Access Your Data... If You Can: An Analysis of Dark Patterns Against the Right of Access on Popular Websites

Alexander Löbel[1 (✉)][0009−0001−2831−885X], René Schäfer[1][0000−0002−0078−1412], Hanna Püschel[2][0000−0003−4352−6777], Esra Güney[1][0009−0007−8848−9961], and Ulrike Meyer[1][0000−0002−2569−1042]

[1] RWTH Aachen University, Aachen, Germany
{loebel@itsec.,rschaefer@cs.,esra.gueney@,meyer@itsec.}rwth-aachen.de
[2] TU Dortmund University, Dortmund, Germany
hanna.pueschel@tu-dortmund.de

Abstract. Various regulations including the GDPR empower users with the right to request a copy of their personal data processed by data holders. This *right of access* can serve as the foundation of exercising other data subject rights, including erasure, rectification, and objection of the processed data. Like other regulations, the GDPR does not prescribe any specific procedure data holders need to implement to handle data subject access requests but requires them not to erect any material or formal hurdles in the assertions of their rights. In this paper, we focus on popular online service providers as data holders and investigate in which form they allow users to make data access requests directly on their websites and whether they use any strategies to impede such requests. Our systematical analysis of the process of submitting access requests on 166 account-based websites from the top 500 entries of the Tranco list reveals 238 instances of dark patterns impeding the submission of data subject access requests on 113 (68%) of the examined websites.

Keywords: right of access · dark patterns · usable privacy

1 Introduction

Data protection regulations around the world currently govern the collection and processing of personal data, including the *California Consumer Protection Act* (CCPA) [14] or the *General Data Protection Regulation* (GDPR) [20]. These regulations aim to enhance data transparency and empower users with rights to control the use of their personal data. These rights include the right to access, the right to erase, and the right to rectify personal data. While each of these rights is granted independently, exercising the right of access may often be the initial step to exercise the other rights. Like other regulations, the GDPR does not require data holders to follow any specific technical procedure to grant these rights, but rather only generally *Article 12 para. 2 GDPR* requires them to facilitate the exercise of data subject rights without material or formal hurdles.

Previous studies have emphasized the importance of the right of access [47, 48, 43], yet challenges persist in its implementation. Studies involved users requesting data from controllers [46, 2, 10, 57, 58], researchers initiating access requests [60, 54, 66, 11, 39, 65, 59], and examinations of the usability of returned data [70, 68]. These studies consistently highlight issues with data subject access request (DSAR) submissions and controller compliance. Notably, Pöhn et al. [59] described dark patterns hindering DSARs with 27 data controllers. Such dark patterns – deceptive design choices tricking users into behaving differently than originally intended – have been documented across various domains [23, 5, 18, 16, 24], such as in shopping platforms [50], social networking sites [52], games [72], and mobile platforms [26, 32], among others. Particularly concerning privacy and transparency, dark patterns have been observed extensively [8, 29, 34, 40, 36]. Consent banners stand out as a popular domain for dark pattern usage [45, 67, 55, 64, 38, 7, 28], prompting researchers to automate checks and countermeasures for consent banner-related dark patterns [4, 27, 35].

Existing research has not focused on a particular way to submit a DSAR. Nonetheless, online service providers have to inform users about their data subject rights. However, there is no detailed analysis of whether service providers leverage the control they have over their own websites to hinder the submission of DSARs directly on their websites. To address this, we concentrate on online service providers and on how they allow users to submit DSARs on their websites. Specifically, we explore whether popular online service providers utilize dark patterns that hinder DSARs on the website itself.

This study contributes to the examination of dark patterns in transparency by expanding upon the descriptive data of Pöhn et al. [59] through a larger-scale study. Additionally, we utilize the EDPB taxonomy [19] to categorize our findings, facilitating the mapping of identified dark patterns to GDPR articles potentially breached. Overall, we explore the following research questions:

1. Do popular online service providers employ dark patterns that hinder the submission of DSARs on their websites?
2. What mechanisms are available for users to submit a DSAR on these websites?
3. Which types of dark patterns, based on the EDPB taxonomy, are most common on popular websites?

To answer these questions, we systematically analyzed the process of finding a method to submit a DSAR directly on 166 account-based websites from the top 500 entries of the Tranco list [42]. Our analysis reveals 238 instances of dark patterns on popular websites. We provide a fully labeled dataset with descriptions, categorizations into the EDPB taxonomy, and screencasts of our request analysis for each website[3] to enhance transparency of our research and facilitate

[3] For review, we provide only a few representative examples at https://osf.io/4jvhx/?view_only=ab6b8e27e7c34fdb86b7fb47feb89101 of such screencasts since many of the screencasts contain pieces of information that could deanonymize us at least partly.

further research in this area. Note that we deliberately decided not to answer request confirmation e-mails in order to keep manual work for website operators low.

2 Background and Related Work

In this section, we discuss regulations governing personal data usage, with the GDPR being the central legislation for us as we conduct the study from within the EU. We detail work investigating the right of access. Furthermore, we introduce our working notion of dark patterns, outline relevant works about dark patterns, and discuss pertinent taxonomies.

2.1 The Right of Access

The right of access was included in data protection regulations around the world as early as the 1960s [12] and became a cornerstone of data protection law, which it has retained to this day [48]. The right of access was also established for the member states of the EU in *Article 15* of the GDPR. The GDPR initially only referred to the EU but was adopted for the EEA [15]. The GDPR is often seen as a substantial influence for other data protection laws around the world, e.g., in the US, Brazil, Japan, and Switzerland, which also provide a right of access [31, 25]. Although the GDPR is a regional data protection law and does not apply worldwide, its scope of application is enormous [47]. The GDPR regulates the territorial scope of application itself in *Article 3*. Accordingly, the GDPR applies to data processing activities within the EU and includes data subjects located in the Union, even if processing occurs outside the Union (*Article 3 para. 1 GDPR*) and even data processing by controllers not established in the EU is covered by the GDPR under certain conditions (*Article 3 para. 2 GDPR*). The right of access granted by *Article 15* provides data subjects an insight into whether and how their data is being processed. The reasoning for this is that fair and transparent processing is only possible if the data subject can obtain information about the existence of processing operations, their purposes, and various other intentions and legal consequences associated with the processing (*Recital 60*). Other data subject rights can be aggravated if the data subject does not know what data the controller is processing. In addition, the controller shall also provide a copy of the personal data undergoing processing in accordance with *Article 15 para. 3* of the GDPR.

Data Subject Access Requests This right must be asserted by submitting a corresponding request to the controller. However, *Article 15* of the GDPR does not describe how the right to information should be asserted. The request can, therefore, be made without any formal requirements. The process of making a request is at most specified by *Article 12 para. 2 GDPR*, which stipulates that the controller must facilitate the exercise of the data subject's rights in accordance with *Article 15*. Additionally, *Recital 59* states that mechanisms should be established to ensure data subjects can request and obtain access to personal data free of charge. These legal requirements are not particularly specific, as the GDPR deliberately aims to be technology-neutral. In any case, no material or formal hurdles may be erected in the assertion of data subjects' rights. A violation is therefore assumed if access to the information is made considerably more difficult without objective reasons, or if the information can only be obtained by accepting a media breach.

Studies on the Right of Access In practice, the process of submitting DSARs seems to be hampered. One problem constitutes user verification, which should ensure that a user is authorized to the collected data. There are works [13, 49, 56, 11, 17] showing one can abuse the right of access to learn personal information of others. Lauradoux [41] shows that this is facilitated for a governmental adversary having more access to a citizen's information being able to forge documents. In [63, 6], data controllers' perspectives are explored, and recommendations for authorization of data subjects are examined. However, these recommendations can lead to doubtful authentication mechanisms [6].

On the other hand, multiple works show that the implemented processes to submit a DSAR lack usability. Despite the right of access forming the basis for subsequent data subject rights, it has been shown that it falls short of expectations [43]. This is evidenced by empirical studies investigating the process of submitting data subject requests by researchers themselves [54, 60, 66, 65], with the help of volunteers [46, 2, 57, 10], or with the help of students [3]. They show that not only the returned data is often impractical and non-structured for users struggling to make sense of the data [68, 70] but also the path to submit a request seems to be non-ideal [58], clustered with obstacles and data controllers that do not respond adequately [59, 66, 39, 10]. In [69], Waldman raises the assumption that these inconveniences may be intentional and things like privacy dashboards or consent choices are merely symbolic and should primarily maintain the appearance that the industry cares about privacy. Likewise, we suspect these hindrances are not always being placed unintentionally. Rather, we presume that some online services try to implement dark patterns hindering users from accessing their data, where these online services have control, i.e., on their websites. We still remark that it is often not possible to reach a reliable decision of whether a pattern was actually implemented to hinder users, was a sincere programming error, or serves another purpose justifying such obstructions.

