal tracker', i.e., a cross-site tracker that the user voluntarily visits directly, which causes the tracker-owned cookies to be set and then observed on other sites that include social plugins from that tracker.

Conversely, analyzing the intent of web tracking is more difficult: tracking companies essentially operate as a black box. The use of tracking for targeted advertising receives the most scrutiny, although tracking can also be used for less privacy-invasive purposes [93]. Through technical means, the use of browsing history to target ads could be inferred through audits and controlled experiments, although this may not constitute definitive proof. For example, multiple artificial user profiles could be built on certain online activity, after which the ads seen by those profiles can be analyzed to determine whether they are different between or targeted towards those profiles [9, 15, 57, 61]. Listings of user interests inferred through tracking, as provided by trackers to users, serve as more explicit proof that tracking occurs and is used for ad targeting [10]. Finally, privacy or cookie policies can contain statements that a service builds and uses a user profile for ad targeting (or does not), although such statements could be incorrect or incomplete [12], and the lack of such documentation does not confirm that observing browsing activity is *not* intended for or does not result in constructing a user profile. Even if a third-party service does not intend to track, other parties may still abuse the presence of unique identifiers. For example, in their surveillance threat model, Englehardt et al. [37] discuss how passive eavesdroppers such as nation-state surveillance could track users by observing their unique third-party identifiers across multiple websites.

Throughout our analysis, we discuss the cookies that Facebook sets and uses. To avoid an immediate classification as a 'tracking cookie', we designate **'identifier cookies'** as an intermediate. We consider a cookie to be an identifier cookie if it meets two criteria: it must be *persistent* and *uniquely identifying*. We consider a cookie persistent if it remains stored in the browser for a sufficiently long period of time. The longer the cookie remains stored in the browser, the longer it can be used to track a single user, since the browser will send this cookie with every request to the website. In our analysis, we use 90 days as a threshold for persistence; this value has also been used in prior work [36, 37, 55, 103]. We consider a cookie uniquely identifying if the value of the cookie is unique for one visitor, or is sufficiently specific that it is unlikely that two visitors will get the same value. This cookie can be used to link a request for a resource to one specific visitor, allowing to build the browsing history of that person across websites. Note that prior work has used the presence of such identifier cookies to label services as 'trackers' [37, 104], and our definition aligns with such a designation. Conversely, we cannot infer whether the cookie has a tracking intent from its lifetime and composition alone. In our discussion (Section 6), we assess in more depth whether there is any indication that Facebook uses (certain) cookies to profile users.

A last element for assessing a service's tracking potential is its reach. A tracker will only be able to build a meaningful user profile if it can observe visits across a large number of third-party websites. Facebook readily meets this requirement, having historically been present as a third party on around a third of top websites [24, 31, 35, 36, 65, 78].

3.3 Limitations

We select Facebook as a case study of online third-party tracking by a large technology company. Online tracking is supported by a large industry [17], among which figure most large online platforms. We do not compare Facebook's cookie-based tracking to any other company's tracking behavior, and make no statements about whether Facebook is better or worse at user tracking.

Our analysis of potential tracking by Facebook is scoped to consider only cookie-based tracking. We therefore do not consider other technical forms of tracking which do not use cookies, such as browser fingerprinting [34], Adobe Flash cookies [87], evercookies [4], the HTML5 `localStorage` API [7], and CNAME-based tracking [30]. We also do not consider tracking of user actions on Facebook's site itself, nor the privacy implications of users voluntarily sharing their data with Facebook on the platform itself [52].

Our analysis relies on snapshots of Facebook's cookie-related behavior. We therefore cannot observe changes in between, and do not have empirical evidence for the timing when changes observed from one report to another have been implemented. Where available, we complement our observations with external resources, such as blog posts or archived web pages, to more precisely pinpoint when Facebook implemented changes to its cookie-related behavior. Moreover, Facebook may change its behavior at any future time.

The measurements in the reports that we analyze were all conducted on the desktop version of Facebook's website. We therefore cannot observe tracking on mobile devices, either through the mobile version of the website (`m.facebook.com`) or the Facebook mobile app. On third-party websites, we did not interact with their cookie banners. We therefore do not observe whether accepting or rejecting (certain types of) cookies there affects cookie setting by Facebook. We base our findings on websites that – potentially despite a cookie banner – load Facebook resources and trigger requests to Facebook immediately upon page load.

Our measurements are primarily conducted from Belgium. Facebook may adapt its tracking behavior depending on the jurisdiction, in particular since different legislation may apply. In our case, since Belgium is a European Union member state, the GDPR applies there.

Moreover, some resources that we analyze are localized, in particular in Flemish (Belgian Dutch). Some screenshots in this paper therefore show the Flemish version of Facebook's website. To the extent where it is possible, we add the English version of these prompts by retrieving them from online resources such as publicly available screenshots.

4 NON-USERS OF FACEBOOK

In this section, we study whether Facebook stores cookies for a non-user, and how Facebook informs non-users about these cookies. First, we monitor which cookies were observed after a non-user visits Facebook's website, using the home page as a proxy for any page on the `facebook.com` domain; Facebook's privacy-related policy pages; and other websites that include Facebook resources as a third party (Section 4.1). We focus on the most interesting cookies from a tracking viewpoint, i.e., cookies that can be used as identifiers, or are otherwise related to a non-user's privacy choice. For completeness, the overview in Table 3 lists all cookies that have been observed in at least one of the four analyzed reports, including session (i.e., non-persistent) cookies or cookies that are not sufficiently unique to be usable as an identifier. Next, we analyze how Facebook communicates about cookies through cookie banners, the main description of cookies that a regular non-user will see (Section 4.2). Finally, we analyze the full privacy-related policies that non-users (and users) can consult after following a link from the home page or cookie banner (Section 4.3).

4.1 Cookies set by Facebook

4.1.1 Visiting the Facebook homepage. In this scenario, a non-Facebook user visits Facebook's homepage (`www.facebook.com/`) for the first time. In 2015, without any interaction, the page load automatically led to setting the `datr` cookie, with a 2-year lifetime and consisting of a 24-character random-looking string, therefore meeting our definition of 'identifier cookie' (Section 3.2). Facebook's cookies policy states that the `datr` cookie "identifies browsers for purposes of security and site integrity, including for account recovery, and identification of potentially compromised accounts".

By 2018, Facebook had stopped setting cookies automatically upon page load. Instead, cookie setting depended on which parts of the page a user interacted with. The home page, which invites a person to create a Facebook account, contained certain zones which had a `data-nocookies` attribute set in HTML. Clicking any of these zones did not lead to cookie setting. These zones are marked in purple on Figure 1, and consist mostly of statements about and links to Facebook's privacy-related policies, giving the appearance that a non-user is allowed to first read these policies without already receiving cookies. These zones were not visibly marked when visiting the page, and a non-user would have had to consult the HTML source code of the page to find the elements with a `data-nocookies` attribute that would not result in cookie setting upon interaction.

Clicking outside the specially marked zones led to Facebook setting the `datr` cookie and, in contrast to 2015, also an `sb` cookie. This `sb` cookie has a 2-year lifetime and is a 24-character random-looking string, qualifying as an identifier cookie, similarly to `datr`. Facebook's cookies policy states that the `sb` cookie "identifies browsers for login authentication purposes". These cookies are

Figure 1: The Facebook home page in 2018. If a non-user clicks zones marked in purple, no cookies are set. If a person clicks outside these zones, four cookies are set.

set without the need to reload the page. The (future) values for `datr` and `sb` are sent in the body of the initial page load request as a `DeferredCookie`, and the cookies are set by an event listener upon clicking. This means that Facebook already assigns the unique identifier to the non-user upon page load, but only persists it to the browser once the non-user consents to cookie setting.

In 2017 and 2018, when visiting the Facebook home page from another country, in this case France, an interaction similar to the one required to trigger the `datr`/`sb` cookies above also caused an `fr` cookie to be set. This `fr` cookie had a lifetime of 90 days and consisted of a 52-character random-looking string, qualifying as an identifier cookie. Facebook's cookies policy states that the `fr` cookie is "Facebook's primary advertising cookie, used to deliver, measure and improve the relevancy of ads". The value for `fr` was sent in the body of the initial page load request as a `DeferredCookie`. In 2018, the `fr` cookie was also set from Belgium (after interaction) if the Facebook domain was visited through an advertisement seen when searching for the term 'facebook' in the Google search engine. This advertisement did not lead to the home page, but instead to the `https://www.facebook.com/campaign/landing.php` page. This suggests that Facebook may have applied a special, narrow configuration for its cookie setting behavior in Belgium, restricting cookies only for the home page. These observations also suggest that Facebook was both able and willing to adapt its potential tracking behavior to specific countries and interactions.

By 2022, the page load still did not automatically trigger cookie setting. Moreover, a cookie banner blocks any interaction with the login/registration form on the home page. We discuss the composition of this cookie banner in more detail in Section 4.2.1. This cookie banner ultimately provides the non-user with two explicit choices: accept only essential cookies, or both essential and optional (i.e., 'all') cookies. A third option for the non-user would be to navigate away from the page and not accept any cookies at all. Without

making an explicit choice, the non-user cannot continue using the home page. Selecting only essential cookies initially only results in the `datr` cookie being set, with the same lifetime, composition, and purpose as in 2015. Consequently, Facebook considers the `datr` cookie with its "security and site integrity" purpose essential to the operation of its website. However, upon reloading the page, the `sb` cookie is also set, with the same lifetime, composition, and purpose as in 2018 and 2015 respectively. Selecting essential and optional cookies initially also only results in the `datr` cookie being set; reloading also adds the `sb` cookie. As was the case in 2018, the values for `datr` and `sb` are still assigned upon page load and sent in the body of the initial request as a `DeferredCookie`. It appears that Facebook uses the presence of the `datr` cookie to determine whether a non-user has consented to cookies, as deleting this cookie makes the cookie banner reappear.

