A Comparative Study of Dark Patterns Across Mobile and Web Modalities

JOHANNA GUNAWAN, Northeastern University, USA
AMOGH PRADEEP, Northeastern University, USA
DAVID CHOFFNES, Northeastern University, USA
WOODROW HARTZOG, Northeastern University, USA
CHRISTO WILSON, Northeastern University, USA

Dark patterns are user interface elements that can influence a person's behavior against their intentions or best interests. Prior work identified these patterns in websites and mobile apps, but little is known about how the design of platforms might impact dark pattern manifestations and related human vulnerabilities. In this paper, we conduct a comparative study of mobile application, mobile browser, and web browser versions of 105 popular services to investigate variations in dark patterns across modalities. We perform manual tests, identify dark patterns in each service, and examine how they persist or differ by modality. Our findings show that while services can employ some dark patterns equally across modalities, many dark patterns vary between platforms, and that these differences saddle people with inconsistent experiences of autonomy, privacy, and control. We conclude by discussing broader implications for policymakers and practitioners, and provide suggestions for furthering dark patterns research.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; • **Social and professional topics** → **Consumer products policy**.

Additional Key Words and Phrases: Dark Patterns; Consumer Protection; Deceptive Content; Nudging; Manipulation; UX Design

ACM Reference Format:
Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Mobile and Web Modalities. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 377 (October 2021), 29 pages. https://doi.org/10.1145/3479521

1 INTRODUCTION

Dark patterns are user interface (UI) elements that can influence a person's behavior against their intentions or best interests. Since designer Harry Brignull introduced the term [8], thriving online communities have emerged that catalog real-world examples of dark patterns and shame the services that employ them [14, 23, 32]. Lawmakers and regulators are also beginning to take notice [17], demanding that prominent tech executives answer for user interfaces that are criticized as deceptive [28, 51], and considering legislation that bans dark patterns [27, 55, 59].[1]

[1]We note that these proposals to regulate dark patterns may be a bit premature, given that the precise definition of "dark patterns" is not yet settled, as are the underlying harms and contextual boundaries that justify regulation.

Authors' addresses: Johanna Gunawan, Northeastern University, Boston, MA, USA, gunawan.jo@northeastern.edu; Amogh Pradeep, Northeastern University, Boston, MA, USA, amoghbl1@ccs.neu.edu; David Choffnes, Northeastern University, Boston, MA, USA, choffnes@ccs.neu.edu; Woodrow Hartzog, Northeastern University, Boston, MA, USA, w.hartzog@northeastern.edu; Christo Wilson, Northeastern University, Boston, MA, USA, cbw@ccs.neu.edu.

2573-0142/2021/10-ART377 $15.00
https://doi.org/10.1145/3479521

Recent work attempts to systematize our understanding of dark patterns in UI designs. Building on Brignull's original set of example dark patterns [8], researchers have developed taxonomies of dark patterns that are grounded in user studies [16], observations of practice by professional designers [33], and human cognitive biases [46]. Similarly, recent work has identified dark patterns in-the-wild to understand how, where, and at what prevalence they manifest. This includes studies that document dark patterns in privacy polices [2, 41], privacy notices [53, 58, 64], e-commerce websites [46], and popular mobile apps [20].

Although the literature on dark patterns has become increasingly rich, it still has an important gap: little is known about the relationship between technology platforms and dark patterns. For example, based on prior work, we know that dark patterns are present in websites and mobile apps [20, 46]. However, these studies were conducted in isolation and are not comparable—we do not know if dark patterns are more prevalent in one modality or the other, or whether the prevalence of specific types of patterns varies across modalities. These are critical questions, as they speak to the impact of platform *affordances* (e.g., mice vs. touch screens) [52], *capabilities* (e.g., location data APIs), and *design norms* (e.g., windowed vs. full-screen modal dialogs) on the adoption of dark patterns. Furthermore, these questions may speak to designers' intentions and peoples' cognitive vulnerabilities. Consider a case where a dark pattern could be implemented in a website and an app, but the developer deploys it only in the app: does this suggest that the developer views the mobile app as more important, i.e., worthy of investing the time to develop the manipulative interface, or does this suggest that people who use the app are more susceptible to the dark pattern than people who use the website? Or does this suggest neither, that perhaps the deployment choices stem from bugs, forgetfulness, or other everyday reasons?

To begin answering these questions, we conduct a comparative study of dark patterns across mobile app, mobile browser, and web browser-based versions of 105 popular online services. We manually curated a set of services like Facebook, Spotify, and Wish that offer a comparable level of functionality across all three modalities, manually interacted with them to generate video recordings of their user interfaces, and then manually labeled the recordings to identify instances of dark patterns. Our codebook included 50 individual patterns spread across nine thematic categories. One contribution of our work is that we identify 12 specific types of dark patterns that have not been documented in prior studies and place them within existing dark pattern taxonomies.[2]

Using this dataset we investigate the following questions:

- Within a given service, is the use of dark patterns consistent quantitatively (number of observed patterns) and qualitatively (types of observed patterns) across modalities?
- Across modalities, does the overall popularity of different types of dark patterns vary quantitatively and qualitatively?

Our findings show that dark pattern usage is highly inconsistent—for some patterns more dramatically than others—both for the same service and across modalities overall. For example, we find that mobile modalities contain the most dark patterns for 85% of the services we examine, but that differences between modalities vary greatly according to dark pattern count, type, and other traits. Lastly, we take preliminary steps towards understanding dark patterns when framed by features and capabilities across modality, service type, and themes of use. The raw coding data and source code used in this study can be found at `https://darkpatterns.ccs.neu.edu`.

