Redress for dark patterns privacy harms?

Gunawan, Johanna ; Santos, Cristiana; Kamara, Irene

Published in:
CSLAW '22

DOI:
10.1145/3511265.3550448

Publication date:
2022

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

Citation for published version (APA):
Gunawan, J., Santos, C., & Kamara, I. (2022). Redress for dark patterns privacy harms? A case study on consent interactions. In *CSLAW '22: Proceedings of the 2022 Symposium on Computer Science and Law* (pp. 181-194). Association for Computing Machinery (ACM). https://doi.org/10.1145/3511265.3550448

Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions

Johanna Gunawan*
gunawan.jo@northeastern.edu
Northeastern University
Boston, USA

Cristiana Santos*
c.teixeirasantos@uu.nl
Utrecht University
Utrecht, The Netherlands

Irene Kamara**
i.kamara@tilburguniversity.edu
Tilburg University
Tilburg, The Netherlands

ABSTRACT

Internet users are constantly subjected to incessant demands for attention in a noisy digital world. Countless inputs compete for the chance to be clicked, to be seen, and to be interacted with, and they can deploy tactics that take advantage of behavioral psychology to 'nudge' users into doing what they want. Some nudges are benign; others deceive, steer, or manipulate users, as the U.S. FTC Commissioner says, "into behavior that is profitable for an online service, but often harmful to [us] or contrary to [our] intent". These tactics are *dark patterns*, which are manipulative and deceptive interface designs used at-scale in more than ten percent of global shopping websites and more than ninety-five percent of the most popular apps in online services.

Literature discusses several types of *harms* caused by dark patterns that includes harms of a *material nature*, such as financial harms, or anticompetitive issues, as well as harms of a *non-material nature*, such as privacy invasion, time loss, addiction, cognitive burdens, loss of autonomy, and emotional or psychological distress. Through a comprehensive literature review of this scholarship and case law analysis conducted by our interdisciplinary team of HCI and legal scholars, this paper investigates whether harms caused by such dark patterns could give rise to redress for individuals subject to dark pattern practices using consent interactions and the GDPR consent requirements as a case study.

CCS CONCEPTS

• **Human-centered computing → HCI design and evaluation methods**; Web-based interaction; • **Social and professional topics** → *Computing / technology policy*; • **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

dark patterns, deceptive design, redress, damages, consent, GDPR, data protection infringement, harm, policy and law

ACM Reference Format:
Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW '22), November 1–2, 2022, Washington, DC, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3511265.3550448

1 INTRODUCTION

Internet users are constantly subjected to incessant demands for attention in a noisy digital world. Countless inputs compete for the chance to be clicked, to be seen, and to be interacted with, and they can deploy tactics that take advantage of behavioral psychology to 'nudge' users into doing what they want. Some nudges are benign; others deceive, steer, or manipulate users, as the U.S. FTC Commissioner says, "into behavior that is profitable for an online service, but often harmful to [us] or contrary to [our] intent" [25]. These tactics are *dark patterns*, which are manipulative and deceptive interface designs used at-scale in more than ten percent of global shopping websites [89] and more than ninety-five percent of the most popular apps in online services [43]. These deceptive practices may have profound consequences impacting users in general, but may cause even more problems for vulnerable populations such as minors, and other users who may be especially susceptible or do not have the online experience to identify them.

Literature discusses several types of *harms* caused by dark patterns, including harms of a *material nature*, such as financial harms, or anti-competitive issues, and harms of a *non-material nature*, such as privacy invasion, time loss, addiction, cognitive burdens, loss of autonomy, and emotional or psychological distress. Reviewing and building on such scholarship, this paper investigates whether harms caused by dark patterns could give rise to redress for individuals using consent interactions as a case study.

Since dark patterns rely heavily on the collection and processing of personal information of users, the basis for our analysis focuses of privacy and data protection law. Through comprehensive literature review and case law analysis in Systematization-of-Knowledge style conducted by our interdisciplinary team of HCI and legal scholars, our contribution aims at investigating whether data protection legislation may offer a framework for redress for the material and immaterial damages a natural person has suffered by dark patterns. Specifically, we focus on the EU General Data Protection Regulation (GDPR) [115], as the GDPR establishes the right to an effective judicial remedy and compensation for any person who has suffered material or non-material damages. Thus, this paper aims to:

- systematically bring together in an interdisciplinary manner two bodies of literature: dark pattern harms and EU data protection law remedies
- articulate the contours for awarding damages by selected national courts of EU Member States and by data protection authorities

[*] All authors contributed equally to this research.

CSLAW '22, November 1–2, 2022, Washington, DC, USA.
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9234-1/22/11…$15.00
https://doi.org/10.1145/3511265.3550448

- present consent under the GDPR as a case study to explore potential for redress regarding dark patterns
- identify areas for further research towards models of redress for dark pattern harms

The contribution is structured as follows. In section 2, we review dark patterns harms taxonomies and scholarship, followed by section 3 where we more closely inspect privacy contexts wherein dark patterns have been identified, including dark patterns triggered by online consent requests. Then, in section 4, we analyze how regulations approach redress and the requirements for potentially awarding damages for dark pattern-related harms and infringements. This section provides an analysis of the two-tier remedies system of the GDPR, namely the civil courts redress and the administrative penalties mechanism, in an exploration of what remedies are available to users. This section also presents the limitations of the GDPR remedies system, especially as regards, for example, the difficulty of courts to set appropriate thresholds for damages and harmonised calculation methods. Those limitations in turn may bring practical obstacles to materialising the potential of the GDPR system for delivering actual redress to individuals targets of dark pattern practices. We then utilize the GDPR consent requirements as a case study to explore how various dark patterns might violate regulations in section 5, uniting our discussion of dark patterns privacy harms to consent regimes as outlined by the GDPR. In section 6, we briefly discuss how privacy dark patterns harms, GDPR consent requirements, and avenues for redress might be linked to compensate users targeted by dark pattern trickery as a preliminary investigation into the feasibility of user recourse. Finally, section 7 concludes by providing an outlook for further research towards regulating dark patterns harms.

2 UNDERSTANDING DARK PATTERN HARMS

This section proceeds with a survey of dark patterns literature and specifically examines discussions of harms, or negative consequences or outcomes caused by dark patterns. We then address the general harm categories taxonomized by existing work in subsubsection 2.1.1, and categorize descriptions of harms from other literature in subsubsection 2.1.2. This paper builds upon prior frameworks and focuses on privacy-related harms, insofar as dark patterns contribute to them within a case study on consent practices.

Methodology for Collecting Dark Patterns and Harms Literature. The first comprehensive survey of dark patterns literature with regards to a harms was conducted by Mathur et. al. [90]. We begin with their dataset, originally compiled in late 2020. We append recent publications to this collection [90] by compiling work during February and March 2022, following similar methods for identifying and filtering dark patterns work – that is, we first search the ACM Digital Library, arXiV, SSRN, and Google Scholar for 'dark patterns' work seen in academic venues or forthcoming work. However, we additionally include related papers that discuss dark patterns (thus including work like [52], which discusses user experiences of manipulation) and privacy UX papers (like [6] which explores UI issues with Do Not Sell My Private Information requests) if the focus of the work contributes to an understanding of dark pattern or deceptive design harms; we exclude papers that incidentally mention dark patterns if the work does not support deeper discussion into such harms or design.[1] We also include other resources like the Dark Patterns Tipline [125] or FTC workshop materials [18] if their contribution to advancing dark patterns knowledge is potentially

Document Type	**Prior Work**
Taxonomies and Framing	Brignull [17] Gray et. al. [53] Mathur et. al. [90] **Bösch et. al.** [16] Dark Patterns Tipline [125] Lacey & Caudwell [78] Greenberg et. al. [56] ***Jarovksy** [71]
Measurement Work	Zagal et. al. [140] Mathur et. al. [89] **Habib et. al.** [60] **Sanchez-Rola et. al.** [121] **Soe et. al.** [126] **Gray et. al.** [54] **Matte et. al.** [91] Gunawan et. al [57] **Van Nortwick & Wilson** [6]
User Studies	Acquisti et. al. [8] Fansher et. al. [47] **Utz et. al.** [133] **Habib et. al.** [59] Maier & Harr [88] Bhoot et. al. [86] **Machuletz & Böhme** [87] Bongard-Blanchy et. al. [15] Gray et. al. [52] **Graßl et. al.** [55]
Multi-Method Work	Conti & Sobiesk [27] DiGerinomo et. al. [43] **Nouwens et. al.** [96] Mildner & Savino [93]
Policy and Regulatory Literature	Forbrukerrådet [28] **Hartzog** [66] Frischmann [49] Day & Stemler [38] *Berbece [13] CNIL: Shaping Choices in the Digital World [24] **CCPA/CPRA** [2, 10] Luguri & Strahilevitz [83] DETOUR Act [135] **Waldman** [134] FTC: Bringing Dark Patterns to Light [18] **King & Stephan** [75] Hung [69]

Table 1: The documents used in our dark patterns literature survey, organized by contribution type and publication date (N=44). Bolded titles refer to work that extensively or exclusively focuses on consent, opt-out, similar decision-making privacy interactions like DNSMPI, or otherwise significantly focus on privacy (N=17).