In summary, cookie setting for non-users who visit the Facebook home page for the first time evolved to require more (explicit) consent. While in 2015, merely visiting the home page resulted in uniquely identifiable cookies being set automatically, by 2017 cookie setting required interaction with the page, albeit under the assumption that any interaction except for consulting policy pages meant implicit consent to set cookies. By 2022, this consent has become more explicit, requiring a non-user to make an active choice to accept cookies before they can continue visiting (the home page of) Facebook.

4.1.2 Visiting policy pages. As mentioned above, the Facebook home page links to several pages that allow a non-user to consult Facebook's policies related to privacy and cookies in more detail. We analyze these policies in more detail in Section 4.3. In 2015, cookies were set automatically upon loading the home page, so these cookies would naturally be set already whenever a non-user follows the links to the policy pages. A direct visit to the data policy page, without a prior visit to the home page, resulted in the `datr` cookie being set (for the first time). In contrast, in 2018, the zones on the home page with links to these policy pages were explicitly configured to not result in cookie setting. When following these links, initially no cookies were set either. However, some interactions with the policy pages would result in cookie setting, either directly or through redirection to other pages. In 2018, four links on the data policy page led to a page on `research.fb.com`, which loaded the Facebook pixel and caused an `fr` cookie to be set (Section 4.1.3). Clicking on the cross in the cookie banner, or the header with the Facebook logo (which would lead the non-user back to the home page) on both the cookie and data policy pages resulted in the `datr` and `sb` cookies being set. Clicking the whitespace to either side of (only) the data policy page also resulted in these cookies being set (Figure 2). In 2022, no interaction with the cookie or data policy pages ever led to cookies being set, except for clicking any of the two buttons in the non-blocking cookie banner at the bottom of the page (Section 4.2.2).

4.1.3 Visiting web pages with Facebook resources without a prior visit to Facebook. In this scenario, a non-user visits a website other than `facebook.com` that embeds any of the Facebook resources listed in Section 2.2.2, without having visited `facebook.com` beforehand. We analyze whether such visits may still result in cookie setting for the `facebook.com` domain, even though the non-user may not be aware that a Facebook resource has been loaded.

Figure 2: The Facebook data policy page in 2018. If a non-user clicks zones marked in yellow, four cookies are set. If a person clicks outside these zones, no cookies are set.

In 2015, visiting a page with any Facebook social plugin without a prior visit to Facebook's home page initially did not result in any cookie being set. However, some social plugins requested additional resources on `pixel.facebook.com`, which led to the `datr` cookie being set. It appears that this domain is unrelated to the Facebook pixel. Loading the actual Facebook pixel did not cause any cookie setting. Moreover, certain websites loaded a script from `connect.facebook.com`, upon which the `datr` cookie was also set in a third-party position. In 2017 and 2018, visiting a page with any Facebook social plugin without a prior visit to Facebook's home page also did not result in any cookie being set. In contrast to 2015, loading the Facebook pixel did result in the `fr` identifier cookie being set in a third-party position. In 2022, visiting a page with any Facebook social plugin without a prior visit to Facebook's home page also did not result in any cookie being set. In contrast to 2017 and 2018, loading the pixel also does not result in cookie setting.

4.1.4 Visiting web pages with Facebook resources after a prior visit to Facebook or a page with Facebook resources. In this scenario, a non-user visits Facebook's home page and then a third-party website with Facebook resources. This scenario combines the observations of first-party cookie setting by Facebook with the subsequent third-party collection of these cookies, which enables the ability to track. Alternatively, a non-user may have visited one third-party website with Facebook resources and then another third-party website with Facebook resources. If Facebook sets cookies on the former visit, it can collect them on the latter.

In 2015, Facebook set the `datr` identifier cookie automatically when visiting the home page or a third-party website that made requests to `connect.facebook.com` or `pixel.facebook.com`. After such a visit, Facebook would collect this `datr` cookie on every visit to a third-party website with any Facebook resource. Moreover, for requests to `connect.facebook.com`, the URL of the visited page was included in the `Referer` header and sent to Facebook. As the `Secure` attribute was not set for this `datr` cookie, it would also be sent on non-HTTPS requests, i.e., in plaintext. The value of this cookie could therefore be trivially read by a passive traffic observer, allowing them to build a user profile [37]. In 2017, Facebook set the `datr`, `sb`, and `fr` (outside Belgium) identifier cookies after interaction with the home page. The `fr` identifier cookie was also set when loading a third-party page with the Facebook pixel. On subsequent

visits to sites with a social plugin, the URL of the visited page was included in the `Referer` header of the social plugin request. Only the `sb` cookie had the `Secure` attribute, meaning `datr` and `fr` could be intercepted from network traffic.

In 2018, the `datr`, `sb`, and `fr` cookies were set in the same circumstances as in 2017. On subsequent visits to sites with a social plugin, the URL of the visited page was included in the `Referer` header, and in the `origin` GET parameter of the social plugin request. The domain was also included in the `domain` GET parameter. On subsequent visits to sites with a pixel, the URL of the visited page was included in the `Referer` header and in the `dl` GET parameter of the pixel request. By 2018, all Facebook cookies had the `Secure` attribute, meaning they were never sent in plaintext anymore.

In 2022, accepting essential cookies on the home page ultimately led to the `datr` and `sb` identifier cookies being set. On subsequent visits to sites with a social plugin, the URL of the visited page was included in `href` GET parameter of the social plugin request. The domain was included in the `Referer` header, since browser defaults for the Referrer Policy stripped the URL path from this header by 2022 [31]. On subsequent visits to sites with a pixel, the URL of the visited page was included in the `dl` GET parameter of the pixel request. The domain was included in the `Referer` header. The `datr` and `sb` identifier cookies, alongside all other observed identifier cookies (`c_user`, `fr`, `xs`), all had their `SameSite` attribute set to `None`. This means that Facebook explicitly configured these cookies to be sent along with all third-party requests. The default `Lax` value would have stripped these cookies from those third-party requests. As such, Facebook has the technical ability to restrict cookies to only the first-party context `facebook.com` via `SameSite`, without us being able to infer whether this could interfere with essential back-end functionality. A non-user also has no way of accepting cookies only for first-party use.

In summary, if a non-user previously received Facebook cookies, including identifier cookies, these will be sent along with every subsequent third-party request for a Facebook resource. Moreover, the URL of the visited page is sent along with this request, usually in multiple places. This allows Facebook to link the visit to the third-party page with the non-user's unique identifier cookies, some of which Facebook deems essential. Across all third-party pages with Facebook resources that the non-user visits, Facebook would have the technical ability to build a profile of that user's browsing activity, i.e., track that user.

4.1.5 Opting out of cookies. Throughout time, Facebook's cookies policy has referred non-users who wanted to opt out of its tracking practices to the European Interactive Digital Advertising Alliance's website[5]. Completing this opt-out process resulted in the setting of the `oo` cookie, which does not qualify as an identifier cookie, as it only contains a version number and optionally a timestamp. In 2015, Facebook set the `datr` identifier cookie during the status check of this opt-out process. Consequently, opting out actually caused an identifier cookie to be set (alongside the `oo` cookie). In other years, no additional cookies were set during the opt-out process.

We did not observe any difference in the set of identifier cookies stored or collected during any of the scenarios discussed above when the opt-out is registered through `oo`. This means that non-users who opted out still received and sent identifier cookies such as `datr` and `fr` (if applicable), alongside page URLs in the case of Facebook resources embedded in third-party pages (Section 4.1.4). Interestingly, in 2022, rejecting optional cookies through the cookie banner did not result in the `oo` cookie being set.

[5] youronlinechoices.eu

4.2 Cookie banner

4.2.1 Cookie banner on home page. The main method used for communicating to non-users about cookies and requesting their consent is the 'cookie banner' [56]. In 2015, no such notice was present. In 2017 and 2018, a cookie banner (Figure 1) was placed at the top of the page, just above the Facebook logo and login form. The text of this banner was in a relatively small font, on a dark blue background similar to the page header. The banner assumed consent upon any interaction of the non-user with the site, as observed in Section 4.1.1. Explicitly closing the cookie banner by clicking the cross was therefore one, but not the only trigger for cookie setting.

In 2022, the cookie banner on the home page is blocking any other interaction with the home page: the cookie banner overlays the home page, and the non-user must make a choice before being able to continue navigating the home page. Any choice results in cookies being placed (Section 4.1.1). The non-user can only avoid cookies by leaving the page. We observed two versions of the blocking banner. The first version, observed in January 2022 was large enough to display the entire content of the first panel. The user then saw two buttons. The grey 'Allow all cookies' button closed the cookie banner, led to cookie setting, and allowed the user to continue browsing the home page. The longer blue 'More options' button opened a second panel, whose content overflowed the panel, i.e., a non-user would have to scroll to read the entire panel. This panel contained a brief explanation of essential cookies: "These cookies are required to use Facebook Products. They're necessary for these sites to work as intended". The cookies themselves were not described in further detail. Next to this explanation, a button was toggled on, and could not be toggled off. This was followed by a brief description of optional cookies, being "Cookies from other companies". Next to this explanation, a button was toggled off, and could be toggled on. The banner continued with reasons to allow optional cookies, and "other ways [the non-user] can control [their] information". On this second panel, the user saw two different buttons: a grey 'Only allow essential cookies' button, and a blue 'Allow selected cookies' button. Selecting either option would result in cookie setting, with the cookies depending on the choice.