Nonetheless, Pöhn et al. [59] describe occurrences of dark patterns they found in their exploration of DSAR submissions. Our work adds to their descriptions of found dark patterns by specifically looking into dark patterns hindering a request submission on the websites of popular services on a larger data set. Furthermore, we categorize our findings into a pertinent taxonomy, providing references to the GDPR articles the found dark patterns might breach. We confirm some of the patterns described by Pöhn et al., e.g., *making it impossible to access GDPR requests* [59] often translates to the dark pattern *Dead End* of the EDPB taxonomy [19] that we found multiple times. Before we describe the methodology used to carry out this larger-scale study, we introduce dark patterns and where they can be found in the context of transparency.

2.2 Dark Patterns

Dark patterns[4] are malicious user interface design strategies that influence the decision-making of users in favor of an online service [50, 23]. The term *dark pattern* was coined by Harry Brignull in 2010, who created a website[5] showcasing actively used dark patterns. Deceptive designs have been shown in various contexts on the web [18, 16, 26, 32, 36]. In addition to research papers, governmental reports and guidelines on dark patterns exist. In their report[6], the *Norwegian Consumer Council* explains how companies use dark patterns to nudge people into choosing privacy-intrusive user settings. Additionally, an extensive report by the EU [18] analyzed dark patterns and stressed their prevalence on websites and in apps. This ubiquity of manipulative designs led to diverse countermeasures, including user awareness [5, 16, 53], automatic detection [50, 64, 30, 4, 35], and visual countermeasures [62]. Bongard-Blanchy et al. [5] categorized countermeasures by splitting them into four regions of action (*educational*, *design*, *technical*, and *regulatory*) and four intervention scopes (*awareness*, *detection*, *resisting*, and *elimination*). However, as technical countermeasures are an arms race between developers and service providers, researchers and experts still underline the need for stronger regulations [33, 61, 71].

Legislation on Dark Pattern Usage One response to such calls is the *Digital Services Act* (DSA) [21]. It explicitly includes a ban on dark patterns. *Article 25* of the DSA prohibits arrangements whereby users are deceived in their decision-making. Although the DSA already came into force in November 2022, most of the provisions, including *Article 25*, only apply from February 2024 (*Article 93*). We conducted the study before February 2024, and hence service providers did not have to comply with these provisions yet. Thus, we cannot say how this new regulation affects them in practice. However, there are other works also concerned with the legality of dark patterns. The website of Harry Brignull provides an overview of passed laws concerned with dark patterns and manipulative designs. Additionally, Luguri and Strahilevitz [44] argue that some dark patterns can be considered unlawful.

Dark Patterns Undermining Transparency There are works (e.g. [45, 64, 38, 37, 7]) that provide evidence supporting the claim about the industry's unwillingness by looking at the design of consent choice banners. Krisam et al. [38] reviewed consent choice banners on Germany's top 500 visited websites and

[4] Sometimes also referred to as *deceptive patterns* or *deceptive designs*.

[5] https://www.deceptive.design/ *(accessed 31.01.2024)*

[6] https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf *(accessed: 20.01.2024)*

found that 85% used visual nudges to make people accept cookies. Nouwens et al. [55] scraped consent pop-ups on 680 websites in the UK and found that only 12% met basic requirements regarding European law. The authors additionally confirmed the influence of the designs of commonly used consent choice banners in a user study with 40 participants. This agrees with Habib et al. [28], who investigated cookie consent forms in an online user study and derived design implications regarding usability. Further research includes the automatic detection of dark patterns in consent notices [35, 27] and user behavior dealing with dark patterns in cookie banners [67, 5]. Apart from consent choice banners, dark patterns were also found in other parts of websites, such as account management [34], pages concerned with opting-out of advertisement options [29], or pages dealing with legitimate interest [40] which might give online services a ground to process personal data. Bösch et al. [8] created a general framework of *privacy dark patterns* and showed how they follow common templates.

Dark Pattern Taxonomies As an ever-growing number of dark patterns is identified, several taxonomies [51] try to provide an overview of the situation by grouping dark patterns by their characteristics. These taxonomies focus on, inter alia, games [72], shopping [50], social network services [52], attention-capture dark patterns [53], and privacy [8]. One well-established taxonomy is given by Gray et al. [23] and was extended and adapted to the context of shopping by Mathur et al. [50]. Additionally, researchers collected definitions and types of dark patterns from existing taxonomies and included further research and governmental reports [51, 44], leading to more general taxonomies. A recent work by Gray et al. [24] combined this knowledge and clustered dark patterns into high-level, meso-level, and low-level.

While the taxonomies and reports above help to understand the range of dark patterns in various contexts, they are less helpful for scenarios closely related to the right of access. Here, the taxonomy of the EDPB [19] is applicable when investigating account-based websites that are subject to rules of the GDPR. The taxonomy maps manipulative website parts to concrete dark patterns sorted into six categories *Overloading*, *Skipping*, *Stirring*, *Obstructing*, *Fickle*, and *Left in the Dark*. Each category contains 2–4 dark patterns, totaling 16 dark patterns. A detailed description follows in Section 3.4. Compared to [8], it offers a more nuanced differentiation between individual dark patterns regarding the GDPR and is well received within the dark pattern community [9, 1]. Overall, the taxonomy by the EDPB is suitable for our study due to its proximity to the GDPR.

Summarizing, dark patterns seem to be popular in the online space to subvert user's choices. A body of work has documented the real-world use of deceptive designs, ranging from shopping to transparency and privacy. In the realm of privacy and transparency, the prevalence of dark patterns, especially in consent choice banners, has been well-researched. We add to this by investigating the process of submitting a DSAR on popular websites for dark patterns. While Pöhn et al. [59] also described the dark patterns they encountered while investigating DSAR submissions, we complement this data with a larger scale analysis and a categorization of dark patterns into a fitting taxonomy providing references to the GDPR articles that might be breached.

3 Methodology

Following, we outline the methodology for examining the prevalence of dark patterns that can hinder a user's ability to request a copy of their personal data directly on a visited popular website taken from the first 500 entries of the Tranco list [42]. We first describe the process of creating our dataset of popular websites and the exclusion criteria used. Then, we detail our systematic process for the analysis on each website. Subsequently, we explain how we conducted qualitative analysis of dark patterns based on screencasts of these request attempts.

3.1 Website Corpus

The most clear ways to argue that a controller has to adhere to the GDPR are as follows. Either the establishment of the controller itself is located in the EU (*Article 3 I GDPR*) or the service is offered to users in the EU (*Article 3 para. 2 lit. a) GDPR*). This constitutes one of the reasons why we exclude any website without native English interface (mostly excluding websites with main user base in Asia or Russia) or is non-reachable since we try to access the websites from a country within the EU. Furthermore, consider that the GDPR also applies if citizens from the EU are tracked on the online service according to *Article 3 para. 2 lit. b).* As we consider only the top 500 entries of the Tranco list - hence highly popular online services - we argue that it is highly probable that the service offered is directed to EU citizens (too), as long as they also have a native English interface. While this does not always imply that a website has to adhere to the GDPR, the impact of the GPDR on regulations in other regions of the world analyzed in [47] supports the assumption that these websites fall under similar regulations. Hence, we do not include additional checks that websites must adhere to a fitting regional data policy.

Furthermore, we excluded websites requiring a verified phone number to register to protect the researchers' privacy[7]. For other personal information, such as addresses, we use fictitious data. Websites without a way of creating an account were also excluded. Those were usually governmental or educational websites. Lastly, we excluded websites using an account basis already present in the set of included websites. Those were usually services provided by bigger companies such as Google or Microsoft. Concluding, we excluded websites meeting any of the following criteria:

- The website was not reachable.
- The website lacked a native English user interface.
- No method for creating an account was found.

[7] As this was only the case for five websites, we did not obtain an anonymous phone number to create an account for each of the three researchers.

- A verified phone number was required for account creation.
- The website obviously utilized the account basis of another service already included in our list.

We started with an initial list of the 500 most visited websites according to the Tranco list[8] [42] generated on 18.07.2023. Three researchers independently accessed each website from the same country within the EU and following the exclusion criteria resulted in 166 websites to be considered. The complete list of 500 websites, including the exclusion reasons, can be found in the OSF repository[9]. The distribution of the 166 websites according to the "Website Categorization API" of WhoisXMLAPI[10] is shown in Figure 1. Most websites belong to the category "Computer and Internet Info" (35), closely followed by "Business and Economy" (26) and "News and Media" (19). Despite this skew at the top, we have 33 different categories in our dataset, providing some diversity.