[1] For example, while Matte et. al. [92] acknowledge dark patterns, the paper does not closely examine designs or interfaces and focuses instead on an analysis of policies and legal purposes. Such work is useful for a broader inspection of data collection, consent, and user experiences, it is not within scope for the purposes of our paper.

significant. This final dataset of dark pattern documents examined includes 44 items and is represented in Table 1.

We secondarily consider early-stage work informally presented at academic venues, e.g. workshop position papers, as we find that this early work is useful for an understanding of how scholars perceive dark pattern harms. This secondary set of 17 documents is described in section 8 and shown in Table 4.[2]

2.1 How Dark Patterns Literature Understands Harms

2.1.1 Harm Taxonomies in Dark Patterns Literature. Herewith we acknowledge explicit taxonomies of dark pattern harms provided by prior work, of which there are two main contributions. Mathur et. al. provide a brief discussion of end-user harms in their description of individual welfare-based normative perspectives of dark patterns [90]. For this paper, we focus on individual or end-user perspectives, of which Mathur et. al. identify four main types of problems: *Financial Loss, Invasion of Privacy, Cognitive Burden, and Individual Autonomy.*

The Consumer Reports Dark Patterns Tipline (jointly run by Stanford University) lists other harmful outcomes of dark patterns [125]. Intended as a consumer resource, the Tipline organizes dark patterns harms primarily by resultant end user experiences in layperson language – e.g., Individual Autonomy loss is described as "Denied Choice," and Cognitive Burden are presented as "Wasted Time" [125]. Some harms are described by feelings (Felt Shamed, Felt Tricked), losses (Lost Money, Lost Privacy), or actions (Forced Subscription), while other harms are aligned to things that happen to a user (Experienced Discrimination, Denied Choice) or specific situations (California Do Not Sell) [125].

2.1.2 Potential Harms in Dark Patterns Literature. We now examine how papers in our dataset identified harms and negative outcomes, classifying prior work within the Mathur et. al. [90] harms taxonomy. For this categorization, we did not only seek explicit mentions of 'harms,' 'damages,' or 'injuries,' but looked for broader descriptions of poor outcomes or problems and similarly do not use a narrow definition of harms in this section.

Loss of autonomy and control. Not unsurprisingly, many dark pattern papers consider loss of autonomy and decision-making capability in conjunction with other dark pattern harms. From the nature of dark patterns and how nudges operate on user choice, we did not notice any work that *failed* to recognize an autonomy cost of dark patterns. This is an interesting point of note for the individual welfare items from the Mathur et. al. [90] as follows and suggests that most, if not all, dark patterns may be considered as harmful to user decision-making. Whether this loss of autonomy constitutes legal recourse, or when, remains to be seen.

Financial harms. Dark patterns literature considers financial harms in two main categories: i) financial losses to the individual, and ii) anticompetitive harms. Luguri and Strahilevitz [83] found that dark user interfaces caused participants in their survey and experiment to accept costly service almost four times as often as the same interface without dark patterns. Mathur et. al. [90] discusses Zagal et. al., Conti et. al., and Lewis' [27, 80, 140] descriptions of dark patterns extracting additional money from users, as well as their own work on e-commerce dark patterns [89]. Participants in Bongard-Blanchy et. al. showed concerns over the influence of manipulative interfaces over their spending behavior and subsequent financial losses, and considered how users influenced by dark patterns might experience financial harms like debt or unreasonable spending [15]. In games, users additionally face potential financial losses, in particular when games prompt users to pay money for skipping locks or similar obstacles, or when being sold incomplete games [140]. Day & Stemler consider whether dark patterns constitute anti-competitive harms in the effort of extracting wealth from users [38]. [3]

Labor and cognitive burdens. Mathur et. al. [90] also identified cognitive burdens. The Nouwens et al. [96] user study, assessing the effect that consent banner design had on user choice, found that there was an approximate 22% of increase in acceptance when the opt-out option was hidden behind the initial first layer of the cookie banner and a user needed to take at least two clicks to opt out, affirming that labor costs impact users' privacy decisions. The Dark Patterns Tipline [125] describes this harm as "Wasted Time." In a similar theme, Zagal et. al. [140] describe gaming dark patterns as temporally-oriented and capable of 'cheating' users out of their time through things like 'grinding' or 'playing by appointment.' Gunawan et. al. consider effort and labor as a component of dark pattern harms for privacy-erosive outcomes [58, 84]. Users in Di-Geronimo et. al.'s study express concern over minors' cognitive development [43].

Emotional distress. Emotional distress, or otherwise negative emotional responses to dark pattern outcomes, can be considered as part of cognitive burdens, and is an area ripe for further investigation as to consider it as an autonomous category of harm. In this regard, Maier and Harr [88] reveal in the respondents answers awareness, annoyance and resignation, as their participants believed it impossible to avoid online manipulation, and acknowledged that the trade-off (free service) outweighs negative consequences. The Dark Patterns Tipline considers these under "Experienced Discrimination," "Felt Shamed," and "Felt Tricked" [125]. In games, Zagal et. al. consider social pressures and encouragement of anti-social behavior as potential outcomes of dark patterns [140]. Gak et. al. considered the distressing harms of persuasive logic in diet advertisements [50]. In Bongard-Blanchy et. al., participants worried about harms to physical and mental health, particularly for vulnerable individuals as a result of ill-formed decisions, and most prominently fretted over psychological and physical harms to themselves [15]. Mildner & Savino surveyed Facebook users to find cases of addiction and other mental health issues, citing procrastination and distraction as detrimental to their lives and contributing to their dissatisfaction with the platform [93].

Privacy harms. Mathur et. al. [90] identify '*Invasion of Privacy*' as a dark pattern harm, and describe how many dark patterns causing other harm types may also be problematic for user privacy.

[2] Even with this subset of early-stage work, we caution that our dataset represents a lower bound of academic, advocacy, or regulatory work mentioning dark patterns and their harms and note that a more comprehensive review should also consider work on nudges or persuasive technologies and their outcomes more broadly. We limit this dataset for the scope of this case study and paper.

[3] Anticompetitive perspectives of dark patterns echo concerns concerns regarding mechanisms of the attention economy [138], which dark patterns also exploit.

They note that privacy may be perceived through an individual welfarist lens, but may also be considered as "a public good, a human right, or an aspect of individual autonomy." Some authors directly link privacy to the autonomy-based definition as the 'right to be let alone' by considering 'decisional privacy' as the 'ability to make choices free of coercion,' with privacy being the 'right to be let alone' [38, 127, 136]. Bösch et. al. provides a privacy-specific dark patterns taxonomy corresponding to 'malicious dark strategies that harm privacy' underlying their designs [16]. These 'dark' strategies are juxtaposed against their privacy-preserving counterparts, Hoepman's privacy design strategies, which are intended to achieve the goal of improving privacy [68]; Bösch et. al. list the *Maximize, Publish, Centralize, Preserve, Obscure, Deny, Violate, Fake* dark strategies, then map these to specific dark patterns. In user studies, participants could be less aware of privacy harms resulting from dark patterns than of other harms, but the few who did, discussed cybersecurity threats and other harms to their privacy [15]; participants were also keenly aware and frustrated that they were being manipulated [15, 52].

As the focus of our paper warrants an expansion upon dark patterns as they relate to privacy in various contexts, we expand upon privacy dark patterns in greater detail in section 3.

3 DARK PATTERNS IN PRIVACY INTERACTIONS

In this section we further discuss dark patterns as applied in privacy-specific contexts, exploring how they relate to the potential privacy harms outlined in subsubsection 2.1.2. We then briefly consider how dark patterns are currently regulated in order to understand the limits and triumphs of existing regulations.

3.1 Privacy Contexts

Privacy user interactions provide an intriguing problem space. As compared to back-end privacy issues as with data breaches or leaked network traffic, users' immediate experiences of privacy largely have to do with controls – whether or not a service provides those controls can be a dark pattern, but dark patterns that often impede autonomy and decision-making are additionally nefarious within privacy interactions as they risk user data. We investigate the user experience contexts of user settings (as settings provide users some semblance of control), exit requests (as these represent formal privacy decisions users should be entitled to make), and consent interactions (which may also be perceived as entry requests, since most consent requests will appear when a user attempts to interact with a service for the first time). Following this, we explore how entry or consent interactions impact privacy in the exit and settings contexts and discuss how integral consent interactions are to overall privacy experiences.

3.1.1 Dark patterns in user settings. Gunawan et. al. and DiGeronimo et. al. notice dark patterns in website and app settings, primarily with certain controls preselected by default [43, 57]. Specifically, DiGeronimo et. al. observe "send usage data" as on by default for apps like Firefox and Reddit, and describe this dark pattern under an umbrella of 'privacy settings-related DPs' [43]. Gunawan et. al. separate this umbrella into patterns regarding additional labor for toggling settings, missing settings, or default settings that disadvantage user privacy [57].