The second version, observed in March 2022, combines the content into one panel (Figure 3). Instead of buttons next to the descriptions of essential and optional cookies on the second panel in the first version, the non-user sees two buttons: a grey button to 'Only allow essential cookies', or a blue button to 'Allow essential and optional cookies'. Compared to the 45 words in the banner of 2017, the explanation in the lone panel of the second version is much longer: in US English, 184 words are shown immediately, with an additional 557 words hidden under dropdowns. In all 32 languages in which the cookie banner can be shown, the frame of the cookie banner is too small to show the entire explanation, and a non-user must scroll down to read the rest of the description.

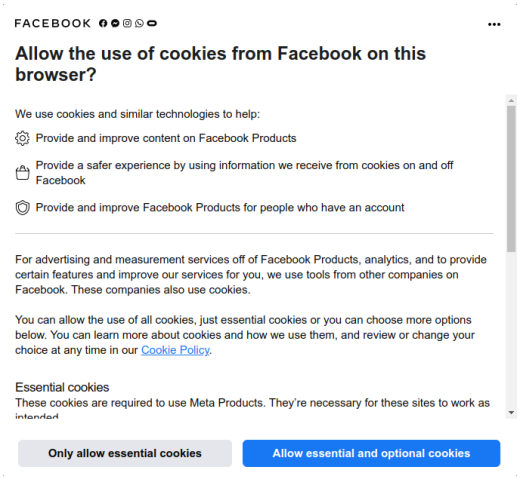

Figure 3: Cookie banner on the home page in July 2022.

The explanation for 'essential cookies' that a non-user sees on the home page is very brief, and nearly circular in reasoning: 'essential' cookies are 'required' to use Facebook and 'necessary' for the site to work as intended. The non-user does not know which cookies are essential, nor what they are used for, nor what their impact on the non-user's privacy is. As we observed in Section 4.1.1, the essential cookies include the `datr` and `sb` cookie, which as identifier cookies may allow to uniquely identify a non-user on visits to third-party websites (Section 4.1.4).

In addition, the layout of the selection buttons bears a strong resemblance to a 'dark pattern' [47, 63] as described in the guidelines of the European Data Protection Board [39]. The layout appears to favor an option for which a user may be unaware that it may have a greater impact on their privacy. Specifically, in both versions of the 2022 cookie banner, the option that would also allow optional cookies is highlighted in a more prominent color (i.e., blue vs. grey). In the EDPB taxonomy, this color contrast may be classified as a 'stirring' pattern called 'Hiding in plain sight' [39, ¶48]. Moreover, in the first version, a non-user had to click through to another panel to decline optional cookies. (On this second panel, however, optional cookies were not toggled on by default.) In the EDPB taxonomy, this additional step may be classified as a 'hindering' pattern called 'Longer than necessary' [39, ¶45]. If cookie banners use such dark patterns, they may no longer be compliant with privacy law such as the GDPR [82].

4.2.2 Cookie banner on policy pages. In case a non-user visits the policy pages and has not yet consented to cookies, those pages may display a cookie banner to inform the non-user or allow them to make a choice. In 2015, Facebook did not use a cookie banner anywhere to inform users about cookies, and policy pages therefore did not include such a banner either. In 2018, both the data and cookies policy pages contained the same style of cookie banner as the home page, i.e., a small dark blue banner at the top of the page, with a cross to dismiss the banner. In 2022, the data and cookies policy pages both had a cookie banner, but in contrast to the home page, this banner is non-blocking and only covers part of the bottom of the page. A non-user can still read the policy pages, without needing to consent to any cookies. The banner provided two buttons for the non-user to make a choice. In January 2022, these buttons read 'Manage Data Settings' (requiring to click through to accept only essential cookies) and 'Accept All' (accepting both essential and optional cookies). In March 2022, these buttons read 'Allow all cookies' and 'Only allow essential cookies'. In both versions, the wording of the buttons differs slightly from that used in the cookie banner on the home page. Possibly due to the banner's smaller size, the description of cookies in the banner is also shorter than that on the home page, requiring a non-user to open additional modals to see the same information. Similar to the home page, the button to accept all cookies is more prominently colored (blue vs. grey), resembling a 'dark pattern' to nudge a non-user towards the more privacy-invasive choice.

This banner style has since remained the same for the cookies policy page. On July 26, 2022, Facebook introduced a new privacy policy page. On this page, a cookie banner of the style of the home page is used, i.e, the banner blocks any interaction with the policy page, and the non-user is unable to read the privacy policy without consenting to at least essential cookies. The banner on the privacy policy page has the same contents as that on the home page, but is styled slightly differently. One artifact of this styling change is that the cookies policy link in this banner is indistinguishable from the rest of the text, being in the same color and font. A non-user would therefore be unlikely to find this link in the banner.

Table 2: Word counts, reading times (estimated at 250 words per minute), and Flesch Reading Ease (FRE) scores for the US English versions of Facebook's cookies policy.

Date	# words	Estimated reading time	FRE score
2016-05-26, 2017-03-20	1536	6'09"	43.0
2018-04-04	1624	6'30"	43.0
2020-10-05	2126	8'30"	44.3
2021-06-23	2111	8'27"	44.1
2022-01-04	2109	8'26"	45.9
2022-07-26 (non-user, no cookies allowed)	2109	8'26"	45.9
2022-07-26 (non-user, cookies allowed)	2126	8'30"	46.0
2022-07-26 (user)	2133	8'32"	45.9

4.3 Policy documents

Facebook has two primary documents describing its privacy-related policies. Its *Data Policy* (before July 26, 2022) or *Privacy Policy*[6] (after July 26, 2022) explains what personal data Facebook collects, how they collect it, and how they use and share that data. On the topic of cookies, this policy is complemented by the *Cookies Policy*[7], which explains how cookies are used and what choices the user has. We mainly focus on this cookies policy throughout the rest of this section.

Revisions. Through the Internet Archive [53], we retrieve the seven revisions of the cookies policy (Table 2). The current cookies policy mentions a revision date, and we recursively trace these

[6] https://www.facebook.com/privacy/policy/
[7] https://www.facebook.com/policies/cookies/

revisions back to May 26, 2016[8], two days after the GDPR entered into force, and coinciding with the apparent expansion of user tracking for the Facebook Audience Network, its ad platform, to non-users [13]. Overall, we find that the revisions are minor: fixing typos, updating domain names of third-party services, or updating 'Facebook' to 'Meta'. The most significant change occurred in 2020, when cookie examples were interleaved with the policy (see "Access" paragraph below). Interestingly, the latest version of the cookies policy differs between non-users who have not accepted cookies (yet), non-users who have, and users, specifically in the "Manage your cookies" section. Non-users who have accepted cookies see an additional paragraph to "manage cookies from other companies on the Meta Products on this browser", which when clicked opens a modal where non-users can allow or revoke these (optional) cookies. The circuitous route through a modal linked at the bottom on the cookies policy page (linked from the homepage) is the only way for non-users to revoke their consent for optional cookies. On the other hand, whether a non-user accepts optional cookies or not, does not affect the cookies set by Facebook, until they actually become a Facebook user and log in. Facebook users see another paragraph instead, linking them to Facebook's cookie settings page, where they can change their cookie preferences for two types of optional cookies (Section 5.2).

Readability. We analyze how much effort a person would have to invest to read and understand the cookies policy, which would allow them to give genuinely informed consent to cookies. Over time, Facebook's cookies policy has gotten longer (Table 2), starting at over 1,500 words in 2016 and having reached over 2,100 words by 2022. Translated into reading time, estimated for a reading speed of 250 words per minute,[9] it would take a person up to 8 minutes and 32 seconds to read the latest US English version of Facebook's cookies policy. Finally, the Flesch Reading Ease score, a readability metric which typically ranges from 0 to 100 and for which higher scores indicate a more readable text, increased from 43.0 to 46.0 between 2016 and 2022. This means that the cookies policy became slightly easier to read over time, but in general such a score still means that it is difficult to read [44]. However, such difficulty levels are common among online privacy-related policies. In 2018, with a score of 48.94, Facebook's privacy (not cookies) policy was actually the most readable among prominent third parties, whose privacy policies had an average score of 35.48 [59].

Access. Since at least 2011, the privacy policy page has been linked from the footer of the home page, joined in June 2012 by a link to the cookies policy page. When launching the new cookies policy page on May 26, 2016, Facebook's home page even highlighted the link with a note that "We've updated our policy." In 2018, the home page continued to provide these links to the data, and non-users could visit these pages without receiving cookies, as clicking these links was an interaction exempted from automatic cookie setting (Section 4.1.1). In 2022, these links still appear in the footer, but with the blocking cookie banner on the home page (Section 4.2.1), a non-user cannot access these links without accepting cookies. Instead, the cookie banner contains a link to the cookies policy page. The data or privacy policy page can only be accessed indirectly through a link on that cookies policy page, and is therefore no longer directly accessible from the home page to a non-user who has not accepted cookies.