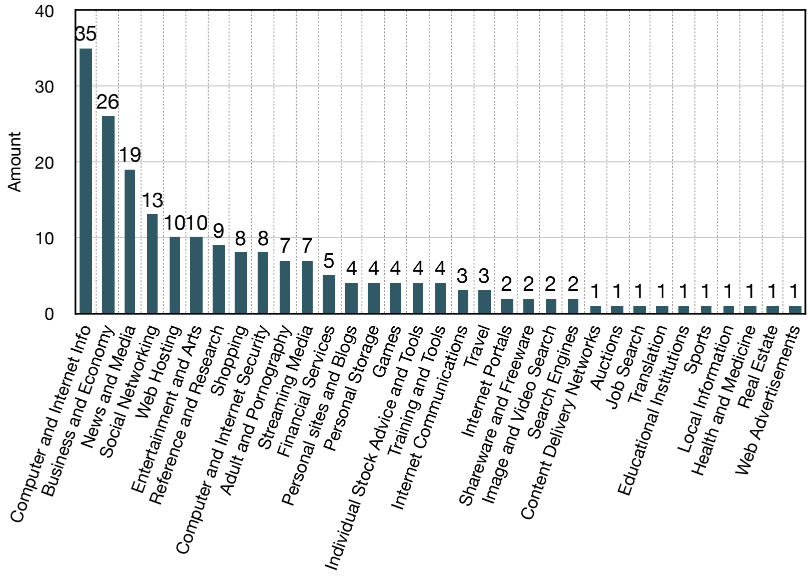


Fig. 1: Distribution of included websites per category. In total, there are 33 different website categories present in the dataset.

3.2 Request Procedure

For each website, we analyzed the path to pose a DSAR within the desktop version of the website. Each of the three researchers created a new account with

[8] https://tranco-list.eu/list/W9Z49 *(accessed: 18.07.2023)*

[9] https://osf.io/4jvhx/?view_only=ab6b8e27e7c34fdb86b7fb47feb89101

[10] https://whois.whoisxmlapi.com/ *(accessed: 13.02.2024)*

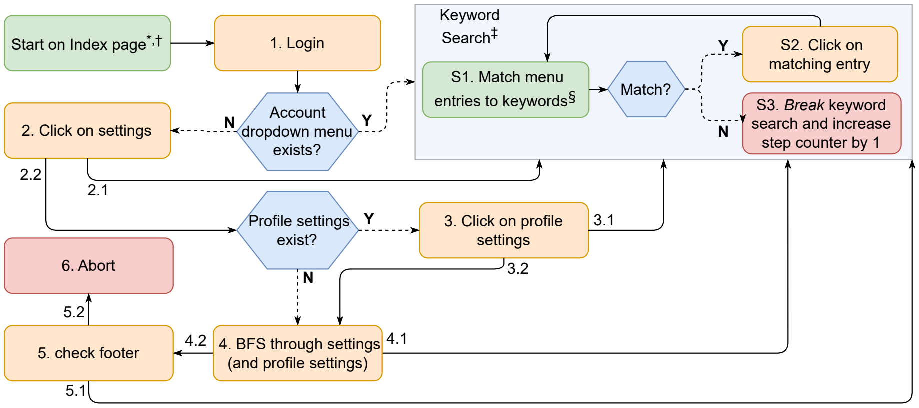
an e-mail address created only for this study and fictitious data (names, addresses,...). Each researcher carried out the request as far as possible on the website to not miss any interaction on the website itself. However, we did not respond to confirmation e-mails to avoid creating unnecessary work for data protection officers of the respective companies. By this, the amount of work created by our study is negligible, since most websites that do not automate the DSAR response require at least confirmation through the registered e-mail address before responding. In the case of direct download buttons, or request buttons (explanations for the request mechanisms encountered are given in Section 3.3), we clicked the respective button as we otherwise could never be sure whether there is additional action needed on the website and thus potentially miss additional hurdles. Note that these also often require confirmation via e-mail or lead to automated responses.

The accounts used did not generate a lot of data through usage of the service since they were often created minutes ago. However, we do not want to investigate the returned data but rather only the existence of dark patterns *until* the DSAR submission. Hence, our analysis is not hindered by this. For account creation and request analysis, each researcher accessed the website from the same country within the EU again. All researchers independently performed their request analysis. Data collection took place from July 2023 to August 2023. To achieve comparability between researchers for the later discussion, a search protocol was created and followed to navigate each website. While we suspect many users would first use a search engine to find out how they can request their data, we investigate the online infrastructure of the services themselves. Hence, we do not start with arbitrary vantage points on which a user could land after using a search engine, but rather with the page of an online service one gets redirected to after connecting to the given domain in our dataset, often called "index page". We do this to ensure we find dark patterns regardless of the vantage point a user would land on, but do not claim a user would necessarily encounter every single dark pattern we found. To achieve such a search protocol, two researchers discussed how they imagined a user searching for the option to request their data on the website. Then, both researchers picked ten random websites from the list and tried to find a way to pose a DSAR through the website using the initially discussed search protocol. The protocol was re-evaluated and updated accordingly. The final protocol can be seen in Figure 2. It consists of the following steps:

1. Log into the website and check whether an account dropdown menu exists. If so, match the entries to the predefined set of keywords from top to bottom. If we find a matching entry, click on it and repeat the search there. Once we cannot find any matching keywords anymore, or if it is obvious that we cannot find anything helpful here, stop the search.
2. If a settings menu entry exists, click on it and start the keyword search again.
3. If a dedicated profile settings menu entry exists, click on it and start the keyword search again.

4. If we did not find anything helpful until now, we click through all settings menu entries in a breadth-first search manner, i.e. we skim through each of them to look for related controls placed in unexpected menu points.
5. As a last resort, we check the website's footer and match for keywords again.

On each screen, we shortly check whether there is an obvious path to pose a DSAR.


Start on Index page*,†
1. Login
Keyword Search‡
S1. Match menu entries to keywords§
Match?
Y
S2. Click on matching entry
N
S3. *Break* keyword search and increase step counter by 1
Account dropdown menu exists?
N
Y
2. Click on settings
2.2
2.1
Profile settings exist?
Y
3. Click on profile settings
3.1
3.2
N
6. Abort
5.2
5. check footer
4.2
4. BFS through settings (and profile settings)
4.1
5.1

Notes

*: On each page load, we skim the page for obvious ways to carry out an access request. If there is an obvious way, it preceedes any other step.
†: If it is necessary to fill out a form, we fill it as far as possible.
‡: When we match for keywords, we do it always in a depth-first and top-to-bottom manner.

§: Keywords: access request, download request, data rights, personal data, privacy rights, GDPR, exercise your rights, privacy, security, compliance

Fig. 2: The final protocol we used to guide the search for ways to pose a DSAR.

After finalizing the search protocol, we used it as guidance for all subsequent request attempts. However, note that it is not feasible to always exactly adhere to this protocol for a corpus of 166 websites because of differences in the interfaces of the websites and derivations introduced by people navigating the web in slightly different ways. This protocol is intended to allow for general comparability between the attempts of the three researchers for the later analysis we describe in Section 3.5. Additionally, we made screencasts of each request attempt per researcher, which we used in the discussion to enrich the researcher's notes and allow us to make our research more transparent. We will make the screencasts available at the OSF repository[11]. In the review phase, we place only some examples in the repository since many of the screencasts would deanonymize us at least partly (e.g., leak affiliation names or IP addresses).

[11] https://osf.io/4jvhx/?view_only=ab6b8e27e7c34fdb86b7fb47feb89101

3.3 Codebook

In the following, we explain the codebook we used to analyze and categorize the request mechanisms and the dark patterns. Because of slight derivations in website usage, different researchers could find different mechanisms. For each website, we thus classified the final results of the request into the following mechanisms:

- **Simple Form**: any form that can be submitted by just using click events
- **Form**: any form that needs more input than just click events to submit it successfully
- **E-Mail**: stating an e-mail address to which one is supposed to write to make a request
- **Request Button**: button to start a data access request without further input
- **Download Button**: button to instantly download your data
- **Form Requiring Personal Data**: forms that require data that we did not want to disclose (e.g., a verified telephone number)
- **No Information Found**: no information how to pose a request was found
- **Impossible To Complete**: it was not possible to go on with the information provided
- **Not Checked**: the website was not checked

3.4 Dark Patterns

As we are not only interested in the DSAR submission mechanisms that users are provided on these popular websites, but specifically in the dark patterns implemented, we touch upon the categories of the EDPB taxonomy [19] in the following and introduce the types of dark patterns present in each category. Concrete examples are included in Section 4.4.