3.1.2 Dark patterns in exit requests. We consider 'exit' requests to include logout, account deletion, Do Not Sell My Information options, and other opt-outs. Several measurement studies find such dark patterns in apps (as 'Not possible to logout or delete') [43], e-commerce websites (as 'Forced Enrollment' and 'Hard to Cancel') [89], and across web modalities (under a series of patterns increasing in friction from tricky to nonexistent exit options) [57]. The fact that these studies focused on different service types indicates that the same dark pattern might be deployed to serve multiple ends (for example, trapping a user within the shopping service while increasing the potential for additional privacy harms or tracking). This is affirmed by an early experiment [81] investigating account deletion interactions in social media sites across the different modalities to find cases where vendors do not offer the option or otherwise confuse the user. Such work highlights the difficulty of leaving an online service or removing one's data from a platform, which leaves consumers effectively trapped (as in a Roach Motel dark pattern) with little control over their personal data. Van Nortwick and Wilson [6] audit California Do Not Sell My Private Information requests for compliance to the CPRA [10], finding that websites can sometimes hide relevant links from users based on geographic region, often present DNSMPI links in potentially unclear and inconspicuous ways, reflecting the same behaviors used in consent regimes. Habib et. al. perform an empirical analysis of opt-outs for email subscriptions, targeted advertising, and data deletion [60] and continue this analysis in a user study [59]. In the user study, Habib et. al. note that the prevalence or existence of such user controls is often not enough to constitute a painless experience, and users continue to struggle with exercising effective autonomy over such exit interactions [59]. Relatedly, Sanchez-Rola et. al. [121] examine cookie controls in the wake of GDPR to find that provided controls are often illusory and do not eradicate privacy risk.

3.1.3 Dark patterns in 'entry' requests and consent interactions. Entry requests can include the following: common consent interactions, like initial consent to use a product or a service (typically seen in account registrations), individual consent requests for permissions within online services, and cookie consent banners presented when users first visit a website and are requested to consent to tracking technologies. Within dark patterns literature, several papers focus specifically on consent regimes, while most at least mention consent as an area of grave dark pattern concern. Gunawan et. al. group such patterns under an 'Initial Use' category [57].

Papers focusing primarily on consent mechanisms take a variety of perspectives, from finding Obstruction and Interface Interference patterns in a significant number of news outlet notices [126] to conducting rigorous A/B tests for influencing user consent decisions [96], to seeking out violations of the GDPR requirements [91]. Others take a holistic interaction criticism approach, inspecting cookie banners and categorizing dark patterns within the context of the entire cookie user flow [54]. These papers and others share glaring evidence that dark patterns in consent regimes 'substantially' influence user behavior [133]. Even studies examining 'bright' patterns see participants feeling the same level of control regardless of whether dark or 'bright' (privacy-forward nudge) patterns were applied to cookie consent requests, despite participants being swayed towards whichever option was nudged towards [55]. In other cases, comparative studies note that users can regret their cookie consent decisions after later being informed of data purposes that are provided in more robust (more-than-binary choice) banners [87].

3.2 How (Privacy) Dark Patterns are Currently Regulated

EU laws. Within the EU, the incoming Digital Single Act [110] bans dark patterns prohibiting online platforms to design, organise or operate their interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs users' free and informed decisions (Article 23a(1)). It bans particularly nagging, false hierarchy, and obstruction. It can be further complemented with GDPR and with the Unfair Commercial Practices Directive. However, criteria to quantify the magnitude of dark patterns and its threshold is absent. Notably, harms and criteria for its quantification are also absent thereof. The European Data Protection Board (EDPB) recently issued Draft Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces [46]. It identifies dark patterns during the life cycle of a social media account and analysed the applicability of GDPR principles regarding the processing of personal data in such settings. It defined that language, UI and UX are factors exploited by dark patterns. It does not recognize that platforms may use different amounts and combinations of various dark pattern categories that can cause harms. The EDPB could further provide a scale of severity of harms regarding the dark patterns presented in the guidelines [117].

The European Data Protection Supervisor [45] acknowledges that many digital service providers are deploying dark patterns to manipulate or deceive consumers into "consenting" to the new contractual terms, and considers this practice is of equal concern for the effectiveness of consumer and data protection law in the EU. The French Data Protection Authority [24], in its report "Shaping Choices in the Digital World", proposes a non-exhaustive typology of potentially deceptive design practices which have a direct impact on data protection. It classifies these practices into four categories from a data protection perspective for which different design tactics can be implemented: enjoy / seduce / lure / complicate / ban. They summarize this classification in a graphical way [24]. In the report, the DPA states that some of these practices may comply with the GDPR but, depending on the time, manner and data in question, they can raise ethical issues and even be non-compliant.

Despite this monumental progress in regulating UX, language and manipulative UIs, the law still does not provide users with avenues for seeking remedy (nor does it provide users outside of California with legal requirements for how they experience online consent). Prohibitive regulations are a step in the right direction, but do not help data subjects that are targets of dark patterns after harms are incurred.

US laws. Though this work primarily uses the GDPR model for analysis, we highlight American regulatory efforts to acknowledge international methods for dark patterns regulation.

In California, dark patterns are explicitly prohibited in concrete under the CCPA, as they pertain to consent interactions – namely through the acknowledgment that "agreement obtained through the use of dark patterns does not constitute consent" [9]. Some dark patterns scholars look to this provision as an example of future regulatory models for dark patterns [75], however others are more critical of its potential [72]. Other proposed federal regulations like the American Data Privacy and Protection Act (ADPPA) [108] and Deceptive Experiences To Online Users Reduction (DETOUR) Act [135] aim to prohibit deceptive designs.

4 GDPR REMEDIES

We next analyse how the GDPR approaches damages. We explore how the GDPR might present a model for provisioning remedies for end users, then visit the civil law mechanisms provided for redress, and lastly inspect the administrative law penalties framework.

4.1 GDPR as a model for remedies

Potential infringements of legal requirements, once materialized, trigger the GDPR's redress mechanisms. The EU data protection law provides for a remedies model to explore dark pattern harms for various reasons.

(1) The GDPR provides a *two-tier remedies system*, with both civil and administrative law mechanisms. This practically means that legal infringements and dark pattern harms can be remedied with judicial remedies in civil law courts and administrative proceedings alongside with the supervisory public authorities (also named data protection authorities or DPAs). While the two redress mechanisms require different conditions to be met, as explained in the following sub-sections, the two-tier system provides a comprehensive approach towards remedying legal violations and harms.
(2) The GDPR remedies system has the potential to have a deterrent effect due to the severity of penalties [95].
(3) The GDPR introduces a collective redress option via its Art. 80, which gives the possibility to Member States of the EU to allow consumer or other organisations to start actions on behalf of data subjects. Those collective actions do not require a specific mandate from individuals. This is particularly useful for the cases of dark patterns, that individuals are largely unaware of they are being targeted, manipulated or otherwise harmed by those practices.
(4) The GDPR remedies model introduces a strict ('no fault') liability, therefore any organization involved in unlawful processing is responsible for that processing without the need to prove negligence nor willful conduct or fault [7, 115, 141] suffices that the data subject can prove a breach of the regulation has occurred on the part of the controller or processor, and that this breach has resulted in eligible damages [23].

4.2 The civil courts redress mechanism

The GDPR, in Article 82(1) – which is directly applicable in all EU member states, provides the **right to redress and obtain compensation** for any person who has suffered material or non-material damage as a result of the controller's infringement of the GDPR.

The GDPR notes that the processing of personal data may cause risks for the rights and freedoms of a person, as illustrated by Recital 75 [115] and indicates the potential for **material or non-material**

damage. *Material damages* may consist of financial losses, can occur, e.g. if the data subject becomes the victim of identity theft or fraud due to a GDPR infringement. *Non-material* can comprise personal disadvantages, such as discrimination or damage to reputation (see Recital 85) [115], and depend on the impact on the data subject in the individual case. This compensation is **conditional** to: i) an organization's infringement of the GDPR, and to ii) a causal link between that infringement and the damage a person suffered. Thus, the standard causal requirement applies: damages suffered *as a result of infringements* are covered by Article 82 [115]. A data subject is hence responsible for demonstrating that the breach in question is relevant for, or has caused, the harm suffered [23]. Lastly, the concept of damage should be broadly interpreted, in the light of the case-law of the Court of Justice (CJEU), and Recital 146 of the GDPR which notes that damages should be **compensated in full** [115].

4.2.1 *Threshold assessment.*

The *Court of Justice of the EU (CJEU)* requires that damage need to be *actual and certain* to assure compensation [113]. Member State courts are ultimately responsible for awarding redress to the persons that suffered damages [131], according to the the principle of procedural autonomy.