Cookie details. One feature of the cookies policy is a detailed overview of which cookies are used by Facebook. Until May 11, 2012, no such overview was given on the help pages about cookies. At this time, the most accurate knowledge of Facebook cookies originated from the Irish DPA audits of Facebook's privacy practices [70, 71, 76, 77] and from a comment by a Facebook engineer on a blog post [23, 25, 80]. From May 11, 2012 until May 26, 2016, an overview was available through a link on the cookies policy page to the Irish DPA audits, which listed all cookies observed on Facebook during in the audit. For each cookie, the document gave a relatively lengthy and detailed description of its purpose, which was provided by Facebook at the request of the DPA. From May 26, 2016 until October 5, 2020, the cookies policy page provided a modal containing a table with a detailed overview of all cookies, grouped by permanent and session cookies, and by the general purpose of the cookie. For each cookie, the table listed the expiration time, the composition of the cookie, and its detailed purpose. Despite this detailed overview, it appeared that in 2018 it was not complete: we observed three cookies (`lh`, `pnl_data2`, and `spin`) that were not listed in the cookies policy, and for which there was therefore no description available. While the maximum lifetime for these cookies was 1 week, and we therefore do not consider them identifier cookies, they do indicate that the cookie overview cannot be assumed as an authoritative source of Facebook's cookie practices. Indeed, the overview modal admits that the cookies used by Facebook may differ from those described in the overview table.

On October 5, 2020, the cookies policy page was updated to remove the modal with the detailed table. Instead, explanations of the cookies' general purposes are interleaved with examples, which sometimes list concrete cookie names, lifetimes, and purposes. Table 3 lists which specific cookies are given as examples. We never observed five of the listed cookies (`csrf`, `dbln`, `dpr`, `_fbc`, `_fbp`), possibly due to our measurements being limited to the desktop website from Belgium (Section 3.3). Of these cookies, the `_fbc` cookie is stated to have a 90-day lifetime, and to be used for "identif[ying] browsers". This suggests that it may also have met our definition of identifier cookie. Conversely, in 2022, we observed two cookies that were not mentioned nor explained anymore in the cookies policy, despite them being present in the 2018 overview table. These cookies are the `locale` cookie and, notably, the `datr` cookie, which is an identifier cookie. Moreover, the policy does not explain which cookies are considered 'essential' or 'optional', and it appears that such detail cannot be found anywhere. Without such an overview, it is impossible to verify whether a person's choice to only allow 'essential' cookies is honored: a person cannot compare the cookies that they have received to a list of cookies that Facebook claims to be essential.

[8]Before 2016, cookie-related policies and help information were hosted across different pages, without a revision date. We sample pages archived on the Internet Archive from before 2016 to discover further policy documents relating to cookies.

[9]A reading speed of 250 words per minute is considered average for people with secondary education [16, 92] and was used in prior work on privacy policies [67, 72].

5 USERS ON THE FACEBOOK WEBSITE

In this section, we study whether Facebook stores cookies for a registered user. We analyze how cookies are set and removed when logging in and logging out respectively. Then, we describe which (additional) cookie controls Facebook provides to its users.

5.1 Cookies set by Facebook

Logging into Facebook. In 2015, when a Facebook user logged into their account, the `c_user`, `datr`, `fr`, `lu`, and `xs` cookies were set (Table 3), all qualifying as identifier cookies. While `datr` (and in some cases `fr`) would have already been set upon visiting the home page with the login form, `c_user` and `lu` are only set for users, containing the user's Facebook ID. In 2017, these cookies were joined by the `sb` cookie, an identifier cookie. In 2018, the `lu` cookie was no longer used.

The most notable change relates to the use of the `fr` identifier cookie, the only cookie that is explicitly related to online advertising and personalised content, according to the cookies policy of Facebook. In 2022, the `fr` cookie is only placed upon consent for non-essential cookies, which the user can indicate by selecting "Allow essential and optional cookies" in the cookie banner on the Facebook homepage (Section 4.2). The user can also decline non-essential cookies by selecting the option "Only allow essential cookies" on the cookie banner. In that case, an opt-out cookie called `oo` is set instead of the `fr` cookie. Facebook's cookies policy states that `oo` "help[s] you opt out of seeing ads from Meta based on your activity on third-party websites".

The mentioned identifier cookies are sent to Facebook when a user visits a web page with a Facebook resource, along with the URL of the visited website (Section 2.2.2). Since 2022, this no longer holds for the `fr` cookie whenever the `oo` cookie is set.

Logging out of Facebook and deactivating a user account. Upon logging out, the `c_user` cookie (for account verification) and the `xs` cookie (a session ID), both identifier cookies, are always deleted. However, the remaining cookies, among which the advertising cookie `fr` up to 2018, are retained even after the browser is restarted and are sent to Facebook on sites which include a Facebook resource, along with the URL of the site. Since 2022, the `fr` cookie is deleted when the user logs out, which was previously not the case. The ones that remain stored in browser are the `datr` and `sb` identifier cookies, therefore still making it possible for Facebook to track logged-out users across different websites.

5.2 Cookie settings for Facebook users

Visual elements. Right after a user registers a new Facebook account and logs in for the first time, a cookie settings menu is shown to the user (Figure 4). The settings shown in this menu are somewhat similar to the cookie banner shown on the homepage before the user is logged in (Section 4.2). However, instead of only two categories of cookies (essential and optional cookies), Facebook allows the user to choose separately whether to allow optional Facebook cookies on other apps and websites, and third-party cookies from other companies. The former category is described as "cookies that help other companies to share information with us about your activity on their apps and websites", and is used for personalization and targeted advertising, but also for social plugins and other services such as Facebook login. Cookies from other companies are used for "advertising and measurement services off Facebook Products, analytics, and to provide certain features and improve services". The user does need to scroll down in order to read the description of all three categories of cookies, since the settings banner does not fit on one page. We note that any first-party statistics or analytics performed by Facebook are not mentioned in this cookie banner. Furthermore, the explanation provided for the category of essential cookies is short, the exact set of essential and both types of optional cookies is not mentioned, and the implications of the use of such cookies remain unclear to the user.

In January 2022, we observed a difference for the cookie settings shown to newly registered users. Back then, the user was immediately given only two options: click on an "Allow all cookies" or a "More Options" button. The latter leads the user to a second panel, where the user can manually select their cookie preference from the same three categories as previously described (essential and two types of optional cookies). This design choice requires the user to perform an additional click in order to reject optional cookies, resulting in it being easier to allow all cookies than to select only essential cookies. On top of that, the button which allows all cookies is highlighted in a more prominent blue color, which the button used to manage cookies has a grey color. Even though the text on the buttons changed by March 2022, the dark pattern concerning the colors of the buttons remains, just like in the cookie banner that is shown to users visiting the Facebook homepage without being logged in (Section 4.2.1). However, the change makes rejecting all optional cookies as easy as accepting them for Facebook users, and the optional cookies are deselected by default.

Changing the cookie settings. The cookie settings are shown to the user on the first ever login with their Facebook account, i.e., no longer on any subsequent Facebook visit. If the user wishes to change their cookie settings, in 2022, they can do this through the "Cookies" tab in the Settings menu, where they can make a new choice for either category of optional cookies. Essential cookies are also listed, but the toggle switch is on by default and cannot be changed. These cookie settings are also linked to from the cookies policy (Section 4.3). A similar process was available in 2018, where users could opt out of (cookies for) the Facebook Audience Network, which was enabled by default for all users.

When a Facebook user visits the homepage with a clean browser state (i.e., previously set cookies have been deleted), the user is once again shown the cookie banner. However, according to their cookie preferences, the Facebook user has adjusted the cookie settings of their account (which are only available to logged in users) in a previous visit, which might differ from the choice that the user can select in the cookie banner on the homepage. In such cases, we examine which settings will apply and which cookies are set.

Even if the user has selected to allow all cookies in their account, if they choose only essential cookies in the cookie banner before logging in, only essential cookies will be retained in the browser and the `oo` cookie will be set instead of the `fr` cookie. Thus, the indicated choice in the cookie banner will override any cookie settings from the user account for the current browser session. Only when the user accepts non-essential cookies in the cookie banner and has set

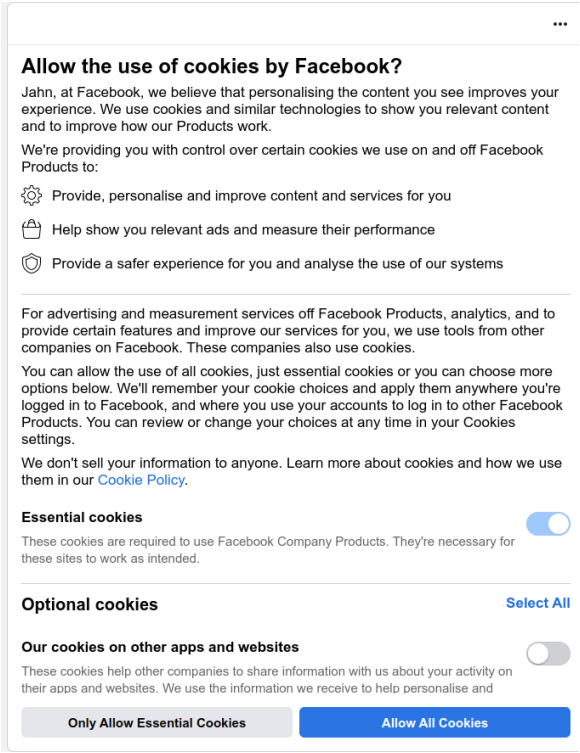

Figure 4: Cookie settings shown to newly registered Facebook users on their first login in July 2022.

their profile settings to allow all non-essential cookies, will the `fr` advertising cookie be set. Facebook users can also use the external European Interactive Digital Advertising Alliance website to opt-out of Facebook tracking, which will have the same effect as for non-users (Section 4.1.5).