Overloading: Dark patterns within this category confuse users by providing *Too Many Options* regarding privacy choices, creating a *Privacy Maze* where users are led in circles, or using *Continuous Prompting* to make users enter more personal data than they initially intended.

Skipping: Dark patterns that use skipping try to distract users by using pointers to different page elements (*Look Over There*), making them overlook privacy choices by defaulting to unwanted options (*Deceptive Snugness*).

Stirring: Stirring is used for *Emotional Steering* where visual information or text influences users' emotions. This includes making buttons look deactivated or mentioning that posing a privacy request might lead to additional costs for the user. Additionally, stirring can be accomplished by placing information or controls *Hidden in Plain Sight*. For example, by burying an unstyled contact e-mail address in a large paragraph of text.

Obstructing: These patterns are rather aggressive as they actively hinder users in their process to exercise their rights by making the required steps or the path *Longer Than Necessary*, or by using *Misleading Actions* where a discrepancy of available information and performable actions confuse users. For example, a site states that users can exercise their rights by clicking on a given link, which takes them to a privacy article without any options to submit a request as promised. A *Dead End* can prevent users from continuing with their request. This includes misfunctioning buttons and websites where participants get stuck without further information on how to continue.

Fickle: Dark Patterns within this category affect the structural integrity of the website itself, through *Lacking Hierarchy* or having an *Inconsistent Interface*, also including *Language Discontinuity* where parts of a site suddenly switch the language without identifiable reasons. Additionally, *Decontextualising* works by hiding controls in unrelated sections or tabs and is also used to make users overlook actionable steps.

Left In The Dark: As the name suggests, dark patterns in this category confuse users by providing *Ambiguous Wording or Information* or *Conflicting Information*, where two pieces of information contradict each other. Through this, users usually do not know how to continue or whether they are following a sensible path to submit a request.

3.5 Analyzing Request Attempts

To analyze the runs for each website per researcher, we followed a qualitative analysis approach [22]. Starting with an open coding approach, each researcher independently noted the timestamps of the screencasts where they felt they saw a deceptive behavior by the website and added a comment describing the manipulation. Afterward, all three researchers sat together to coalesce the independent analyses into a final codebook. For each website and noted possible manipulation, it was discussed whether it

1. actually constitutes a dark pattern according to our notion,
2. in which category of the codebook it belongs,
3. and which specific type of dark pattern it is.

The discussion continued until consensus. If necessary, the respective screencast was reviewed together again. In the independent coding phase, the taxonomy's exact dark pattern was not yet stipulated. Rather, notes were created as basis for the discussion. The discussion was held over multiple meetings in September 2023. In the end, we reached a fully coded table[12] of dark patterns per website, together with a timestamp where one can see the encountered dark patterns in the recordings, a description for each dark pattern, and a categorization as discussed by the three researchers. We further discuss our findings in the following chapter based on this codebook.

[12] https://osf.io/4jvhx/?view_only=ab6b8e27e7c34fdb86b7fb47feb89101

4 Results

Following, we present our results by showing the general prevalence of dark patterns across the investigated websites (RQ1). Subsequently, we present the time spans required to finish all actions on a website for a DSAR to check the impact of dark patterns on request difficulty. Following, we focus on the request mechanisms identified (RQ2). Finally, we outline the distribution of dark patterns (RQ3) based on the EDPB taxonomy.

4.1 Dark Patterns per Website

Of the 166 examined websites, 113 (68%) contained at least one dark pattern, totaling 238 instances. On average, a website contained 1.43 dark patterns with a standard deviation of 1.59. Figure 3 illustrates the number of websites against the number of dark patterns found on a website. We can observe a trend, with many websites having a few patterns, gradually decreasing to a few extreme cases. Approximately one-third (32%) of the examined websites showed no dark patterns.

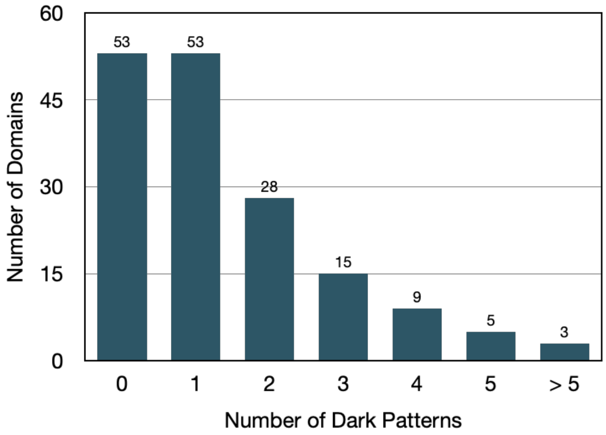


Fig. 3: Dark pattern usage from all websites within our study. Overall, we found that about 68% of all investigated websites utilize at least one dark pattern.

4.2 Timing Measurements

Figure 4 depicts box plots for each class containing websites with a specific number of dark patterns. The box plots represent the time a researcher needed to finish the actions on a website to pose a DSAR. Each attempt by any researcher is included as data point. We can see a trend of the median and, in most cases, the upper and lower percentiles increasing with the number of dark patterns. However, box plots with fewer dark patterns have more outliers, possibly due to more websites with fewer dark patterns (as shown in Figure 3) leading to more timing measurements in that plot.

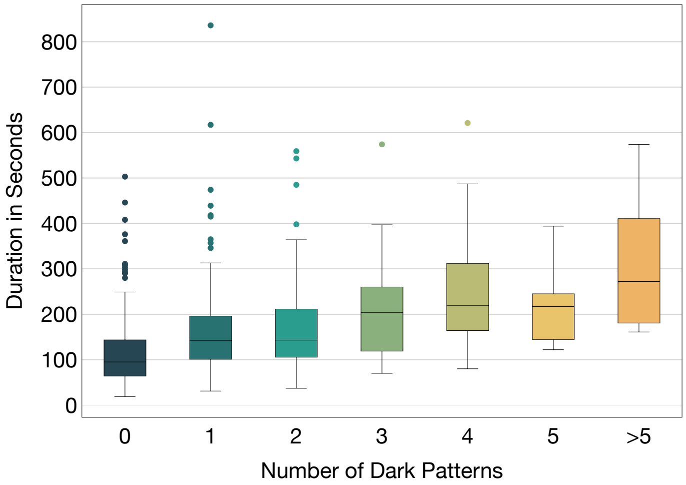


Fig. 4: Timing measurements for each of the website classes. Each box plot represents all the durations it took to finalize all the actions on a website for a DSAR. One can observe a trend of requests taking more time the more dark patterns are present on a website.

4.3 Request Mechanisms

Figure 5 illustrates the 265 identified request mechanisms. Note that it was not always the case that all researchers arrived at the same outcome. On 33 (19.9%) websites, we found more than one mechanism to pose a DSAR. Each share of the left pie chart shows the share of one of the mechanisms explained in Section 3.3. Most prevalent were online forms (26%), closely followed by an e-mail address (24%) to which one should write to submit a request. The smaller portions include simple forms (9%), request buttons (8%), and direct download buttons (3%). In 15% of the examined websites, at least one of the researchers could not find sufficient information. The right pie chart in Figure 5 shows on how many websites either one, two, or all three researchers were not able to find sufficient information.

4.4 Dark Pattern Distribution

As previously noted, we identified 238 instances of dark patterns in our examination of 166 popular websites. The left-hand side of Figure 6 displays the

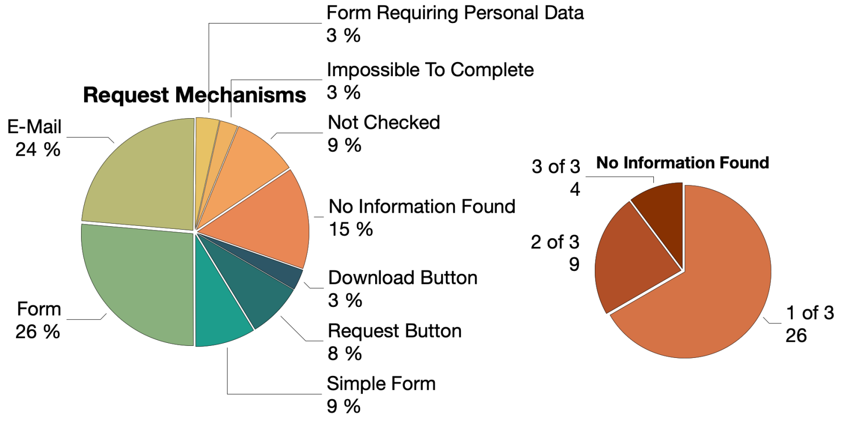


Fig. 5: Distribution of the 265 request mechanisms found on the 166 examined websites together with the amount of websites where one, two, or all three researchers did not find sufficient information for a DSAR.

distribution of these dark patterns across the six main categories of the EDPB taxonomy [19] (see Section 3.4). Besides, a pie chart for each main category shows the number of occurrences of the named dark patterns within the category. In the following sections, we show examples of dark patterns documented in our study for each of the main categories.