Material damages in terms of Article 82 could be awarded relatively easily due to the strict liability conditions and cover financial loss. The question however relies on *how to determine non-material damages.*

Methodology for national court case selection and review. The analysis of how national courts assessed non-material damage followed the *de minimis* or materiality threshold approach of damage, developed within the jurisprudence of German courts regarding compensation for non-material harms [106]. It means that trivial immaterial harms do not always lead to compensation, but only when data subject's rights have been severely infringed. Thus, violations that only constitute an *"individually perceived inconvenience"* would not entitle a data subject to compensation [62, 100] This threshold enabled to distinguish two approaches in our analysis: i) decisions that are below a *de minimis* threshold, ii) decisions that require a *de minimis* or evidentiary threshold. We consulted a non-exhaustive list of national court decisions from the public repository GDPRhub [4], a database provided by the European Center for Digital Rights (NOYB) that is a repository of GDPR-related decisions across Europe with direct links to the official decisions of national courts. We analysed court decisions from courts of Germany, The Netherlands, Austria and the UK related to Article 82 of the GDPR until the 15th March 2022. Table 2 depicts the elicited cases.

Year	Case Number	Court or Case Name
2017	C-337/15 P	European Ombudsman v. Claire Staelen [113]
2018	8 C 130/18	Local Court Diez [100]
2019	17 O 178/18	Regional Court Wuppertal [139]
	7560515 CV EXPL 19-4611	Administrative District Court Amsterdam [98]
	AK-18-2047	Administrative District Court Overijssel [107]
	6 Ob 217	Austrian Supreme Court [29]
	Az.:4U-U-760/19	Higher Regional Court of Dresden [101]
	65 C 485/18	Local Court Bochum [99]
	34 O 13123/19	Regional Court Munich [105]
2020	1 Ca 538/19	Lübeck Labor Court [36]
	9 Ca 6557/18	Düsseldorf Labor Court [31]
	C/18/189406/HA ZA 19-6	Northern Netherlands Court [111]
	13 Ca 1046/20	Dresden Labor Court [30]
	13 C 160/19	Pforzheim Local Court [37]
	13 O 244/19	Darmstadt Regional Court [32]
	2 Sa 358/20	Cologne Regional Labor Court [34]
	28 O 71/20	Cologne Regional Labor Court [35]
	9 O 145/19	Regional Court Lüneburg [85]
	201905087/1/A2	RaadVanState Uitspraak [132]
	324 S 9/19	Hamburg Regional Court [33]
	385 C 155/19 (70)	AG Frankfurt/Main [48]
	1 R 182/19b	Higher Regional Court Innsbruck [102]
	13 Ca 1046/20	Dresden Labor Court [30]
	9 O 145/19	Regional Court Lüneburg [85]
2021	C-687/21	Higher Regional Court Dresden [61]
	6 Ob 35/21x	Supreme Court Austria [104]
	31 O 16606/20	District Court Munich I [70]
2022	9436020 CV EXPL 21-30289	Court of Rotterdam [109]
	13 O 129/21	Regional Court of Hannover [63]
	3 O 17493/20	Regional Court of Munich [106]

Table 2: National court case decisions cited in this paper (N=31).

Below a *de minimis* threshold. For the majority of the analysed court decisions, a mere violation of GDPR requirements could, in principle, give rise to immaterial damage worthy of compensation, since such infringement triggers liability on its own right [97]and hence, no serious infringement is required. As such, it is irrelevant whether a loss of personal data has reached a certain level of materiality (Recital 146). According to this approach, no proven actual damage is required [31, 36]. The reasons sustaining this position refer in general that *all* damage must be compensated and the concept of damage must – in accordance with the objectives of the GDPR – be broadly interpreted (Recital 146). Courts add that the mere fact that the damage cannot be specified precisely and may be relatively small in scope cannot constitute grounds for rejecting any claim thereto [111]. From the case law analysis conducted for this paper, we identify several examples of infringements that awarded non-material damages in subsection 8.2.

The fact however that the infringements in the cases studied for this paper did not lead to awarding damages does not mean with certainty that other courts would not award damages for the above infringements. On the contrary, due to the highly contextual nature of the conditions to determine when an individual has suffered material or immaterial damages, other courts in the future might relate similar types of infringements to awarding damages.

***De Minimis* threshold: proof of damage.** National courts that upheld this positioning rule that not every GDPR infringement leads to redress, solely as punitive damages or prevention of further

[4] https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub

data protection violations: infringements require a certain level of materiality, significance or severity [23, 42] of damage that has actually occurred (either financially or psychologically through distress). These courts acknowledge GDPR infringements, though additionally require: i) a significant and noticeable social or personal disadvantage or deterrent effect that impair personality-related matters [102] ; and ii) the data subject must prove that damages occurred, and not the company; the mere assertion that a person allegedly suffered damage as a result of a GDPR violation is not sufficient [29].

Accordingly, mere fears of such disadvantages regarding infringements (e.g. due to an unauthorized disclosure of personal data) [33], or the perceived uneasy feeling (e.g. that one's personal data could be used by third parties without authorization as a result of a data breach) without serious impairment are not considered sufficient for a claim under Art. 82 GDPR [48]. From the case law analysis conducted for this paper, we provide some examples of infringements that required such evidentiary damage threshold: personal data breach [48], deletion of a video shared in a social network [101], receipt of spam email [100], misdirected email [99], unlawful processing [105], unlawful processing of sensitive personal data relating to political opinion [102], accidental disclosure of bank account record to third party [35], and unlawful transfer of the data subject IP address to Google LLC repeatedly [106].

The national court of Innsbruck [102] held that the data subject must substantiate the damage and additionally prove the *intensity* of the disadvantage in life and the impairment of personality rights suffered from unlawful data processing. In the recent and known UK case of Lloyd v Google LLC, the Supreme Court rejected a collective claim for damages for loss of control of data where4 million Apple iPhone users were affected by Google's alleged unauthorized collection of Safari browser information. The court reasoned that *damages for data privacy infringements require a "damage" in terms of "material damage (such as financial loss) or mental distress distinct from, and caused by, unlawful processing of personal data in contravention of the, and not to such unlawful processing itself"* [112].

4.3 The supervisory authorities penalties framework

The second tier mechanism prescribed is the administrative law redress, providing fines as a remedy for GDPR infringements.

Investigation powers of supervisory authorities. Supervisory authorities (DPAs), which are independent administrative authorities of each Member State, have the power to carry out investigations in forms of data protection audits (Art. 58(1)(b) GDPR) and obtain access to all personal data and necessary information to perform the audit (Art. 58(1)(e)), including accessing the premises of entities processing personal data in their territory of competence. In case of an identified violation, DPAs can impose a ban on processing, but also administrative fines (Art. 58(2)(i)). The administrative procedure may be initiated either by a complaint of an individual (art. 77 GDPR), for example when targeted by a dark pattern practice. But most importantly, the procedure may also be started ex officio [22], without a complaint.

DPA penalties on consent-related dark patterns. Several decisions relate to consent-related dark patterns and herein we provide an overview thereof. In 2019, the French DPA found that Google did not provide clarity to the users in terms of the description of personal data collection, purposes, and that the information provided by the company 'did not allow users to sufficiently understand the particular consequences of the processing for them' [39]. The regulator found that the identified problems as regards clarity and transparency of information also had an impact on the validity of the consent collected to process users' personal data for personalized advertising. In 2021, the French DPA imposed on Google another fine (of 150 million euros) [3] since it offered a button to immediately consent to tracking cookies, but did not allow to refuse consent as easily, since several clicks are necessary to refuse all cookies, violating the GDPR freely given and unambiguous consent requirement. This practice related to the dark pattern of obstruction and sneaking [51]. In 2021, Google was again fined [26] by the same DPA, since when a user deactivated the purpose of ad personalization on Google Search, an advertising cookie was still stored on his or her computer and kept reading information for the serve it is bound to. This practice violated the unambiguous consent requirement. It related to the dark pattern of sneaking and obstruction. In 2021, Amazon was fined [] for its unlawful consent practices, violating a freely given and informed consent. The fact that there was no satisfactory information about the purposes of cookies and the means to reject them relates to the dark patterns of hidden information and sneaking. In 2022, the French DPA fined Facebook [5] as does not allow users to refuse consent as easily as to accept them, violating the freely given and unambiguous consent; additionally, it misinformed users on how to refuse consent, violating an informed consent requirement. Such practices configure the dark patterns of obstruction, sneaking and hidden information. In 2022, the Belgian DPA decision [11] holds that the Interactive Advertising Bureau Europe's Transparency & Consent Framework (IAB TCF), a consent industry standard, failed to provide consent-related transparent practices that were previously addressed as dark patterns in related research [96, 123]. The Belgian DPA imposed recently two fines on Belgium press websites [5] for using cookies on its websites without complying with consent requirements. They violated the prior, informed, unambiguous and revocable consent requirements. The related dark patterns that can be identified from the decision are obstruction, sneaking, preselection and hidden information.

The cases overview show that supervisory authorities are onto identifying and remedying dark pattern wrongdoings.

Fines calculation model. The GDPR in its Article 83 provides a list of mitigating and aggravating factors for the decision of supervisory authority to impose an administrative fine for an infringement, and for the determination of the amount of the fine. Factors include nature, gravity and duration of the infringement, the intentional or negligent character, previous infringements from the same entity (data controller). On the basis of those factors, some supervisory authorities have adopted calculation method models. The Dutch Data Protection Authority for example provides four categories of violations and corresponding fines [130].