6 DISCUSSION

Our analysis shows that over time, Facebook has become more cautious in setting cookies for non-users, reducing the potential for these non-users to be tracked by Facebook. While in 2015 visiting the Facebook website and sometimes even third-party websites that loaded Facebook resources could result in cookies automatically being set, Facebook has since started requiring interaction as a signal of consent (Section 4.1.1), at least in the European region [96]. It appears that the difficulty of asking for such consent on third-party websites [3] has also caused cookie setting to be eliminated by 2022 when loading any of the Facebook resources listed in Section 2.2.2 (Section 4.1.3). The `datr` cookie, which was the main subject of scrutiny in the past [18, 24, 85], is therefore also no longer set for non-consenting non-users (i.e., those who do not select any option on the cookie banner), conforming to the recommendations of the Belgian DPA [2]. Facebook also appears to consider the pages with the privacy and cookies policy as special resources that non-users must be able to access without the need to consent to cookies (Section 4.1.2).

However, on some occasions, Facebook does appear to nudge non-users towards accepting all of its cookies. Access to most of the Facebook website is prevented by a cookie banner which can only be dismissed by a non-user consenting to at least 'essential' cookies, including the `datr` cookie, without mention of which cookies are deemed essential. Moreover, this cookie banner appears to deploy 'dark patterns' to entice non-users into making a more privacy-invasive choice, by making the button to accept all cookies more prominent (Section 4.2.1). Regulatory action has proven effective to reduce these 'dark patterns'. The French DPA gave Facebook a 60 million euro fine for making rejecting optional cookies a more laborious process than accepting them [20]. Indeed, we saw in January 2022 that rejecting optional cookies required navigating two panels as opposed to one click for accepting them (Section 4.2, Section 5.2). In response to the fine, Facebook updated the cookie banner to make a button to accept only essential cookies available in its first (and only) panel, as we saw in March 2022, to the satisfaction of the French DPA [19]. A similar evolution is to be seen in the cookie settings which Facebook users can access after logging in. However, the button for rejecting all non-essential cookies remains more prominent in both the cookie banner and the cookie settings interfaces. Facebook's process to require non-user consent also appears to sometimes introduce artifacts. In 2018, cookie setting differed by the parts of the home page with which a user interacted (Section 4.1.1). At the time of writing (July 2022), non-users must accept at least essential cookies to read the new version of Facebook's privacy policy (Section 4.2.2).

Facebook has also improved communication about cookies to non-users by adding a cookie banner in 2017. They may have done this to comply with the GDPR, as has been observed on other websites [29]. By 2022, this cookie banner blocked a non-user from further interaction with Facebook's website. Indeed, in 2021 Facebook announced that they would roll out "a new consent prompt", to "align with evolving privacy requirements, such as the [...] GDPR and the ePrivacy Directive" [96]. This roll-out also added granular settings for Facebook cookies on other apps and websites, and third-party cookies from other companies, albeit only for registered users (Section 5.2). This cookie banner provides a short and generic description of the purposes and uses of cookies by Facebook. Non-users are referred to Facebook's cookies policy for more information. While this policy is relatively easy to read compared to its industry peers, it is overall still a difficult and long text that requires significant effort to read and understand (Section 4.3). However, the level of available detail with regards to cookies has actually decreased over time: since 2020, the cookies policy only gives examples of certain cookies instead of a full overview table. The `datr` cookie is no longer listed in this new cookies policy version, despite the 2017 recommendation from the Belgian DPA that "Facebook should offer full transparency on the use of cookies" and "specify for each cookie separately the content [...] and purpose [...]" [2]. This makes it difficult for both users and non-users to fully understand the implications of their privacy settings.

As described in Section 3.2, we primarily assess whether cookies could be used as identifiers, i.e., whether they are persistent and uniquely identifiable. Over time, we observed six cookies that meet this definition (Table 3). Five of these are stated to relate to authentication, account verification, and security. Of these, two are set

for non-users (`datr`, `sb`), and three for logged-in Facebook users (`c_user`, `lu`, `xs`). When a registered user logged out, the `datr` and `sb` cookies remained stored on the user's device, joined until 2018 by the `lu` cookie, although the user ID component was stated to be removed from the `lu` cookie [70, 71]. Because of the `SameSite` attribute being explicitly set to `None` by Facebook for these cookies, they will be sent along with requests to Facebook on third-party websites (e.g., for embedded social plugins), contrary to the 2017 Belgian DPA recommendation [2]. The identifying nature of these cookies, combined with page URLs also being sent along with third-party requests, enables the technical ability to use them for tracking. Whether the intent to use these cookies for tracking and building a user profile is present or even necessary to be harmful can be a matter of debate. To an extent, some of these cookies may only be useful *if* they build some form of profile, e.g., monitoring suspicious login behavior, even though this profile is not necessarily used for personalization. This reflects a tension between data protection and vulnerability to certain security threats [8]. However, at the moment, a web visitor has no choice but to accept that Facebook has configured its identifier cookies in such a way that Facebook can access them on third-party websites, even though first-party-only cookies (using `SameSite`) might yield a better balance between privacy and security. Regardless, the presence of these identifiers may induce a risk of unintentional data collection and tracking [104], future profiling, or surveillance by a passive observer [37].

The `fr` identifier cookie is more ostensibly intended for tracking and profile building, as Facebook states it is used for "improv[ing] the relevancy of ads", i.e., ad targeting. This form of tracking and profiling is more commonly accepted as being harmful for privacy, and people are concerned about the data collection and profiling for the purpose of behavioral advertising [73, 97]. Facebook's use of the `fr` cookie has evolved alongside its ad targeting practices. In May 2016, Facebook expanded its Audience Network ad platform to non-users, with the apparent goal of "show[ing] better ads to everyone" [13]. We hypothesize that this expansion may have coincided with the `fr` cookie being set for non-users. Indeed, in our 2017 and 2018 measurements, we see at least some scenarios where non-users receive the `fr` cookie, as opposed to 2015 when this was only the case for registered users, albeit not when visiting the Facebook home page from Belgium. This last observation may have been a result from the Belgian DPA's case against Facebook's cookie practices. By 2022, the `fr` cookie is once again gone for non-users, and is only set as an 'optional' cookie for users. This change is seemingly caused by Facebook shutting down support for social plugins in the European Region for non-users [86] and stopping to serve targeted ads from Audience Network to non-users and users who reject optional cookies [3]. In contrast to before, the `fr` cookie is also deleted for registered users when they log out.

7 RELATED WORK

In general, online tracking has been studied extensively in prior work, usually measuring its prevalence across the web [4, 36, 54, 66, 78, 98]. Bujlow et al. [14] surveyed web tracking threats, mechanisms and defenses. Lerner et al. [58] studied the historical evolution of tracking in particular, measuring cookie-based third-party tracking from 1996 to 2016 using the Internet Archive. They found an increase in tracking across the top 500 websites over time, and note how tracking through social media widgets like Facebook's social plugins was an emerging phenomenon.

A number of studies have evaluated the impact of the GDPR on online privacy. In the area of online tracking, the introduction of the GDPR has generally been found to lead to a decrease in the number of third-party tracking cookies being used [29, 50, 81] and has even had an effect outside of Europe [26], although Sørensen and Kosta found no clear effect [88]. Privacy policies have become longer as a result of the GDPR, but therefore also have a higher coverage of privacy-related topics and are more likely to comply [29, 60]. Cookie banners have also become a staple [29, 49]. However, their design often contains dark patterns [22, 47, 48, 69, 94, 100], which might even introduce legal violations [64]. Jha et al. [51] found that online tracking increases greatly after accepting all cookies in a cookie banner. Kretschmer et al. [56] surveyed recent work on the impact of the GDPR on cookie banners and privacy policies.

Specifically concerning technical evaluations of cookies set by Facebook, Cubrilovic [25] found that certain cookies, among which the `datr` cookie, were not deleted when logging out of Facebook. Roosendaal [79] discussed third-party cookie settings by Facebook in 2012, across scenarios where a person does or does not have a Facebook account. They also describe how this may harm an individual's privacy and identity. Shore and Steinman [84] studied the evolution of Facebook's privacy policy from 2005 to 2015. Bekos et al. [11] showed how Facebook could combine pixel cookies with a URL parameter to persistently track browsing behavior across websites. To our knowledge, no study examines historically Facebook's cookie setting practices for both users and non-users across both Facebook's own website and third-party websites in recent time. We provide an updated and longitudinal view of Facebook's cookie setting behavior, contextualize it with recent developments in privacy regulations and Facebook's tracking practices, and analyze these cookies and their potential for tracking in depth.