Obstructing The most prevalent category is *Obstructing*, which is nearly evenly split into the three available dark patterns. With 28 cases, *Dead End* is the most common. Examples include services limiting the number of requests a user can submit in a long period, while providing a shorter timeframe for downloading the data. One example is `epicgames.com`, which gives the user three days to download the data once it is prepared. Simultaneously, the user can request it only once every 90 days. Note that policies such as the GDPR often allow for limiting the frequency of requests to prevent services from being overburdened by a mass of requests from a single user. Nonetheless, the inability to retrieve their data if the user missed the shorter timeframe until the time for another request to be allowed makes this combination a *Dead End*. In one case (`soundcloud.com`), a request form could not be completed because it claimed the provided e-mail address was invalid, despite being the exact e-mail address used for registration. Another variant of this pattern involves broken links leading nowhere, as defined by the EDPB taxonomy [19]. A remarkable case of unclickable links were links shown on an image within a privacy policy on `quora.com`, allowing users to click only the image, not the included links. Some websites lead to a *Dead End* by requiring identifiers not all users necessarily possess (such as booking numbers on `booking.com`) as a means of identification, limiting DSARs to only a subset of users (such as paying customers).

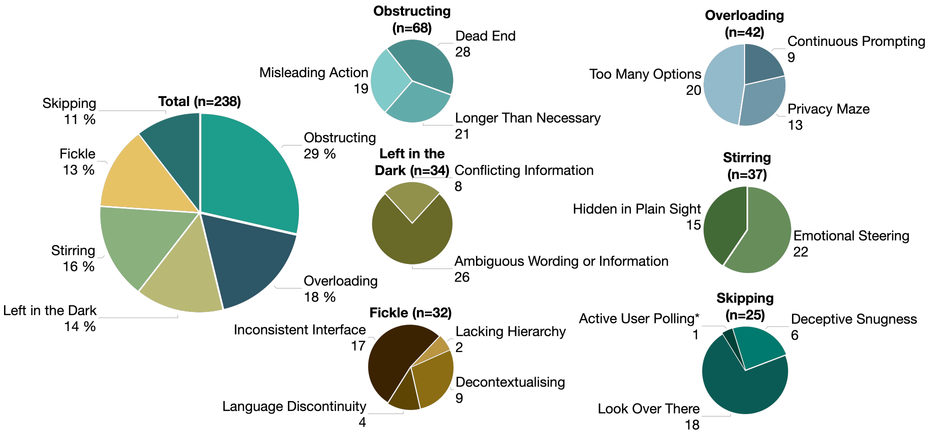
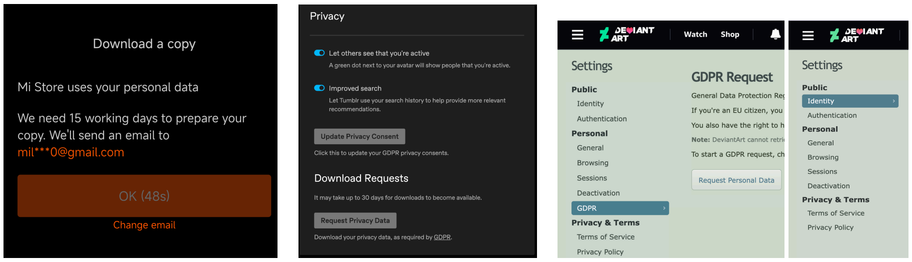


Fig. 6: The distribution of all 238 dark patterns found. Overall, dark patterns using *Obstructing* were used most often with 68 instances (29%). Regarding individual dark patterns across categories, the most frequently used were *Dead End* with 28 occurrences, *Ambiguous Wording* (26), *Emotional Steering* (22), *Longer Than Necessary* (21), and *Too Many Options* (20). We found a new pattern *Active User Polling* and added it to the *Skipping* category in the EDPB taxonomy [19].

Examples of *Misleading Actions* include websites such as `salesforce.com` stating in their privacy policy that users can exercise their rights in the account settings, while no controls are available there. In other instances, we were misled when attempting to change the language of the privacy policy back to English because it defaulted to another language, resulting in redirection to the start page. Examples of *Longer Than Necessary* (22 cases) involve service providers forcing users to make DSARs for each product individually instead of providing the option to request all stored data at once. On the website `xiaomi.com`, you have to wait for a 60-second timer before being able to click on the request confirm button as shown in Figure 7a.

Overloading The second-largest category is *Overloading* (18%), with nearly half of the dark patterns as *Too Many Options*. This often occurred on websites providing a plethora of links or documents seemingly related to privacy. In one extreme case, on `cisco.com`, we found a link directing to a database of "Privacy Sheets" containing documents in multiple languages for any product they offered. This is followed by the closely related *Privacy Maze* with 13 cases, often resulting from many different links linking back and forth, resulting in users going in circles. *Continuous Prompting* is primarily executed through DSAR forms asking for unnecessary personal information such as telephone numbers, which might discourage privacy-aware users from submitting.



Download a copy

Mi Store uses your personal data

We need 15 working days to prepare your copy. We'll send an email to mil***0@gmail.com

Let others see that you're active

A green dot next to your avatar will show people that you're active.

Improved search

Let Tumblr use your search history to help provide more relevant recommendations.

Click this to update your GDPR privacy consents.

Download Requests

It may take up to 30 days for downloads to become available.

Download your privacy data, as required by GDPR.

GDPR Request

General Data Protection Reg

If you're an EU citizen, you

You also have the right to h

Note: DeviantArt cannot retri

To start a GDPR request, ch

(a) The button on `xiaomi.com` is overlaid with a 60-second timer. After this time, you can click the button to send the request.

(b) The two buttons on `tumblr.com` look greyed out, suggesting they are disabled. However, they are working.

(c) The menu item "GDPR" on `deviantart.com` is only visible on a specific URL found in the privacy policy. Clicking on any other setting hides the menu item again.

Fig. 7: Some examples of dark patterns we found in our analysis. From left to right: (a) a button timer, (b) two greyed-out buttons, and (c) a hidden menu item. The timer (a) obstructs users from exercising their rights and the buttons (b) might make users question whether they are active. Hiding the "GDPR" menu item as default (c) makes people easily miss it.

Left in the Dark The category *Left in the Dark* has a share of 14% of the total number of dark patterns. The main dark pattern encountered here was presenting users with *Ambiguous Wording or Information*. For example, some services offer a way to "export their data" while hinting the returned data may be incomplete, e.g., on `bbc.com` where one is told "they won't include everything" without specifying how to achieve an export with "everything" included. Sometimes, we faced confusing explanations on checkboxes or other UI elements, e.g., on `salesforce.com` where the checkbox description does not clearly state whether one has to check or uncheck to receive all data. Similarly, we found 8 instances of *Conflicting Information*, such as stating different preferred paths for a DSAR without clarity on the currently intended path.

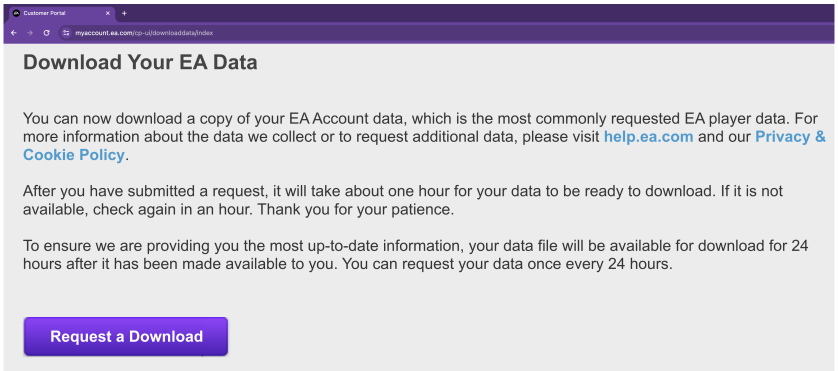
Stirring Here, we have two types of dark patterns, namely *Emotional Steering* with 22 occurrences, often achieved by intimidating the user by suggesting multiple requests could impose a cost on the user, especially without specifying what number of requests would lead to a charge or in what dimension this charge would lie in, e.g., on `issuu.com` or `tradingview.com`. This is often included in the privacy policy along with information about the user rights. One website, namely `mediafire.com`, also used the privacy policy to assure they are "not in the business of tracking [. . .]", painting a positive picture about their data processing practices. Some services (e.g., `bloomberg.com`) explicitly state that users exercising their rights might impact the provider's ability to maintain the service. The other 15 cases in the category *Stirring* are of the type *Hidden in Plain Sight*, which is already quite descriptive. Instances of this pattern include myspace.com where the request button is greyed out and placed non-prominently or, on mediafire.com, where the link to the privacy policy only becomes visible after clicking on a small icon in one of the bottom corners.