[5] https://www.autoriteprotectiondonnees.be/citoyen/enquete-cookies-sur-les-sites-de-presse-le-groupe-rossel-mis-a-lamende;https://www.autoriteprotectiondonnees.be/citoyen/enquete-cookies-sur-les-sites-de-presse-roularta-mis-a-lamende

5 CASE STUDY ON CONSENT DARK PATTERNS

In this section we inspect consent requests as a case study for determining consent dark patterns.

In section 3 we highlighted the main interaction contexts where dark patterns impact privacy wherein consent is regarded within 'entry' interactions. Problems in entry requests lead to further issues if dark patterns are found in the settings or exit contexts. Addressing dark patterns at the point of user entry to a product or service offers the greatest potential for stronger consumer and privacy protections, and entry interactions are a primary opportunity for dark patterns redress. King & Stephen also inspect consent as a case study for broadly regulating dark patterns [75], though we deviate from their work by examining the GDPR consent requirements and by narrowing our scope to investigating damages. Since an existing and growing subset of dark patterns literature focuses on cookies, consent, and such 'entry' contexts as shown in Table 1, we find consent to be a useful case study.

Consent as a legal basis for processing personal data. Consent in the GDPR consists of the legal grounds for processing personal data (Article 6(1)) [115] and, according to the French DPA, is an instrument for users to protect their rights [24].

Legal requirements for consent request. *Consent* is defined in Article 4(11) and complemented by Articles 6 and 7 of the GDPR which state that for consent to be valid, it must satisfy the following seven requirements: it must be prior to any data collection, freely given (without any pressure, coercion, detriment), given to specific purposes, informed, unambiguous (univocal and balanced choices), must be readable and accessible, and finally, revocable at any time [44, 103, 122]. Thus, the *main* legal requirements for providing consent for processing of personal data are free/freely given (R1), specific (R2), informed (R3), unambiguous (R4), provided in further detail in subsection 8.1.

Infringements to consent requirements. Dark patterns have immense potential to violate the EU data protection law, both the General Data Protection Regulation and the Privacy and Electronic Communications Directive [1] (ePrivacy Directive) in multifold manners. Leiser has explained that companies nudge users toward satisfying the legal conditions required to process personal data, such as for example providing their consent [79]. Studies have shown that one way to achieve this is by "placing controls or information below the first layer', and these practices "renders it effectively ignored" [4, 54, 73, 91, 96]. However, it is rather questionable whether those practices would truly satisfy the requirements of an unambiguous and freely given consent [14, 24, 39, 122].

Consent Dark Patterns Following our literature review of consent dark patterns in section 3, we turn to the widely used classification of dark patterns categories from Gray et. al. [53]: obstruction, sneaking, interface interference, and forced action.[6] We explore patterns within each category, articulate examples of that pattern as applied to consent interactions, and map the patterns to the GDPR consent requirements they potentially violate in Table 3. From this mapping, we denote that the existence of several and common practices that recurrently appear in consent requests [40, 54, 91, 92, 122, 124, 133] constitute violations to legal requirements for consent. Herewith, consent is often not freely given and ambiguous, which results to violation of the conditions for lawful ground for processing (Art. 6(1) GDPR), when the collection of data is based on consent.

Summary. The violation of the requirements for valid consent constitutes an infringement of the GDPR, which triggers the remedies system. Data subject can thus resort to redress at the respective courts due to the liability regime for data controllers and processors.

6 DISCUSSION

We now examine redress within the breadth of our collected dark pattern harms, GDPR damages court cases, and case study, and discuss implications for modeling dark pattern remedies.

6.1 Current State of Consent Damage Claims

From the surveyed national court decisions we did not encounter so far damage claims regarding consent infringements; this suggests an underutilization of dark pattern redress potential, as in section 5 we denote that several recurrent practices concerning consent requests embedding dark patterns cause direct GDPR infringements.

Regarding the materiality of certain consent related infringements damages, though concrete dark pattern practices need to be evaluated in a case by case basis, it has been established that when consent requests present unlawfully preselected options for processing personal data purposes, or when the user interface design offers the option "accept all" purposes at the very first layer of the banner, consequently, the personal data (or very sensitive categories of data) of the user will be shared *by default* with all the potential third-party advertisers that the website operates with [123, 137]. Regarding severity, dark patterns literature noted in section 2.1.2 identifies several harms in consent related studies. For example, Nouwens et al. [96] and Utz et al. [133] reports labor and cognitive harms; Grassl et al. [55] refer to privacy harms; Kulyk et al. [76] report negative emotional responses to unlawful consent requests; Machuletz et al. [87] mention that users end up regretting their privacy choices when they know they have better options. We find the non-existence of damage claims in case law to be concerning when considering the materiality of damages and potential severity of dark pattern harms. Further scholarship is needed to explore this disparity.

6.2 On the Matter of Assessing Damages

Lack of standardized criteria for assessment of damages. None of the existing applied thresholds from the consulted cases resides on harmonised measurable benchmarks or metrics or calculation methods. Some authors [23] assert an explicit connection between the determination of fines from Article 83(2)(a) (nature, gravity, duration of the infringement, level of damage suffered) and damage assessment itself and question whether the assessment factors in Article 83(2) most closely related to harmful act be seen as relevant for a damages assessment according to Article 82. The author argued the GDPR contains no indication that inspiration can be drawn in this way, but at the same time the flexibility of Article

[6] While *Nagging* is one of the main categories in the Gray [53] taxonomy and scholars [69] do link nagging to privacy harms, this link is often considered as an indirect harm. A consent-based nag could be seen as improperly registered consent by a CMS, or disregard of a user's privacy-forward choices, in which the consent banner constantly appears until desirable choices are opted for.

Category [53]	Dark Pattern	Examples in Consent Requests	Consent Requirements Violated
Obstruction	Obstruction	Information Overload	Readable; Freely given; Accessible
	Roach Motel	Consent interaction introducing considerably more friction for options other than "acceptance"	Revocable; Unambiguous
Sneaking	Sneaking (General)	Consent is assumed through the provision of fine print	Freely given
	Bait and Switch	Closing a consent interaction or cookie banner with an ’X’ assumes consent	Unambiguous; Freely given
Interface Interference	Hidden Information	Demphasized or missing “configure” button”	Specific; Freely given
	Preselection & Default Settings	Preselection of “Accept all” purposes in the settings menu	Unambiguous
	Toying with Emotion	Use of emotionally-driven colors for accept or reject buttons, e.g. red for reject and green for accept	Unambiguous; Freely given
	False Hierarchy	A box with a bigger “OK” button and small “Configure” button gives hierarchy to “OK”	Unambiguous
	Trick Questions or Manipulation through Framing	Cute, goading language, e.g. "Can I have a cookie?”; Phrases like "we care about your privacy" to dissuade users from viewing fine-tune options	Freely given
	Aesthetic Manipulation	Custom options are greyed-out buttons or in-line text links, giving the user the false impression that the option is disabled.	Unambiguous
Forced Action	Forced Action (General)	Tracking-walls or cookie-walls hold content hostage	Freely given
	Privacy Zuckering	Multiple, separate data collection purposes are presented as one	Specific; Freely given

Table 3: Our mapping of dark patterns to their potential deployment in consent interactions, which expands upon Fig. 7 in [54] and is organized by the Gray et. al. [53] categories.

82 does not argue against it either. Notably, in a Düsseldorf court case [31] the court ruled that the amount of damage could be determined on the basis of the criteria of Article 83(2) GDPR, which are otherwise used to calculate fines. In this case, the court specifically considered the financial strength and high degree of culpability of the company, the significance of the infringed right and the severity of the violation. As regards appropriate threshold for damages, there are unsettled questions [82]. The case law analysis showed that national courts of EU Member States currently use different thresholds for assessing damages: either requiring a *de minimis* threshold (severity of damages), or below it. While the case law reviewed for this paper is not exhaustive of all possible GDPR-related in all Member States, the study of selected cases already gives an indication of the application of different thresholds for damages in national courts.

Recently, the matter was referred to the Court of Justice EU for a preliminary ruling by the Supreme Court of Austria (Oberster Gerichtshof) [61, 104, 120]. The Austrian Court asked the CJEU whether a person must have suffered harm to be awarded redress or if it is sufficient that provisions of the GDPR have been infringed. The request for a preliminary ruling also asked the Court about the de minimis threshold, and whether the "the award of compensation for non-material damage presupposes the existence of a consequence of the infringement of at least some weight that goes beyond the upset caused by that infringement" [61, 104, 120].

International Requirements for Damages. In the U.S. State of California, § 1798.150 of the California Consumer Privacy Act of 2018 (Title 1.8.5 of the California Civil Code) provides for a private cause of action to a consumer who has suffered a data breach, permitting recovery of damages of between $100 and $750, or "actual damages, whichever is greater" (see §1798.150.(a)(1)(A)) [9]. While this paper focuses on the GDPR in scope, further scholarship following King & Stephan's work [75] is needed to investigate how other users might find redress, for those to whom the GDPR does not apply. Such work on dark pattern damages may provide better guidance for developing effective thresholds and measurements.