8 CONCLUSION

Through a longitudinal and in-depth case study, we analyzed how Facebook's cookie-based tracking behavior evolved from 2015 to 2022. While tightened privacy regulations appear to have positively impacted tracking behavior for non-users, Facebook still appears to go beyond what is strictly necessary for its operations, such as not limiting identifier cookies to a first-party context, nudging (non-)users towards more privacy-invasive options through dark patterns, or cookies being seemingly unaffected by opt-outs. Given increasing regulatory pressure, including ongoing investigations [19, 42], these practices are likely to remain the subject of scrutiny in future. However, this can have the positive effect of further compliance with privacy law, a reduction in online tracking, and therefore a better preservation of people's privacy online.

ACKNOWLEDGMENTS

We thank the authors of the 2015 and 2017 reports. This research is partially funded by the Research Fund KU Leuven, and by the Flemish Research Programme Cybersecurity. Victor Le Pochat holds a PhD Fellowship of the Research Foundation Flanders - FWO (11A3421N).

REFERENCES

[1] 2015. Aanbeveling 4/2015. Commissie voor de bescherming van de persoonlijke levenssfeer, (May 13, 2015). https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-04-2015.pdf.

[2] 2017. Aanbeveling 3/2017. Commissie voor de bescherming van de persoonlijke levenssfeer, (Apr. 12, 2017). https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-03-2017.pdf.

[3] 2021. About updates to our cookies consent prompt and privacy controls in Europe. Meta Business Help Center. https://www.facebook.com/business/help/348535683460989.

[4] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. 2014. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. In *ACM SIGSAC Conference on Computer and Communications Security* (CCS '14), 674–689. DOI: 10.1145/2660267.2660347.

[5] Güneş Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel. 2015. Facebook Tracking Through Social Plug-ins. Technical report prepared for the Belgian Privacy Commission. Version 1.1. COSIC, ICRI/CIR, DistriNet (KU Leuven), (June 24, 2015). https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf.

[6] Article 29 Working Party. 2013. Opinion 03/2013 on purpose limitation. (Apr. 2, 2013). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[7] Mika D Ayenson, Dietrich James Wambach, Ashkan Soltani, Nathan Good, and Chris Jay Hoofnagle. 2011. Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning. (July 29, 2011). SSRN: 1898390. DOI: 10.2139/ssrn.1898390.

[8] Victoria Baines. 2021. On Joined Up Law-making: The Privacy/Safety/Security Dynamic, and What this Means for Data Governance. (Nov. 28, 2021). SSRN: 3958982. DOI: 10.2139/ssrn.3958982.

[9] Paul Barford, Igor Canadi, Darja Krushevskaja, Qiang Ma, and S. Muthukrishnan. 2014. Adscape: Harvesting and Analyzing Online Display Ads. In *23rd International Conference on World Wide Web* (WWW '14), 597–608. DOI: 10.1145/2566486.2567992.

[10] Muhammad Ahmad Bashir, Umar Farooq, Maryam Shahid, Muhammad Fareed Zaffar, and Christo Wilson. 2019. Quantity vs. Quality: Evaluating User Interest Profiles Using Ad Preference Managers. In *26th Annual Network and Distributed System Security Symposium* (NDSS '19). DOI: 10.14722/ndss.2019.23392.

[11] Paschalis Bekos, Panagiotis Papadopoulos, Evangelos P. Markatos, and Nicolas Kourtellis. 2022. The Hitchhiker's Guide to Facebook Web Tracking with Invisible Pixels and Click IDs. (2022). arXiv: 2208.00710. DOI: 10.48550/arxiv.2208.00710.

[12] Dino Bollinger, Karel Kubicek, Carlos Cotrini, and David Basin. 2022. Automating Cookie Consent and GDPR Violation Detection. In *31st USENIX Security Symposium* (USENIX Security '22). https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger.

[13] Andrew Bosworth. 2016. Bringing People Better Ads. Meta. (May 26, 2016). https://about.fb.com/news/2016/05/bringing-people-better-ads/.

[14] Tomasz Bujlow, Valentín Carela-Español, Josep Solé-Pareta, and Pere Barlet-Ros. 2017. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proceedings of the IEEE*, 105, 8, 1476–1510. DOI: 10.1109/JPROC.2016.2637878.

[15] Juan Miguel Carrascosa, Jakub Mikians, Ruben Cuevas, Vijay Erramilli, and Nikolaos Laoutaris. 2015. I Always Feel like Somebody's Watching Me: Measuring Online Behavioural Advertising. In *11th ACM Conference on Emerging Networking Experiments and Technologies* (CoNEXT '15) Article 13, 13 pages. DOI: 10.1145/2716281.2836098.

[16] Ronald P. Carver. 1983. Is Reading Rate Constant or Flexible? *Reading Research Quarterly*, 18, 2, 190–215. DOI: 10.2307/747517.

[17] Wolfie Christl. 2017. Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. Cracked Labs, (June 2017). https://crackedlabs.org/en/corporate-surveillance.

[18] 2017. Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium. (May 16, 2017). https://web.archive.org/web/20171109044229/https://www.cnil.fr/en/common-statement-contact-group-data-protection-authorities-netherlands-france-spain-hamburg-and.

[19] 2022. Cookies: closure of the injunction issued against FACEBOOK. Commission Nationale de l'Informatique et des Libertés. (July 28, 2022). https://www.cnil.fr/en/cookies-closure-injunction-issued-against-facebook.

[20] 2022. Cookies: FACEBOOK IRELAND LIMITED fined 60 million euros. Commission Nationale de l'Informatique et des Libertés. (Jan. 6, 2022). https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros.

[21] Kovila P.L. Coopamootoo, Maryam Mehrnezhad, and Ehsan Toreini. 2022. "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. In *31st USENIX Security Symposium* (USENIX Security '22), 287–304. https://www.usenix.org/conference/usenixsecurity22/presentation/coopamootoo.

[22] Lorrie Faith Cranor. 2022. Cookie Monster. *Communications of the ACM*, 65, 7, (June 2022), 30–32. DOI: 10.1145/3538639.

[23] Nik Cubrilovic. 2011. Facebook Fixes Logout Issue, Explains Cookies. (Sept. 27, 2011). https://nikcub.me/posts/facebook-fixes-logout-issue-explains-cookies/.

[24] Nik Cubrilovic. 2011. Facebook Re-Enables Controversial Tracking Cookie. (Oct. 3, 2011). https://nikcub.me/posts/facebook-re-enables-controversial-tracking-cookie.

[25] Nik Cubrilovic. 2011. Logging out of Facebook is not enough. (Sept. 25, 2011). https://nikcub.me/posts/logging-out-of-facebook-is-not-enough.

[26] Adrian Dabrowski, Georg Merzdovnik, Johanna Ullrich, Gerald Sendera, and Edgar Weippl. 2019. Measuring Cookies and Web Privacy in a Post-GDPR World. In *20th International Conference on Passive and Active Measurement* (PAM '19), 258–270. DOI: 10.1007/978-3-030-15986-3_17.

[27] Els De Busser. 2021. Data Protection Around the World: Belgium. In *Data Protection Around the World: Privacy Laws in Action*. Elif Kiesow Cortez, (Ed.) T.M.C. Asser Press, 7–21. ISBN: 978-94-6265-407-5. https://doi.org/10.1007/978-94-6265-407-5_2.

[28] Jos De Wachter and Charlotte Peeters. 2021. Advocate General Rules on the One-Stop Shop Mechanism. *European Data Protection Law Review*, 7, 1. DOI: 10.21552/edpl/2021/1/17.

[29] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *26th Annual Network and Distributed System Security Symposium* (NDSS '19). DOI: 10.14722/ndss.2019.23378.

[30] Yana Dimova, Gunes Acar, Lukasz Olejnik, Wouter Joosen, and Tom Van Goethem. 2021. The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion. *Proceedings on Privacy Enhancing Technologies*, 2021, 3, (Apr. 2021), 394–412. DOI: 10.2478/popets-2021-0053.

[31] Yana Dimova and Victor Le Pochat. 2021. Privacy. In *The 2021 Web Almanac*. HTTP Archive. Chap. 11. https://almanac.httparchive.org/en/2021/privacy.

[32] 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Union*, L 201, (July 31, 2002), 37–47. https://eur-lex.europa.eu/eli/reg/2002/58/oj.

[33] 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*, L 281, (Nov. 23, 1995), 31–50. https://eur-lex.europa.eu/eli/dir/1995/46/oj.

[34] Peter Eckersley. 2010. How Unique Is Your Web Browser? In *10th International Conference on Privacy Enhancing Technologies* (PETS '10), 1–18. DOI: 10.1007/978-3-642-14527-8_1.

[35] Amir Efrati. 2011. 'Like' Button Follows Web Users. *The Wall Street Journal*, (May 18, 2011). https://www.wsj.com/articles/SB10001424052748704281504576329441432995616.

[36] Steven Englehardt and Arvind Narayanan. 2016. Online Tracking: A 1-Million-Site Measurement and Analysis. In *2016 ACM SIGSAC Conference on Computer and Communications Security* (CCS '16), 1388–1401. DOI: 10.1145/2976749.2978313.

[37] Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan, and Edward W. Felten. 2015. Cookies That Give You Away: The Surveillance Implications of Web Tracking. In *24th International Conference on World Wide Web* (WWW '15), 289–299. DOI: 10.1145/2736277.2741679.

[38] European Court of Justice. 2019. Judgement nr. C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, ECLI:EU:C:2019:801. (Oct. 1, 2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0673.