Fickle The second least common category *Fickle* consists mostly of the dark pattern *Inconsistent Interface* with 17 occurrences, where user expectations are not met with the usual website structure, e.g. a footer containing a link to the privacy policy only on some of the pages as seen on salesforce.com, linktr.ee, or slack.com. In this category, 9 patterns were found to be a way of *Decontextualizing*, often done by placing data request buttons in unrelated settings, such as in the "Notification Settings" (figma.com). Examples of *Language Discontinuity* (4 occurrences) are showing parts of the privacy policy in a different language than the rest of the privacy policy. We also found interfaces that are *Lacking Hierarchy* in 2 cases, for example, services that split information about the privacy controls across their different products or across different categories, such as unity3d.com.

Skipping The most common dark pattern in *Skipping* is *Look Over There* with 18 cases, where a user is diverted from their primary goal by placing distracting elements concurrently with the desired actions. For example, banners that show up with information about other privacy rights while trying to exercise a data subject right, as encountered on ibm.com. Trying to keep unfavorable options for the user by defaulting to them (*Deceptive Snugness* with 6 examples) was mostly found by services trying to give users incomplete data through defaulting to a short timespan (e.g., facebook.com) for the report of the personal data or pre-selecting only some data categories (e.g., google.com).

We found one particular interesting new dark pattern we placed in the category *Skipping*. Namely, on the website ea.com, one is told to actively check every hour whether the data is now prepared and ready to download, while also giving only 24 hours to download (see Figure 8) instead of sending an e-mail notification. This could lead to users forgetting about it for a sufficient time and then having to re-request the data. According to the description in the taxonomy, such behavior is in the category *Skipping* because the interface seems to be *designed in such a way that users forget* (cf. description in [19]) to actively check sufficiently frequent in the timeframe of 24 hours. However, it does not fit into the type of *Deceptive Snugness* as there are no pre-selected default options. Furthermore, the type *Look Over There* is not fitting as no elements compete for the user's attention. One could argue this creates a *Dead End (Obstructing)* for the user since they will not be able to download the data anymore once they forgot to actively check for the readiness of the download (until re-requesting). However, we argue that this constitutes another dark pattern, which only results from the dark pattern we currently have at hand. Namely, to burden the user with the task of actively polling for the download, while the service would have the means to send e-mail notifications. Hence, we name this dark pattern *Active*

User Polling. We do not consider this as indicative of a non-fitting taxonomy, as this is quite a specific implementation unlikely to occur frequently.



Download Your EA Data

You can now download a copy of your EA Account data, which is the most commonly requested EA player data. For more information about the data we collect or to request additional data, please visit help.ea.com and our Privacy & Cookie Policy.

After you have submitted a request, it will take about one hour for your data to be ready to download. If it is not available, check again in an hour. Thank you for your patience.

To ensure we are providing you the most up-to-date information, your data file will be available for download for 24 hours after it has been made available to you. You can request your data once every 24 hours.

Fig. 8: When requesting a copy of your data, the site states that the data should be ready in an hour. Instead of notifying the user when the data is available, the user is asked to return to the site after an additional hour. We call this dark pattern *Active User Polling*.

5 Discussion

The systematic examination of 166 popular websites led to 238 instances of identified dark patterns (RQ1) as shown in Figure 6. This finding would support the claim of service providers strategically introducing barriers on their websites, potentially discouraging users from exercising their right of access. Interestingly, some descriptions found by [59] were observed on a larger scale in our study as well. For instance, *making it impossible to access GDPR requests* [59] often aligns with the dark pattern *Dead End* from the EDPB taxonomy [19], which we encountered multiple times. Within our dataset of popular account-based websites, approximately one-third showed no dark patterns. However, in extreme cases we labeled up to 11 dark patterns on a single website (Figure 3).

Regarding the types of dark patterns (RQ3), obstructive patterns were the most prevalent, confirming findings similar to those of Kelly and Burkell [34] who categorize *Obstruction* as one of the main categories in their typology. The distribution across the other five categories did not show a significant preference. During the coding phase, placing instances into categories and corresponding types proved straightforward, supporting our assumption that the EDPB taxonomy [19] is appropriate for studies investigating data subject rights. Despite this, we added a new dark pattern, *Active User Polling*, to the existing category *Skipping*, although we suspect this to be a rare implementation.

While the amount of dark patterns could align with Waldman's assumption [69] of the industry's disinterest in meaningful privacy, we also acknowledge that discerning intentional dark patterns from unintentional is not always straightforward. Some patterns we described might serve a non-malicious purpose. The 60-second timer shown in Figure 7a could safeguard against denial-of-service attacks, while the hidden menu item in Figure 7c could be a programming error. In the end, it is not possible to be sure whether some observed behavior was intentional, and it always remains some plausible deniability. Note that this uncertainty is inherently in the nature of dark patterns. Consequently, we provide the codebook including notes and screencasts to make each case transparent. However, the observed increase in time with a higher number of labeled dark patterns (Figure 4) suggests actual hindrances in posing DSARs on websites with more dark patterns, potentially infringing on *Article 12 para. 2* of the GDPR. This aligns with previous findings [68, 10] which show at least questionable usability of DSAR submission processes. Such shortcomings can induce a negative view of data protection policies for end users [5] and distrust in providers employing dark patterns [10]. This may even lead users to abstain from exercising their rights [65].

Similar to prior studies [3, 66], we found that various websites offer multiple DSAR submission mechanisms (RQ2), with e-mail addresses and website forms being the most common as shown in Figure 5. Direct data download buttons are scarce, suggesting manual DSAR responses over automated ones. Furthermore, we see there are three websites where all three researchers struggled to find adequate information, suggesting a lack of information or even intentional concealment. While the number of such cases seems low compared to [3], it is noteworthy that each of the three researchers searched for a mechanism and only in three cases, none of all three could find enough information. Furthermore, our corpus consists of highly popular websites that presumably try to adhere to different regional data policies nowadays and thus often provide at least an e-mail address for DSARs.

5.1 Ethical Considerations

In this study, we did not deal with the personal data of other users. Rather, we used freshly generated anonymous e-mail accounts and fictitious data. Nonetheless, online services might have stored secondary data, e.g., IP addresses. To authenticate to such data, we relied on account credentials, assuming any data potentially returned is associated with our test accounts. Additionally, we limited the dataset to websites that we could investigate without requiring privacy-sensitive information. We introduce as little manual work and expenses for data protection officers of companies as possible by restricting our actions to the website interfaces. Typically, this meant refraining from following up on automated e-mails requesting DSAR submission confirmation. In a few other cases, the response was anyway automated and gave a direct download link and hence did not generate additional manual work.

Note that we decided against notifying the 113 website operators about the dark patterns detailed in our study. Responsible disclosure, common in vulnerability reporting, involves notifying responsible actors to fix issues before public disclosure to prevent malicious exploitation by third parties. However, none of the identified dark patterns allowed for third-party exploitation. The potential impact on company reputation was also deemed low, given the extensive documentation of dark pattern use across various domains such as shopping [50], consent notifications [38, 55, 35], legitimate interest [40] and even in the case of the right of access [43, 59], with some already explicitly naming companies. Hence, we think the reputational impact is marginal at most. Nevertheless, we would welcome an effect on stricter enforcement of regional data regulations such as the GDPR or even regular audits for dark patterns as proposed by [44]. Due to the inherent plausible deniability of dark patterns, we also refrain from seeking statements from website operators, since we have no reliable way to verify the veracity of such statements. Reporting only trends or aggregated numbers would compromise the transparency and reproducibility of our work by keeping codebooks and screencasts unpublished. We think transparent publication still allows willing companies to address unintentional dark patterns without significant reputational risk.