Legal Requirements for Non-Material Harms. While some scholars have discussed nonmaterial dark pattern harms, like Hung on nagging [69] and [50] on emotional distress, much work remains to be done in exploring how these might be addressed. Beyond financial and privacy spaces, users are at risk of dark patterns that cost their time, attention, cognitive load, and opportunities. Measurements of such harms in addition to a critical examination of existing harms thresholds in the law may bridge the gap of understanding how users might find dark pattern remedies. More research is needed to directly correlate non-material harms to damages in order to build effective models of redress.

6.3 Potential for Improving Remedies

Providing Evidentiary Value to Damage Claims. Given the opacity surrounding dark pattern practices, a remedial mechanism based on the investigative powers of DPAs, which is not dependent on prior knowledge and awareness of the malpractices by the targeted individual, removes a considerable barrier towards access to remedies. Even though the actions from data supervisory authorities are not directly linked to awarding compensation to data subjects, those administrative proceedings could have *evidentiary value* in civil courts proceedings, if those are initiated by data subjects that suffered damages from dark patterns.

Alternative Remedies. This paper provides a cursory exploration into how dark patterns might trigger redress. However, deceptive designs might be mitigated in other ways, as already seen in the CCPA's explicit prohibition of dark patterns [9]. While redress may warrant additional research, so do other potential mitigations that could more rapidly address dark patterns than attempts to match dark pattern harms to significant thresholds. For example, perceiving websites (and the designs contained therein) as contract [65] might provide opportunities to address dark pattern damages from other areas of law.

7 CONCLUSION

Dark patterns are a way for companies to "ruthlessly nudge consumers to disregard their privacy and to provide more personal data than necessary", as the previous European Data Protection Supervisor has stated [20]. The EDPS warned that the boundaries between nudging and 'recklessly taking advantage of natural human traits' are blurry. The literature review in this paper showed indeed that users are certainly subject to harms, when exposed to dark pattern practices, especially in relation to consent interactions. The GDPR was examined and assessed as a model for redress. The doctrinal analysis of the legal requirements for consent and the two-tier remedies model of civil law courts redress and supervisory authority penalties, showed that it has the potential to offer redress to users who suffered damages from dark pattern practices. The legal requirements for valid consent are violated by the use of the various dark pattern techniques. The violation of conditions for valid consent constitutes an infringement of the GDPR, which triggers the remedies system. Individuals may seek redress and damages in civil courts, with relatively low burden, since there is a strict (no fault) liability regime for data controllers, though the problem of rational apathy remains – data subjects don't want to litigate because a procedure is expensive, while damages are low.

However, the full potential of the GDPR remedies system is not realised due to some limitations in the way courts of national EU Member States interpret and apply Art. 82 GDPR. Specifically, the analysis of the selected case law revealed that courts apply different thresholds and lack harmonised calculation methods. In terms of thresholds, some courts tend to not award damages for what they call below *de minimis* threshold cases, e.g. when the damage caused was too trivial and insignificant. Some others courts look beyond such a *de minimis* threshold, and award damages considering only the severity of distress or other materialised harm as a condition for awarding damages, but mostly as a condition for the calculation of those damages. Such discrepancy between the approaches adopted by national courts hampers the full potential of the remedies system of the GDPR, contrary to the spirit of Recital 11 of the GDPR (effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects [115], as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States). The issue of a *de minimis* threshold is currently pending at the CJEU and will be hopefully clarified.

In conclusion, users might access a remedy for harms caused by dark patterns, on the conditions that those are concretely linked to the prescribed legal requirements e.g. for consent as explored in the case study and that the harms constitute damages. However, a dark pattern might be deployed to serve multiple ends, and may cause harm to an individual in multiple ways. This cumulative negative harmful effect of dark patterns is not properly addressed by the GDPR. Further, the case law analysis demonstrated that there are implementation difficulties regarding evidentiary issues and calculation methods for awarding damages. Last but not least, further research should be conducted on calculation methods and metrics for awarding material and non-material damages for dark pattern harms across the various harm types. Similarly, further work should explore regulatory models beyond the GDPR to better understand the nature of dark pattern harms.

ACKNOWLEDGMENTS

The research for this paper is partially funded by the Horizon Europe ENCRYPT project (Grant Agreement nr. 1010706), RENFORCE, Google ASPIRE award, and an NSF SaTC Frontiers grant (#1955227).

REFERENCES

[1] 2009. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC.
[2] 2020. California Privacy Rights Act of 2020 (CCPA).

[3] 2021. Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED. https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf.

[4] 2022. Automating Cookie Consent and GDPR Violation Detection. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA. https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger

[5] 2022. Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED. https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf.

[6] 2022. Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA? *Proceedings on Privacy Enhancing Technologies* (2022). https://doi.org/10.2478/popets-2022-0030

[7] A.B.Cordeiro. 2019. Civil liability for processing of personal data in the GDPR. *European Data Protection Law Review* 5 (2019). Issue 492.

[8] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[9] California Consumer Privacy Act. 2020. California Consumer Privacy Act (Final Text of Proposed Regulations). https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf

[10] California Privacy Rights Act. 2020. California Privacy Rights Act. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[11] APD2022 2022. Decision on the merits 21/2022 of 2 February 2022? Complaint relating to Transparency & Consent Framework. https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf

[12] Beth Bell and Daniel Fitton. 2021. Dark Patterns in Mobile Games: A Source of Online Risk for Youths? *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1Y5hbXyc1QAwaSSICcj8NJWG8eLgBv2zo/view

[13] Sorin Berbece. 2019. 'Let There Be Light!' Dark Patterns Under the Lens of the EU Legal Framework. (2019). http://dx.doi.org/10.2139/ssrn.3472316

[14] European Data Protection Board. 2020. Guidelines 05/2020 on consent under Regulation 2016/679. (2020).

[15] Kerstin Bongard-Blanchy, Ariana Rossi, Salvador Rivas, Sophie Doublet, Vincent Koening, and Gabriele Lenzini. 2021. "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*. http://doi.org/10.1145/3461778.3462086

[16] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proc. of PETS* 2016, 4 (2016), 237–254. https://content.sciendo.com/view/journals/popets/2016/4/article-p237.xml

[17] Harry Brignull. 2010. Dark Patterns. https://www.darkpatterns.org/.

[18] Bringing Dark Patterns to Light: An FTC Workshop 2021. https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop

[19] Chris Brown and Chris Parnin. 2021. Dark Patterns for Influencing Developer Behavior. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/18IvdlVvViukCW8xvBEdcGSqiXvBfdh3w/view

[20] G. Butarelli. 2019. Speech on Dark Patterns, Legal Design Roundtable. https://edps.europa.eu/sites/edp/files/publication/19-04-27_dark_patterns_en.pdf

[21] Daniel Capurro. 2021. Dark Patterns, Electronic Medical Records, and the Opioid Epidemic. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1Cf-EXPJhd7_2ZGT0utmTN0JgXuvAFg58/view

[22] Federica Casarosa. 2020. Transnational collective actions for cross-border data protection violations. *Internet Policy Review* 9 (2020). Issue 3. https://doi.org/10.14763/2020.3.1498

[23] Johanna Chamberlain and Jane Reichel. 2019. The relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation. *Mississippi Law Journal* 667 (2019). https://www.mississippilawjournal.org/journal-content/the-relationship-between-damages-and-administrative-fines-in-the-eu-general-data-protection-regulation/

[24] Regis Chatellier, Geoffrey Delcroix, Estelle Hary, and Camille Girard-Chanudet. 2019. Shaping Choices in the Digital World.

[25] Rohit Chopra. 2020. Statement of Commisioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc.

[26] CNIL. 2020. Délibération de la formation restreinte no SAN-2020-012 du 7 décembre 2020 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED . https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706.

[27] Gregory Conti and Edward Sobiesk. 2010. Malicious Interface Design: Exploiting the User. In *Proc. of WWW*.

[28] Forbrukerrådet (Norwegian Consumer Council). 2018. Deceived By Design. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[29] Austrian Supreme Court. 2019. 6 Ob 217.

[30] Dresden Labor Court. 2020. 13 Ca 1046/20.

[31] Düsseldorf Labor Court. 2020. 9 Ca 6557/18.

[32] Darmstadt Regional Court. 2020. 13 O 244/19.

[33] Hamburg Regional Court. 2020. 324 S 9/19.

[34] LG Cologne (Cologne Regional Labor Court). 2020. 2 Sa 358/20.

[35] LG Cologne (Cologne Regional Labor Court). 2020. 28 O 71/20.

[36] Lübeck Labor Court. 2020. 1 Ca 538/19.

[37] Pforzheim Local Court. 2020. 13 C 160/19.

[38] Gregory Day and Abbey Stemler. 2019. Are Dark Patterns Anticompetitive? *Alabama Law Review, Forthcoming* (2019). http://dx.doi.org/10.2139/ssrn.3468321

[39] Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority). 2019. Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. (2019). https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf

[40] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, F. Schaub, and T. Holz. 2019. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *ArXiv* abs/1808.05096 (2019).