[39] European Data Protection Board. 2022. Dark patterns in social media platform interfaces: How to recognise and avoid them. Guidelines 3/2022. Version 1.0. (Mar. 14, 2022). https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

[40] European Data Protection Board. 2020. Guidelines 05/2020 on consent under Regulation 2016/679. (May 4, 2020). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[41] European Data Protection Board. 2019. 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. (Oct. 8, 2019). https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

[42] 2021. Facebook case : the CJEU has ruled. Gegevensbeschermingsautoriteit. (June 15, 2021). https://www.dataprotectionauthority.be/citizen/facebook-case-the-cjeu-has-ruled.

[43] 2017. Facebook tracking via social plug-ins. Dutch. Aanvullend technisch rapport. Version 1.1. Commissie voor de bescherming van de persoonlijke levenssfeer, (Feb. 24, 2017).

[44] James N. Farr, James J. Jenkins, and Donald G. Paterson. 1951. Simplification of Flesch Reading Ease Formula. *Journal of Applied Psychology*, 35, 5, (Oct. 1951), 333–337. DOI: 10.1037/h0062427.

[45] Gertjan Franken, Victor Le Pochat, Yana Dimova, Tom Van Goethem, Wouter Joosen, and Lieven Desmet. 2022. Cookie-gebaseerde tracking door Facebook. Dutch. (Apr. 22, 2022), commissioned by the Data Protection Authority Belgium (https://www.dataprotectionauthority.be/).

[46] Gertjan Franken, Victor Le Pochat, Tom Van Goethem, Wouter Joosen, and Lieven Desmet. 2018. Cookie-gebaseerde tracking door Facebook. Dutch. (July 9, 2018), commissioned by the Data Protection Authority Belgium (https://www.dataprotectionauthority.be/).

[47] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *2021 CHI Conference on Human Factors in Computing Systems* (CHI '21) Article 172, 18 pages. DOI: 10.1145/3411764.3445779.

[48] Philip Hausner and Michael Gertz. 2021. Dark Patterns in the Interaction with Cookie Banners, (Mar. 2021). Position Paper at the Workshop "What Can CHI Do About Dark Patterns?" at the 2021 CHI Conference on Human Factors in Computing Systems. arXiv: 2103.14956. DOI: 10.48550/arxiv.2103.14956.

[49] Maximilian Hils, Daniel W. Woods, and Rainer Böhme. 2020. Measuring the Emergence of Consent Management on the Web. In *2020 ACM Internet Measurement Conference* (IMC '20), 317–332. DOI: 10.1145/3419394.3423647.

[50] Xuehui Hu and Nishanth Sastry. 2019. Characterising Third Party Cookie Usage in the EU after GDPR. In *10th ACM Conference on Web Science* (WebSci '19), 137–141. DOI: 10.1145/3292522.3326039.

[51] Nikhil Jha, Martino Trevisan, Luca Vassio, and Marco Mellia. 2021. The Internet with Privacy Policies: Measuring The Web Upon Consent. arXiv: 2109.00395. DOI: 10.48550/arxiv.2109.00395.

[52] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and Privacy: It's Complicated. In *8th Symposium on Usable Privacy and Security* (SOUPS '12) Article 9, 15 pages. DOI: 10.1145/2335356.2335369.

[53] Brewster Kahle. 1997. Preserving the Internet. *Scientific American*, 276, 3, 82–83.

[54] Arjaldo Karaj, Sam Macbeth, Rémi Berson, and Josep M. Pujol. 2018. WhoTracks.Me: Shedding light on the opaque world of online tracking. (2018). arXiv: 1804.08959. DOI: 10.48550/arXiv.1804.08959.

[55] Martin Koop, Erik Tews, and Stefan Katzenbeisser. 2020. In-Depth Evaluation of Redirect Tracking and Link Usage. *Proceedings on Privacy Enhancing Technologies*, 2020, 4, 394–413. DOI: 10.2478/popets-2020-0079.

[56] Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle. 2021. Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web*, 15, 4, Article 20, (July 2021), 42 pages. DOI: 10.1145/3466722.

[57] Mathias Lécuyer, Guillaume Ducoffe, Francis Lan, Andrei Papancea, Theofilos Petsios, Riley Spahn, Augustin Chaintreau, and Roxana Geambasu. 2014. XRay: Enhancing the Web's Transparency with Differential Correlation. In *23rd USENIX Security Symposium*, 49–64. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/lecuyer.

[58] Adam Lerner, Anna Kornfeld Simpson, Tadayoshi Kohno, and Franziska Roesner. 2016. Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016. In *25th USENIX Security Symposium* (USENIX Security '16), 997–1013. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner.

[59] Timothy Libert. 2018. An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. In *2018 World Wide Web Conference* (WWW '18), 207–216. DOI: 10.1145/3178876.3186087.

[60] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2020. The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020, 1, 47–64. DOI: 10.2478/popets-2020-0004.

[61] Bin Liu, Anmol Sheth, Udi Weinsberg, Jaideep Chandrashekar, and Ramesh Govindan. 2013. AdReveal: Improving Transparency into Online Targeted Advertising. In *12th ACM Workshop on Hot Topics in Networks* (HotNets-XII) Article 12, 7 pages. DOI: 10.1145/2535771.2535783.

[62] 2014. Making Ads Better and Giving People More Control Over the Ads They See. Meta. (June 12, 2014). https://about.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/.

[63] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In *2021 CHI Conference on Human Factors in Computing Systems* (CHI '21) Article 360, 18 pages. DOI: 10.1145/3411764.3445610.

[64] Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2020. Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. SP '20, 791–809. DOI: 10.1109/SP40000.2020.00076.

[65] Surya Mattu and Aaron Sankin. 2020. How We Built a Real-time Privacy Inspector. *The Markup*, (Sept. 22, 2020). https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector.

[66] Jonathan R. Mayer and John C. Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In *2012 IEEE Symposium on Security and Privacy* (SP '12), 413–427. DOI: 10.1109/SP.2012.47.

[67] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, 4, 3, 543–568.

[68] Rowan Merewood. 2019. SameSite cookies explained. web.dev. (May 7, 2019). https://web.dev/samesite-cookies-explained/.

[69] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *2020 CHI Conference on Human Factors in Computing Systems* (CHI '20), 1–13. DOI: 10.1145/3313831.3376321.

[70] Dave O'Reilly. 2011. Facebook Technical Analysis Report. Appendix 1 to the Report of the Audit on Facebook Ireland by the Irish Data Protection Commissioner. (Dec. 16, 2011). https://web.archive.org/web/20160514040554/https://dataprotection.ie/documents/facebook%20report/report.pdf/appendices.pdf.

[71] Dave O'Reilly. 2012. Report on Facebook Ireland (FB-I) Audit 2-3 May & 10-13 July 2012. Annex 1 to the Report of the Re-Audit on Facebook Ireland by the Irish Data Protection Commissioner. FTR Solutions, (Sept. 21, 2012). https://web.archive.org/web/20130208064544/https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.

[72] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23, 1, 128–147. DOI: 10.1080/1369118X.2018.1486870.

[73] Emilee Rader. 2014. Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google. In *10th USENIX Conference on Usable Privacy and Security* (SOUPS '14), 51–67. https://www.usenix.org/conference/soups2014/proceedings/presentation/rader.

[74] Filippo Raso. 2016. Facebook Belgium v. Belgian Privacy Commission: Belgian Court of Appeals Reverses Order Prohibiting Facebook from Tracking Non-Users. JOLT Digest. (July 12, 2016). https://jolt.law.harvard.edu/digest/belgian-court-of-appeals-reverses-order-prohibiting-facebook-from-tracking-non-users.

[75] 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, (May 4, 2016), 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[76] 2011. Report of the Audit on Facebook Ireland by the Irish Data Protection Commissioner. Office of the Data Protection Commissioner of Ireland, (Dec. 21, 2011). https://www.pdpjournals.com/docs/87980.pdf.

[77] 2012. Report of the Re-Audit on Facebook Ireland by the Irish Data Protection Commissioner. Office of the Data Protection Commissioner of Ireland, (Sept. 21, 2012). https://web.archive.org/web/20130208064544/https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.

[78] Franziska Roesner, Tadayoshi Kohno, and David Wetherall. 2012. Detecting and Defending Against Third-Party Tracking on the Web. In *9th USENIX Symposium on Networked Systems Design and Implementation* (NSDI '12), 155–168. https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner.

[79] Arnold Roosendaal. 2012. We Are All Connected to Facebook … by Facebook! In *European Data Protection: In Good Health?* Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet, (Eds.), 3–19. DOI: 10.1007/978-94-007-2903-2_1.

[80] JD Rucker. 2011. The End of Privacy: Facebook Tracks Your Moves Even If You Log Out. Soshable. (Sept. 25, 2011). https://web.archive.org/web/20130124214200/http://soshable.com/facebook-tracking/.

[81] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. In *2019 ACM Asia Conference on Computer and Communications Security* (Asia CCS '19), 340–351. DOI: 10.1145/3321705.3329806.

[82] Cristiana Santos, Nataliia Bielova, and Célestin Matte. 2020. Are cookie banners indeed compliant with the law? : Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technology and Regulation*, 2020, (Dec. 2020), 91–135. DOI: 10.26116/techreg.2020.009.

[83] Saptak Sengupta, Tom Van Goethem, and Nurullah Demir. 2021. Security. In *The 2021 Web Almanac*. HTTP Archive. Chap. 12. https://almanac.httparchive.org/en/2021/security.