5.2 Limitations

Our study was conducted through manual analysis, thus it is possible that we did not encounter every dark pattern implemented on a website. The search protocol used might have excluded request paths, leading to reported dark pattern numbers possibly representing the lower boundary of actual occurrences. Additionally, as already discussed, we can never be sure that a dark pattern was intentional or incorrectly labeled by the researchers conducting the study. We tried to counteract the ambiguity by having three researchers with different backgrounds (security and privacy, human-computer interaction, and technical communication) conduct the analysis and by discussing all the results until consensus. We focused solely on the websites of online services, while there is no specific manner prescribed on how data subjects have to pose a DSAR. Additionally, we concentrated on the DSAR submission process, omitting the recording or examination of responses. Existing work, such as [66, 39, 68, 10, 59], already show a trend of low usability for end users in data controller responses. We intentionally made no statements about the conformity of singular webpages, as this needs to be decided on a case-by-case basis. We can merely supply evidence for or against the conformity. Additionally, there are other data subject rights which may face similar hindrances from deceptive design choices. Investigating different data subject rights helps to enhance the understanding of the practical implementations of data protection regulations. While our work shows a trend in dark pattern usage among popular websites, further research with larger datasets is essential to strengthen such findings. Finally, our assessments were conducted exclusively on desktop versions of the websites. The dark pattern landscape may differ on mobile versions or on apps. Kröger et al. [39] have highlighted numerous issues with the right of access on apps. Hence, it is not too far off to suspect dark patterns on mobile platforms.

6 Conclusion

We analyzed 166 of the 500 most popular websites for their use of dark patterns inhibiting DSARs and found that on 113 of 166, i.e., 68%, websites there is at least one dark pattern, and often more than one, totaling 238 instances of dark patterns. We used the taxonomy given by the EDPB [19] to categorize our findings, linking related GDPR articles that might be breached. Furthermore, we found that patterns of obstructing type are the most common and showed that higher numbers of dark patterns correlate with longer times to invoke the right of access. Our work adds to documenting dark patterns in various areas, highlighting their prevalence in the realm of data subject rights, particularly against the right of access.

6.1 Future Work

Future steps include expanding measurements to validate findings on a larger scale. To enable larger-scale studies, it is necessary to investigate the feasibility of automating such dark pattern checks, as manual inspection becomes impractical with a sufficiently extensive data set. This could even facilitate periodic measurements to evaluate the impact of new regulations, such as the *Digital Services Act* [21]. Furthermore, assessments of dark patterns hindering data subject rights should extend to platforms other than desktop websites, such as mobile browsers or apps. As there are more data subject rights than just the right of access, it can also be suitable to explore dark patterns in relation to these rights. Researchers should examine different countermeasures and stronger regulations against dark patterns in the realm of user privacy rights, and keep investigating the practical effects of introduced regulations.

Bibliography

[1] Access Now, Simply Secure, World Wide Web Foundation: Comments to the EDPB consultation on Guidelines 3/2022 on dark patterns in social media platform interfaces (2023), https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/EDPB%20consultation%20-%20Guidelines%20on%20dark%20patterns%20in%20social%20media%20platform%20interfaces.pdf

[2] Alizadeh, F., Jakobi, T., Boldt, J., Stevens, G.: GDPR-Reality Check on the Right to Access Data: Claiming and Investigating Personally Identifiable Data from Companies. In: Proceedings of Mensch Und Computer 2019. p. 811–814. MuC '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3340764.3344913

[3] Ausloos, J., Dewitte, P.: Shattering One-Way Mirrors. Data Subject Access Rights in Practice. International Data Privacy Law **8**(1), 4–28 (2018). https://doi.org/10.1093/idpl/ipy001

[4] Bollinger, D., Kubícek, K., Jiménez, C.C., Basin, D.A.: Automating Cookie Consent and GDPR Violation Detection. In: USENIX Security Symposium (2022), https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger

[5] Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., Lenzini, G.: "I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" - Dark Patterns from the End-User Perspective. In: Designing Interactive Systems Conference 2021. p. 763–776. DIS '21, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3461778.3462086

[6] Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., Santos, C.: Security Analysis of Subject Access Request Procedures: How to Authenticate Data Subjects Safely When They Request for Their Data. In: Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7. pp. 182–209. Springer (2019). https://doi.org/10.1007/978-3-030-21752-5_12

[7] Borberg, I., Hougaard, R., Rafnsson, W., Kulyk, O.: "So I Sold My Soul": Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions. Proceedings 2022 Symposium on Usable Security (2022), https://www.ndss-symposium.org/wp-content/uploads/usec2022_23026_paper.pdf

[8] Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S.: Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proc. Priv. Enhancing Technol. **2016**(4), 237–254 (2016). https://doi.org/10.1515/popets-2016-0038

[9] Botes, W.M., Carli, R., Rossi, A., Sanchez Chamorro, L., Santos, C., Sergeeva, A.: Feedback to the Guidelines 3/2022 on "Dark patterns in social media platform interfaces: How to recognise and avoid them" (2022),

https://orbilu.uni.lu/bitstream/10993/52741/1/comments_to_edpb_guidelines_on_dark_patterns_for_social_media_-_decepticon_unilu_0.pdf

[10] Bowyer, A., Holt, J., Go Jefferies, J., Wilson, R., Kirk, D., David Smeddinck, J.: Human-GDPR Interaction: Practical Experiences of Accessing Personal Data. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3491102.3501947

[11] Bufalieri, L., Morgia, M.L., Mei, A., Stefa, J.: GDPR: When the Right to Access Personal Data Becomes a Threat. In: 2020 IEEE International Conference on Web Services (ICWS). pp. 75–83 (2020). https://doi.org/10.1109/ICWS49710.2020.00017

[12] Bygrave, L.A.: Data Privacy Law: An International Perspective. Oxford University Press (2014). https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

[13] Cagnazzo, M., Holz, T., Pohlmann, N.: GDPiRated – Stealing Personal Information On- and Offline. In: Computer Security – ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part II 24. pp. 367–386. Springer (2019). https://doi.org/10.1007/978-3-030-29962-0_18

[14] California Consumer Privacy Act of 2018 (2018), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[15] Decision of the EEA Joint Committee No. 154/2018 of July 6, 2018 (2018), https://op.europa.eu/en/publication-detail/-/publication/03c28303-8b25-11e8-8a53-01aa75ed71a1/language-en

[16] Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., Bacchelli, A.: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. p. 1–14. CHI '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3313831.3376600

[17] Di Martino, M., Meers, I., Quax, P., Andries, K., Lamotte, W.: Revisiting Identification Issues in GDPR 'Right Of Access' Policies: A Technical and Longitudinal Analysis. Proceedings on Privacy Enhancing Technologies **2022**(2), 95–113 (2022). https://doi.org/10.2478/popets-2022-0037

[18] European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., Rodríguez de las Heras Ballell, T.: Behavioural study on unfair commercial practices in the digital environment - Dark patterns and manipulative personalisation - Final Report. Publications Office of the European Union, Brussels, Belgium (2022). https://doi.org/10.2838/859030

[19] European Data Protection Board: Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them (2022), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

[20] European Parliament, Council of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council (2016), https://data.europa.eu/eli/reg/2016/679/oj

[21] European Parliament, Council of the European Union: Regulation (EU) 2022/2065 of the European Parliament and of the Council (2022), https://data.europa.eu/eli/reg/2022/2065/oj

[22] Flick, U.: An Introduction to Qualitative Research. Sage publications (2022), https://uk.sagepub.com/en-gb/eur/an-introduction-to-qualitative-research/book278983

[23] Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The Dark (Patterns) Side of UX Design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. p. 1–14. CHI '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3173574.3174108

[24] Gray, C.M., Santos, C., Bielova, N.: Towards a Preliminary Ontology of Dark Patterns Knowledge. In: Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems. CHI EA '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3544549.3585676

[25] Greenleaf, G.: Global Tables of Data Privacy Laws and Bills. Privacy Laws & Business International Report. (2021). https://doi.org/10.2139/ssrn.3836261

[26] Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., Wilson, C.: A Comparative Study of Dark Patterns Across Web and Mobile Modalities. Proc. ACM Hum.-Comput. Interact. **5**(CSCW2) (oct 2021). https://doi.org/10.1145/3479521

[27] Gundelach, R., Herrmann, D.: Cookiescanner: An Automated Tool for Detecting and Evaluating GDPR Consent Notices on Websites. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3605000

[28] Habib, H., Li, M., Young, E., Cranor, L.: "Okay, Whatever": An Evaluation of Cookie Consent Interfaces. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3491102.3501985

[29] Habib, H., Pearman, S., Wang, J., Zou, Y., Acquisti, A., Cranor, L.F., Sadeh, N., Schaub, F.: "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. p. 1–12. CHI '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3313831.3376511

[30] Hausner, P., Gertz, M.: Dark Patterns in the Interaction with Cookie Banners (2021). https://doi.org/10.48550/arXiv.2103.14956, https://dbs.ifi.uni-heidelberg.de/files/Team/phausner/publications/Hausner_Gertz_CHI2021.pdf, position Paper at the Workshop "What