[41] Maarten Denoo, Bruno Dupont, Eva Grosemans, and Bieke Zaman. 2021. Dark design patterns and simulated gambling in videogames: Embracing a broader context-sensitivity in an environment of expected use. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1i88sq_vOTuBG2kI4bg5eqqj7xQaVMffc/view

[42] Gabel Detlev, Markus Langen, Sylvia Lorenz, and Dominik Stier. 2021. Compensating non-material damages based on Article 82 GDPR – is there a de minimis threshold? (2021). https://www.whitecase.com/publications/alert/compensating-non-material-damages-based-article-82-gdpr-there-de-minimis

[43] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *Proc. of CHI*.

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

[45] EDPS. 2018. EDPS Opinion 8/2018 on the legislative package "A New Deal for Consumers". https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf

[46] European Data Protection Board. 2022. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0 Adopted on 14 March 2022. https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

[47] Madison Fansher, Shruthi Sai Chivukula, and Colin M. Gray. 2018. #darkpatterns: UX Practitioner Conversations About Ethical Design. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3188553

[48] AG Frankfurt/Main. 2020. 385 C 155/19 (70).

[49] Brett M. Frischmann. 2021. Nudging Humans. *Social Epistemology: A Journal of Knowledge, Culture and Policy* (2021). http://dx.doi.org/10.2139/ssrn.3440791

[50] Liza Gak, Seyi Olojo, and Niloufar Salehi. 2021. The Distressing Ads That Persist: Uncovering The Persuasive Logics and Emotional Harms of User Targeted Diet Ads. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1AETDbMWpWlzPJQtYKPT2oMzWekjNGxzN/view

[51] Colin M. Gray. 2019. The dark side of UX Design. https://darkpatterns.uxp2.com/.

[52] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. 2021. End User Accounts of Dark Patterns as Felt Manipulation. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct 2021), 372:1–372:25. https://doi.org/10.1145/3479516

[53] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proc. of CHI*.

[54] 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 *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 172, 18 pages. https://doi.org/10.1145/3411764.3445779

[55] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. 2021. Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research* 3, 1 (Feb. 2021), 1–38. https://doi.org/10.33621/jdsr.v3i1.54

Number: 1.

[56] Saul Greenberg, Sebastian Boring, Jo Vermeulen, and Jakub Dostal. 2014. Dark Patterns in Proxemic Interactions: A Critical Perspective. In *Proc. of the Designing Interactive Systems Conference.*

[57] Johanna Gunawan, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Mobile and Web Modalities. (Oct. 2021).

[58] Johanna Gunawan, Dave Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. Towards an Understanding of Dark Pattern Privacy Harms. https://drive.google.com/file/d/1Myh4mL6ul9e4bKkmPccwIHFNlpPHx_8-/view

[59] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proc. of CHI.*

[60] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Proc. of the Workshop on Usable Security.*

[61] AG Hagen. 2021. C-687/21 – Saturn Electro.

[62] Magistrate Court Hannover. 2020. 531 C 10952/19, BeckRS 2019.

[63] Regional Court Hannover. 2022. 13 O 129/21.

[64] Rikard Harr and Annakarin Nyberg. 2021. "It depends upon whether it's true or not:" Entrepreneurs' Perspective on Dark Design Patterns. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1mhBtxWCoMcyTZ8X5LN5SDdhFsVAEAYse/view

[65] Woodrow Hartzog. 2011. Website Design as Contract. *American University Law Review* 60, 1635 (2011). https://ssrn.com/abstract=1808108

[66] Woodrow Hartzog. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies.* Harvard University Press.

[67] Philip Hausner and Michael Gertz. 2021. Dark Patterns in the Interaction with Cookie Banners. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1lIIbR93bXYMbV19bs-jpxTMN6oozYxXa/view

[68] Jaap-Henk Hoepman. 2012. Privacy Design Strategies. (2012). https://cs.ru.nl/~jhh/publications/pdp.pdf

[69] Alison Hung. 2021. Keeping Consumers in the Dark: Addressing 'Nagging' Concerns and Injury. *Columbia Law Review* 121, 8 (2021). http://dx.doi.org/10.2139/ssrn.3803936

[70] District Court Munich I. 2021. 31 O 16606/20.

[71] Luisa Jarovsky. 2022. Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness. (2022). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4048582

[72] Margot Kaminski, Jacob Snow, Felix Wu, and Justin Hughes. 2020. Symposium: The California Consumer Privacy Act. *Loyola of Los Angeles Law Review* 54 (2020). Issue 1.

[73] Georgios Kampanos and Siamak F. Shahandashti. 2021. Accept All: The Landscape of Cookie Banners in Greece and the UK. In *ICT Systems Security and Privacy Protection*, Audun Jøsang, Lynn Futcher, and Janne Hagen (Eds.). Springer International Publishing, Cham, 213–227.

[74] Thejus Kayadanath and Haig Armen. 2021. Dark Patterns in Ubiquitous Computing. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1Ib_YhVrXa7bc17489G0qnJdJw1LMCOBg/view

[75] Jennifer King and Adriana Stephan. 2021. Regulating Privacy Dark Patterns in Practice - Drawing Inspiration from the California Privacy Rights Act. *Georgetown Law Technology Review* 5 (2021). Issue 250.

[76] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. "This website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC).* https://doi.org/10.14722/eurousec.2018.23012

[77] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler. 2020. *The EU General Data Protection Regulation (GDPR): A Commentary.*

[78] Cherie Lacey and Catherine Caudwell. 2019. Cuteness as a 'Dark Pattern' in Home Robots. In *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI).* 374–381. https://doi.org/10.1109/HRI.2019.8673274

[79] M.R. Leiser and M. Caruana. 2022. *Journal of European Consumer and Market Law* 10 (2022). Issue 6.

[80] Chris Lewis. 2014. *Irresistable Apps: Motivation Design Patterns for Apps, Games, and Web-based Communities.* Apress.

[81] Neha Lingareddy, Brennan Schaffner, and Marshini Chetty. 2021. Can I Delete My Account? Dark Patterns in Account Deletion on Social Media. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://www.google.com/url?q=https://drive.google.com/file/d/190uWk2bhJngE0J_K_kGt2v91z_f01Ocz/view?usp%3Dsharing&sa=D&source=editors&ust=1619579203736000&usg=AFQjCNHhFRvNyZ0NrYr7AVXUqAKvIKd-tQ

[82] Mona Naomi Lintvedt. 2021. Putting a price on data protection infringement. *International Data Privacy Law* (12 2021). https://doi.org/10.1093/idpl/ipab024 arXiv:https://academic.oup.com/idpl/advance-article-pdf/doi/10.1093/idpl/ipab024/41537497/ipab024.pdf ipab024.

[83] Jamie B. Luguri and L. Strahilevitz. 2019. Shining a Light on Dark Patterns. *Behavioral & Experimental Economics eJournal* (2019).

[84] Kai Lukoff, Alexis Hiniker, Colin M. Gray, Arunesh Mathur, and Shruthi Sai Chivukula. 2021. *What Can CHI Do About Dark Patterns?* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411763.3441360

[85] LG Lüneburg. 2020. 9 O 145/19.

[86] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. 2020. Towards the Identification of Dark Patterns: An Analysis Based on End-User Reactions. In *IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction* (Online, India) *(IndiaHCI 2020).* Association for Computing Machinery, New York, NY, USA, 24–33. https://doi.org/10.1145/3429290.3429293

[87] Dominique Machuletz and Rainer Böhme. 2020. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 481–498. https://doi.org/doi:10.2478/popets-2020-0037

[88] Maximilian Maier and Rikard Harr. 2020. Dark Design Patterns : An End-user Perspective. *Human Technology* 16 (2020), 170–199.

[89] Arunesh Mathur, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (2019).

[90] Arunesh Mathur, Jonathan Mayer, and Kihir Kshirsagar. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. https://arxiv.org/pdf/2101.04843.pdf

[91] Celestin 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. In *Proc. of IEEE Symposium on Security and Privacy.*

[92] Celestin Matte, Cristiana Santos, and Nataliia Bielova. 2020. Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?. In *Proc. of Annual Privacy Forum.*

[93] Thomas Mildner and Gian-Luca Savino. 2021. *Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411763.3451659

[94] Thomas Mildner and Gian-Luca Savino. 2021. How Social are Social Media: The Dark Patterns in Facebook's Interface. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/184v2Amr2camaw2EKceQlCkht0m-r7gyY/view

[95] Paul Nemitz. 2019. *Fines under the GDPR.* Hart Publishing. http://dx.doi.org/10.5040/9781509926237.ch-010

[96] 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 *Proc. of CHI.*

[97] Eoin O'Dell. 2017. Compensation for Breach of the General Data Protection Regulation. *Dublin University Law Journal* 40, 1 (2017), 97–164.

[98] Administrative District Court of Amsterdam. 2019. 7560515 CV EXPL 19-4611. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6490

[99] Local Court of Bochum. 2019. 65 C 485/18.

[100] Local Court of Diez. 2018. 8 C 130/18.

[101] Higher Regional Court of Dresden. 2019. Az.:4U-U-760/19.