[84] Jennifer Shore and Jill Steinman. 2015. Did You Really Agree to That? The Evolution of Facebook's Privacy Policy. *Technology Science*, (Aug. 10, 2015), 2015081102. https://techscience.org/a/2015081102/.

[85] Stephanie De Smedt. 2015. Facebook Loses the First Round of Its Battle with the Belgian Privacy Commission. *European Data Protection Law Review*, 1, 4, 293–298. DOI: 10.21552/EDPL/2015/4/8.

[86] [n. d.] Social Plugins. Section on "Changes to Social Plugins in the European Region". Meta for Developers. https://developers.facebook.com/docs/plugins.

[87] Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, and Chris Hoofnagle. 2010. Flash Cookies and Privacy. In *2010 AAAI Spring Symposium Series*, 158–163. https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1070/1505.

[88] Jannick Sørensen and Sokol Kosta. 2019. Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites. In *2019 World Wide Web Conference* (WWW '19), 1590–1600. DOI: 10.1145/3308558.3313524.

[89] Dina Srinivasan. 2019. The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy. *Berkeley Business Law Journal*, 16, 1, 39–101. https://lawcat.berkeley.edu/record/1128876.

[90] Alex Stamos. 2015. Preserving Security in Belgium. Facebook. (Oct. 13, 2015). https://web.archive.org/web/20160131084643/https://www.facebook.com/notes/alex-stamos/preserving-security-in-belgium/10153678944202929.

[91] Alex Stamos. 2015. Preserving Security in Belgium - An Update. Facebook. (Dec. 3, 2015). https://web.archive.org/web/20190809000806/https://www.facebook.com/notes/alex-stamos/preserving-security-in-belgium-an-update/10153771198542929.

[92] Stanford E. Taylor. 1965. Eye Movements in Reading: Facts and Fallacies. *American Educational Research Journal*, 2, 4, 187–202. DOI: 10.3102/00028312002004187.

[93] Omer Tene and Jules Polonetsky. 2012. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science and Technology*, 13, 1, 281–358, 9. https://scholarship.law.umn.edu/mjlst/vol13/iss1/9.

[94] Michael Toth, Nataliia Bielova, and Vincent Roca. 2022. On dark patterns and manipulation of website publishers by CMPs. *Proceedings on Privacy Enhancing Technologies*, 2022, 3, 478–497. DOI: 10.56553/popets-2022-0082.

[95] Maarten Truyens. 2016. No More Cookies for Unregistered Facebook Users in Belgium: *European Data Protection Law Review*, *2*, 1. DOI: 10.21552/EDPL/2016/1/20.

[96] 2021. Updating Our Cookie Controls in Europe. Meta. (Sept. 23, 2021). https://about.fb.com/news/2021/09/updating-our-cookie-controls-in-europe/.

[97] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *8th Symposium on Usable Privacy and Security* (SOUPS '12) Article 4, 15 pages. DOI: 10.1145/2335356.2335362.

[98] Tobias Urban, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. 2020. Beyond the Front Page: Measuring Third Party Dynamics in the Field. In *The Web Conference 2020* (WWW '20), 1275–1286. DOI: 10.1145/3366423.3380203.

[99] 2022. Using HTTP cookies. MDN Web Docs. (Apr. 27, 2022). https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

[100] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *2019 ACM SIGSAC Conference on Computer and Communications Security* (CCS '19), 973–990. DOI: 10.1145/3319535.3354212.

[101] Gerrit Vandendriessche and Louis-Dorsan Jolly. 2016. Belgium: Facebook Not to Tracking Non-Facebook Subscribers. *Computer Law Review International*, 17, 2, 57–60. DOI: 10.9785/cri-2016-0206.

[102] Michael Veale and Frederik Zuiderveen Borgesius. 2022. Adtech and Real-Time Bidding under European Data Protection Law. *German Law Journal*, 23, 2, (Mar. 2022), 226–256. DOI: 10.1017/GLJ.2022.18.

[103] Zhiju Yang and Chuan Yue. 2020. A Comparative Measurement Study of Web Tracking on Mobile and Desktop Environments. *Proceedings on Privacy Enhancing Technologies*, 2020, 2, 24–44. DOI: 10.2478/popets-2020-0016.

[104] Zhonghao Yu, Sam Macbeth, Konark Modi, and Josep M. Pujol. 2016. Tracking the Trackers. In *25th International Conference on World Wide Web* (WWW '16), 121–132. DOI: 10.1145/2872427.2883028.

A APPENDIX

Table 3: Overview of cookies observed on the Facebook website. The description is sourced from the 2018 version of Facebook's cookies policy, unless otherwise noted. ?: Cookie present. 🔒: `Secure` flag set on cookie. SS: Value of the `SameSite` cookie attribute. E: Set if (at least) essential cookies are allowed. O: Set if (also) optional cookies are allowed. EX: Listed as an example in the 2022 cookies policy. ID: Identifier cookie. *: session if "Keep me logged in" was unchecked, 1 month if checked.

				2015		2017		2018		2022					
Name	Example value	Description	Expires after	?	🔒	?	🔒	?	🔒	?	SS	E	O	EX	ID
act	1529503857162%2F12	Timestamp and action counter [23]	session	✓	✗	✓	✗	✓	✓	✗	–	–	–	–	✗
csm	2	HTTPS needed for access to FB servers	session/1 month* (2015), 90 days (2017)	✓	✗	✓	✗	✗	–	✗	–	–	–	–	✗
c_user	100026475650953	User ID for account verification	90 days (2018), 1 year (2022)	✓	✓	✓	✓	✓	✓	✓	None	✓	✓	✓	✓
datr	XMgoW2nMBzOMLFvCAvIZXyMW	Browser ID for security and site integrity	2 years	✓	✗	✓	✗	✓	✓	✓	None	✓	✓	✗	✓
fr	096ZZfC5sBSEGN7BT.AWV5n1dp TfF1cOGQwCON8bQR5CE.BbJME S.Pt.AAA.0.0.BbJMES.AWUPcC3a	User/browser ID used to deliver, measure and improve relevancy of ads	90 days	✓	✗	✓	✗	✓	✓	✓	None	✗	✓	✓	✓
lh	en_US%2Cfr_FR	*Not listed in cookies policy*	1 week	✗	–	✗	–	✓	✓	✗	–	–	–	–	✗
locale	fr_FR	Region (country and language)	1 week	✓	✗	✓	✗	✓	✓	✓	None	✓	✓	✗	✗
lu	wfKm8IfbXqRklNoERo10HIH	Saved user ID and login data [23]	2 years	✓	✓	✓	✗	✓	–	✗	–	–	–	–	✓
oo	v1%7C1%3A1529151909	Store ad opt-out	5 years	✓	✗	✓	✗	✓	✓	✓	None	✓	✗	✓	✗
p1	n	Logged in via Facebook platform	90 days	✗	–	✓	✓	✓	✓	✗	–	–	–	–	✗
p	-2	User's channel partition [70]	session	✓	✗	✓	✗	✗	–	✗	–	–	–	–	✗
pnl_data2	eyJhIjoib25hZnRlcmxvYWQiL CJjIjoiLyIsImIiOmZhbHNlLC JkIjoiLyIsImUiOltdfQ%3D%3D	*Not listed in cookies policy*	2 seconds	✗	–	✗	–	✓	✓	✗	–	–	–	–	✗
presence	EDvF3EtimeF1529135377EuserF A21B2647565095 3A2EstateFDu tF1529135377532CEchF_7bCC	Chat state [70]	session	✓	✓	✓	✓	✓	✓	✓	*not set; default: Lax*	✓	✓	✓	✗
reg_ext_ref	https%3A%2F%2Fwww.google.com%2F	Referer to first visited Facebook page [70]	session	✓	✗	✓	✗	✓	✓	✗	–	–	–	–	✗
reg_fb_gate	https%3A%2F%2Fwww.facebook.com%2F	First visited Facebook page [70]	session	✓	✗	✓	✗	✓	✓	✗	–	–	–	–	✗
reg_fb_ref	https%3A%2F%2Fwww.facebook.com%2F	Last visited Facebook page [70]	session	✓	✗	✓	✗	✓	✓	✗	–	–	–	–	✗
sb	XMgoWzNEl74CKz6iY4CnPHz_	Identify browser for login verification	2 years	✗	–	✓	✓	✓	✓	✓	None	✓	✓	✓	✓
s	Aa67DZudqH2wPHl9	Timestamp of last password entry	session/1 month* (2015), 90 days (2017)	✓	✓	✓	✓	✗	–	✗	–	–	–	–	✗
spin	r:4032753_b.trunk_t.1529598 307_s.1_v.2_	*Not listed in cookies policy*	25 hours	✗	–	✗	–	✓	✓	✗	–	–	–	–	✗
wd	1920x869	Window dimension [70]	session (2015/2017), 1 week (2018/2022)	✓	✗	✓	✗	✓	✓	✓	Lax	✓	✓	✓	✗
xs	16%3ALXzrNJlk_Lys4Q%3A2%3 A1529135378%3A-1%3A-1	Session ID for account verification	session/1 month* (2015), 90 days (2017/2018), 1 year (2022)	✓	✓	✓	✓	✓	✓	✓	None	✓	✓	✓	✓
x-src	%2Fdirectory%2Fpeople %2F%7Cpage_footer	Analytics	1 second	✗	–	✓	✗	✓	✓	✗	–	–	–	–	✗