Can CHI Do About Dark Patterns?" at the CHI Conference on Human Factors in Computing Systems (CHI '21)

[31] Hennemann, M., Lienemann, G., Sprikl, C.: Mapping Global Data Law. University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-16. (2022), https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/lehrstuehle/hennemann/Mapping_Global_Data_Law/Hennemann_Lienemann_Spirkl_Mapping_Global_Data_Law_Part_I_Data_Protection_Legislation_August_2022_Version_1.1__1_.pdf

[32] Hidaka, S., Kobuki, S., Watanabe, M., Seaborn, K.: Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3544548.3580942

[33] Jarovsky, L.: Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness (2022). https://doi.org/10.2139/ssrn.4048582

[34] Kelly, D., Burkell, J.: Documenting Privacy Dark Patterns: How Social Networking Sites Influence Users' Privacy Choices. FIMS Publications. 376. (2023), https://ir.lib.uwo.ca/fimspub/376

[35] Kirkman, D., Vaniea, K., Woods, D.W.: DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs. In: 8th IEEE European Symposium on Security and Privacy. IEEE (2023). https://doi.org/10.1109/EuroSP57164.2023.00055

[36] Kowalczyk, M., Gunawan, J.T., Choffnes, D., Dubois, D.J., Hartzog, W., Wilson, C.: Understanding Dark Patterns in Home IoT Devices. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3544548.3581432

[37] Kretschmer, M., Pennekamp, J., Wehrle, K.: Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. ACM Trans. Web **15**(4) (jul 2021). https://doi.org/10.1145/3466722

[38] Krisam, C., Dietmann, H., Volkamer, M., Kulyk, O.: Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. In: Proceedings of the 2021 European Symposium on Usable Security. p. 1–8. EuroUSEC '21, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3481357.3481516

[39] Kröger, J.L., Lindemann, J., Herrmann, D.: How do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on iOS and Android Apps. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3407023.3407057

[40] Kyi, L., Ammanaghatta Shivakumar, S., Santos, C.T., Roesner, F., Zufall, F., Biega, A.J.: Investigating Deceptive Design in GDPR's Legitimate Interest. In: Proceedings of the 2023 CHI Conference on Human Factors in

Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3544548.3580637

[41] Lauradoux, C.: Can Authoritative Governments Abuse the Right to Access? In: Privacy Technologies and Policy. pp. 23–33. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-031-07315-1_2

[42] Le Pochat, V., Van Goethem, T., Tajalizadehkhoob, S., Korczyński, M., Joosen, W.: Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: Proceedings of the 26th Annual Network and Distributed System Security Symposium. NDSS 2019 (Feb 2019). https://doi.org/10.14722/ndss.2019.23386

[43] Li, W., Li, Z., Li, W., Zhang, Y., Li, A.: Mapping the Empirical Evidence of the GDPR (In-)Effectiveness: A Systematic Review (2023), https://doi.org/10.48550/arXiv.2310.16735

[44] Luguri, J., Strahilevitz, L.J.: Shining a Light on Dark Patterns. Journal of Legal Analysis **13**(1), 43–109 (03 2021). https://doi.org/10.1093/jla/laaa006

[45] Machuletz, D., Böhme, R.: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. Proc. Priv. Enhancing Technol. **2020**(2), 481–498 (2019). https://doi.org/10.2478/popets-2020-0037

[46] Mahieu, R., Asghari, H., van Eeten, M.: Collectively Exercising the Right of Access: Individual Effort, Societal Effect. Internet Policy Review **7**(3) (2018). https://doi.org/10.14763/2018.3.927

[47] Mahieu, R., Asghari, H., Parsons, C., van Hoboken, J., Crete-Nishihata, M., Hilts, A., Anstis, S.: Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens? Journal of Information Policy **11**, 301–349 (2021). https://doi.org/https://doi.org/10.5325/jinfopoli.11.2021.0301

[48] Mahieu, R.: The Right of Access to Personal Data: a Genealogy. Technology and Regulation **2021**, 62–75 (Aug 2021). https://doi.org/10.26116/techreg.2021.005

[49] Martino, M.D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., Andries, K.: Personal Information Leakage by Abusing the GDPR 'Right of Access'. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). pp. 371–385. USENIX Association, Santa Clara, CA (Aug 2019), https://www.usenix.org/conference/soups2019/presentation/dimartino

[50] Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A.: Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proc. ACM Hum.-Comput. Interact. **3**(CSCW) (nov 2019). https://doi.org/10.1145/3359183

[51] Mathur, A., Kshirsagar, M., Mayer, J.: What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. CHI '21, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3411764.3445610

[52] Mildner, T., Savino, G.L., Doyle, P.R., Cowan, B.R., Malaka, R.: About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3544548.3580695

[53] Monge Roffarello, A., Lukoff, K., De Russis, L.: Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3544548.3580729

[54] Norris, C., De Hert, P., L'hoiry, X., Galetta, A.: The Unaccountable State of Surveillance. Exercising Access Rights in Europe. Springer, Cham **10**, 978–3 (2017). https://doi.org/10.1007/978-3-319-47573-8

[55] Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. p. 1–13. CHI '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3313831.3376321

[56] Pavur, J., Knerr, C.: GDPArrrrr: Using Privacy Laws to Steal Identities. CoRR **abs/1912.00731** (2019), http://arxiv.org/abs/1912.00731

[57] Petelka, J., Oreglia, E., Finn, M., Srinivasan, J.: Generating Practices: Investigations into the Double Embedding of GDPR and Data Access Policies. Proc. ACM Hum.-Comput. Interact. **6**(CSCW2) (nov 2022). https://doi.org/10.1145/3555631

[58] Pins, D., Jakobi, T., Stevens, G., Alizadeh, F., Krüger, J.: Finding, getting and understanding: the user journey for the GDPR's right to access. Behaviour & Information Technology **41**(10), 2174–2200 (2022). https://doi.org/10.1080/0144929X.2022.2074894

[59] Pöhn, D., Mörsdorf, N., Hommel, W.: Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3605064

[60] Raento, M.: The Data Subject's Right of Access and to be Informed in Finland: An Experimental Study. International Journal of Law and Information Technology **14**(3), 390–409 (10 2006). https://doi.org/10.1093/ijlit/eal008

[61] Schade, F.: Dark Sides of Data Transparency: Organized Immaturity After GDPR? Business Ethics Quarterly **33**(3), 473–501 (2023). https://doi.org/10.1017/beq.2022.30

[62] Schäfer, R., Preuschoff, P.M., Borchers, J.: Investigating Visual Countermeasures Against Dark Patterns in User Interfaces. In: Proceedings of Mensch Und Computer 2023. p. 161–172. MuC '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3603555.3603563

[63] Singh, J., Cobbe, J.: The Security Implications of Data Subject Rights. IEEE Security & Privacy **17**(6), 21–30 (2019). https://doi.org/10.1109/MSEC.2019.2914614

[64] Soe, T.H., Nordberg, O.E., Guribye, F., Slavkovik, M.: Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. NordiCHI '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3419249.3420132

[65] Sørum, H., Presthus, W.: Dude, where's my data? The GDPR in practice, from a consumer's point of view. Information Technology & People **34**(3), 912–929 (2021). https://doi.org/10.1108/ITP-08-2019-0433

[66] Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N.: A Study on Subject Data Access in Online Advertising After the GDPR. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings 14. pp. 61–79. Springer (2019). https://doi.org/10.1007/978-3-030-31500-9_5

[67] Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. p. 973–990. CCS '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3319535.3354212

[68] Veys, S., Serrano, D., Stamos, M., Herman, M., Reitinger, N., Mazurek, M.L., Ur, B.: Pursuing Usable and Useful Data Downloads Under GDPR/CCPA Access Rights via Co-Design. In: Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021). pp. 217–242 (2021), https://www.usenix.org/conference/soups2021/presentation/veys

[69] Waldman, A.E.: Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power. Cambridge University Press (2021). https://doi.org/10.1017/9781108591386

[70] Wong, J., Henderson, T.: How Portable is Portable? Exercising the GDPR's Right to Data Portability. In: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers. p. 911–920. UbiComp '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3267305.3274152

[71] Younas, A., ogli Mirzaraimov, B.T.: To What Extent are Consumers Harmed in the Digital Market from the Perspective of the GDPR? International Journal of Multidisciplinary Research and Analysis **4**(8) (2021). https://doi.org/10.47191/ijmra/v4-i8-17

[72] Zagal, J.P., Björk, S., Lewis, C.: Dark Patterns in the Design of Games. In: Foundations of Digital Games 2013 (2013), https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1043332