[102] OLG Innsbruck (Higher Regional Court of Innsbruck). 2020. 1 R 182/19b.

[103] European Court of Justice. 2017. Case C-673/17 Verbraucherzentrale Bundesverband v.Planet49. http://curia.europa.eu/juris/document/document.jsf;?&docid=218462&doclang=EN&cid=8679428

[104] Supreme Court of Justice (Oberster Gerichtshof – 'OGH') of the Republic of Austria. 2021. 6 Ob 35/21x.

[105] Regional Court of Munich. 2019. 34 O 13123/19.

[106] Regional Court of Munich. 2022. 3 O 17493/20.

[107] Administrative District Court of Overijssel. 2019. AK-18-2047.

[108] United States House of Representatives. 2022. American Data Protection and Privacy Act. https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-1178152ih.pdf

[109] Court of Rotterdam. 2022. 9436020 CV EXPL 21-30289.

[110] Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act). 2022. COM(2020) 825 final.

[111] Administrative District Court of the Northern Netherlands. 2020. C/18/189406/HA ZA 19-6.

[112] Supreme Court of the United Kingdom. 2021. Lloyd v. Google LLC. (2021). https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf

[113] Case C-337/15 P. 2017. European Ombudsman v Claire Staelen.

[114] Harshvardhan J. Pandit, Brian Lynch, and Dave Lewis. 2021. Crowdsourcing Issues Across Domains for Automated Generation of Legal Complaints Regarding Consent. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/17J-wFd94Tqx1xGt3JP98ILS3MCQ0axXD/view

[115] European Parliament and Council of European Union. 2016. EU General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[116] Article 29 Data Protection Working Party. 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies. WorkingDocument02/2013providingguidanceonobtainingconsentforcookies

[117] Collaborative public comments by DECEPTICON Project members and collaborators. 2022. Feedback to the Guidelines 3/2022 on "Dark patterns in social media platform interfaces: How to recognise and avoid them". https://edpb.europa.eu/system/files/2022-05/comments_to_edpb_guidelines_on_dark_patterns_for_social_media_-_decepticon_unilu_0.pdf

[118] Constanta Rosca, Bogdan Covrig, Catalina Goanta, Gerasimos Spanakis, and Gunes Acar. 2021. Digital monitoring of unlawful dark patterns. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1oNkPlhzWncTS2hu_waY_inS1dFfWmshD/view

[119] Arianna Rossi and Kerstin Bongard-Blanchy. 2021. All in one stroke? Intervention Spaces for Dark Patterns. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1aWCBFcOrPLjRlp1PvYINl3nWDA9GD5Hb/view

[120] LG Saarbrücken. 2021. Case 5 O 151/19.

[121] 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 *Proc. of AsiaCCS*.

[122] 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), 91–135. https://doi.org/10.26116/techreg.2020.009

[123] Cristiana Santos, Midas Nouwens, Michal Tóth, Nataliia Bielova, and Vincent Roca. 2021. Consent Management Platforms under the GDPR: processors and/or controllers?. In *APF*.

[124] Cristiana Santos, Arianna Rossi, Lorena Sanchez Chamorro, Kerstin Bongard-Blanchy, and Ruba Abu-Salma. 2021. Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (Virtual Event, Republic of Korea) *(WPES '21)*. Association for Computing Machinery, New York, NY, USA, 187–194. https://doi.org/10.1145/3463676.3485611

[125] Stanford Digital Civil Society. 2021. Dark Patterns Tip Line. https://darkpatternstipline.org

[126] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. *Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3419249.3420132

[127] Daniel J. Solove. 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review. 154 (2006). Issue 3. https://ssrn.com/abstract=667622

[128] Mohammed Tahaei and Kami Vaniea. 2021. Code-Level Dark Patterns: Exploring Ad Networks' Misleading Code Samples with Negative Consequences for Users. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://drive.google.com/file/d/1r1UYAiKwtwEa5d0gKRLl75s31bfE5mZS/view

[129] Arnout Terpstra, Paul Graßl, and Hanna Schraffenberger. 2021. Think before you click: how reflective patterns contribute to privacy. *Position Papers of CHI'22 "What Can CHI Do About Dark Patterns?"* (2021). https://www.google.com/url?q=https://drive.google.com/file/d/1YOJVY3vgSxO5LYyv99FExhaIZcVJrHBI/view?usp%3Dsharing&sa=D&source=editors&ust=1619579203739000&usg=AFQjCNGXu-V5xmrf5eJyRy_0IADbv3zCsw

[130] Authoriteit Persoonsgegevens (the Dutch Data Protection Authority). 2019. AP adjusts fine policy rules. (2019).

[131] Sanna Toropainen. 2019. The Expanding Right to Damages in the Case Law of CJEU. *Maastricht Faculty of Law Working paper 2019-03* (2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3449194

[132] RaadVanState Uitspraak. 2020. 201905087/1/A2. https://gdprhub.eu/index.php?title=RvS_-_201905087/1/A2

[133] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proc. of CCS*.

[134] Ari Ezra Waldman. 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology* 31 (Feb. 2020), 105–109.

[135] Mark R. Warner. 2019. Deceptive Experiences To Online Users Reduction (DETOUR) Act. https://www.congress.gov/bill/116th-congress/senate-bill/1084/text

[136] Samuel D. Warren and Louis D. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4 (1890). Issue 5.

[137] Vera Wesselkamp, Imane Fouad, Cristiana Santos, Yanis Boussad, Nataliia Bielova, and Arnaud Legout. 2021. In-Depth Technical and Legal Analysis of Tracking on Health Related Websites with ERNIE Extension. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (Virtual Event, Republic of Korea) *(WPES '21)*. Association for Computing Machinery, New York, NY, USA, 151–166. https://doi.org/10.1145/3463676.3485603

[138] Tim Wu. 2019. Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal* 82 (2019). Issue 771. https://scholarship.law.columbia.edu/faculty_scholarship/2029

[139] Regional Court Wuppertal. 2019. 17 O 178/18.

[140] Jose P. Zagal, Staffan Bjork, and Chris Lewis. 2013. Dark Patterns in the Design of Games. In *Proc. of Foundations of Digital Games Conference (FDG '13)*.

[141] Gabriela Zanfir-Fortuna. 2020. *Article 82 Right to compensation and liability.*

8 APPENDICES

Document Type	Prior Work
Taxonomies and Framing	*Terpstra et. al [129] *Rossi & Bongard-Blanchy [119] *Bell & Fitton [12] *Brown & Parnin [19] *Denoo et. al [41]
Measurement Work	*Gunawan et. al. [58] *Lingareddy et. al. [81] *Tahaei et. al. [128] *Mildner & Savino [94] ***Hausner & Mertz** [67] *Capurro [21] *Gak [50]
User Studies	*Harr & Nyberg [64] *Kayanadath & Armen [74]
Multi-Method Work	***Pandit et. al.** [114]
Policy and Regulatory Literature	*Rosca et. al. [118]

Table 4: Additional documents inspected for this work. These documents include short workshop papers or unpublished, in-progress, and early-stage work.

8.1 Legal Requirements for Consent Descriptions

(R1) Freely given entails that the individual, whose data will be processed (data subject), has a genuine choice and does not feel compelled to consent, because not consenting would mean endurance of negative consequences for example. Balance of powers plays an important role in assessing whether consent if freely given, and in specific the risk of risk of deception, intimidation, or coercion [14].
(R2) Specific means that the data subject is consenting to the processing of their own data for a specific purpose. If a data controller wants to process the data for different purposes, they must provide separate opt-in choice, one for each purpose [14].
(R3) Informed consent aims at ensuring that individuals are informed of the elements necessary to make a choice, and that is prior to the processing starts taking place [77, 115].
(R4) Unambiguous means that consent must be given through an active behavior of the user through which she indicates acceptance or refusal to certain processing purposes. Such active behaviors can consist of: *"clicking on a link, or a button, box, image or other content on the entry webpage, or by any other active behavior from which a website operator can unambiguously conclude it means consent"* [116]. Accordingly, silence, pre-selected boxes or inactivity should not therefore constitute consent and violate such unambiguous requirement [103].

8.2 Examples of Infringements Awarding Non-Material Damages

- unauthorized disclosure of health data [30]
- insufficient and delayed provision of information under the data subject access request [31]
- unauthorized third-party access to the subject's personal data (customer data) due to a cyber attack [70]
- unauthorized disclosure of very sensitive health data [37]
- accidentally disclosing candidate data to another applicant (wherein it was alleged loss of control over personal data) [32]
- unlawful publication of an employee photo [36]
- failure to remove professional CV from website after the end of employment [34]
- unlawful disclosure of personal data [98]
- freedom of information request shared with other public authorities without document anonymization, wherein the data subject claimed the claimant had suffered anxiety and stress [107]
- unlawful disclosure of personal data through a Facebook message, wherein the data subject claimed fear and stress due to the loss of control of personal data [111]
- disclosing an Excel list in an email with sensitive personal data [109]
- unlawful storage of a negative credit entry [63]
- unauthorized report to credit reference agency [85]