Overview. We structure our study as follows. We begin in § 2 by discussing related work on dark patterns and contextualizing our study in relation to these studies. In § 3 we discuss how we built a corpus of services to test and our codebook of dark patterns, as well as our process for

[2]We describe these dark patterns in depth and provide examples in the Appendix, § 6.

labeling services using the codebook. We present the results of our analysis in § 4 and conclude in § 5 discussing broader implications for design practitioners, researchers, and policymakers, and provide suggestions for furthering dark patterns research.

2 BACKGROUND AND RELATED WORK

In this section, we survey the conceptual origins of dark patterns, discuss experimental and observational studies of dark patterns, and situate this study within the existing literature.

2.1 Design, Deception, and Darkness

Designers, psychologists, and behavioral economists have long interrogated how design orders human interactions. Don Norman popularized James Gibson's concept of *affordances* as a way of thinking about how the design of objects can communicate function to people in a way that makes usage plain and thereby simplifies interaction [52]. Thaler and Sunstein took these concepts a step further in their discussion of how intentionally designed *choice architectures* can *nudge* people into taking actions or making choices that are favored by the designer [62].

Although design paradigms like nudging have been criticized as paternalistic [50], the purpose of tools to nudge is ostensibly noble, i.e., to improve human well-being, either on the individual or group level. Examples include designing affordances that are accessible to people with varying levels of ability, or promoting public health outcomes by nudging people towards altruistic behaviors [62]. Adar et al. go a step farther, articulating cases where outright deception can be used benevolently in the service of user-centered design [1]. In short: user- and value-centered design is not necessarily incompatible with an "ends justify the means" design ethic.

Dark patterns are the antithesis of benevolent deception. In the context of websites and apps, Mathur et al. define dark patterns as "interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make." [46] Note the inversion with respect to benevolent deception: dark patterns benefit the designers' (or their bosses') goals and values, rather than promoting, or sometimes in spite of, the flourishing of users and society. Richard Thaler refers to dark patterns as "sludge" [61] since they weaponize peoples' mental heuristics and cognitive biases against them [7, 50, 66].

The neologism "dark patterns" was popularized by Harry Brignull, who maintains a crowdsourced website of examples [8]. Brignull also developed the first ad hoc taxonomy of dark patterns, which has since been critiqued, systematized, and expanded by academics [20, 33, 46]. Conti et al. also developed a taxonomy of malicious user interface designs in 2010, before the term "dark patterns" was widely used in academia [16]. Mathur et al. provide a through review of dark patterns literature across disciplines and organize it conceptually and thematically [47].

Building upon this body of theoretical conceptualization, we introduce the taxonomy of dark patterns that we use in this work in § 3.3. Throughout this work, we use the phrase "dark pattern" in isolation to refer to specific types of dark UI designs that have been documented in prior work (e.g., pop-ups nag dialogs, text that shames people [33], or pre-selected checkboxes in privacy settings [53, 58, 64]), rather than using it to refer to these design patterns in the abstract, categories of thematically similar design patterns, or taxonomies of dark patterns.

Dark patterns have profound consequences for user and societal wellbeing because they can influence user actions and perceptions [39]. For example, they can shape a user's understanding about the terms of engagement between user and service, or formal and informal agreements between users [38]. Dark patterns can convince users to share personal information when they ordinarily would not, possibly in ways that lead to regret and harm. Few legal rules constrain the use of dark patterns, which leaves users exposed and vulnerable to manipulation, wheedling, and fraud [39]. One possible reason the law has been slow to hold app and website designers accountable for dark patterns is the difficulty in conceptualizing when user interfaces are "dark," [47] the lack of data about how pervasive dark patterns are on the internet, and the nebulous and incremental nature of harm resulting from dark patterns. One of the aims of this study is to help mitigate these uncertainties.

2.2 Observation and Measurement

In tandem with the growth of theoretical insights around dark patterns there is growing interest in empirical studies of dark patterns. Academic studies have investigated dark patterns in real-world contexts, such as video games [67], proxemic interactions [35], visualizations [54], two-factor authentication schemes [65], and marketing email opt-outs [19]. Journalists and activists have also documented dark patterns being used by major online services like Google [6, 9], Facebook [15], Yelp [40], Match.com [24], and TurboTax [21].

Laboratory studies have begun to confirm that, unsurprisingly, dark patterns are effective at bending people towards choices that are not in their own interest. For example, Liguri et al. found that an extremely dark user interface caused participants in a survey and experiment to accept a useless, costly service almost four times as often as the same interface sans the dark patterns [45].

Two studies have examined the general public's conceptualization of dark patterns through the lens of online social communities that seek to document unethical designs. Fansher et al. focused on tweets containing the #darkpatterns hashtag, finding that it was often used by professional user experience (UX) practitioners to highlight dark designs they encountered in-the-wild [23]. Chivukula et al. performed a similar content analysis on threads from the highly active `/r/assholedesign` subreddit [14, 32]. Both studies observed remarkably similar behavior: these self-organized, self-selected communities uniformly opposed dark patterns in design, and they often attempted to shame offending service providers by sharing screenshots of dark UI designs.

In the following sections, we highlight empirical studies of dark patterns that are particularly relevant to the context of our study.

2.2.1 Privacy. There is a large body of journalistic and academic work that has examined how online services employ dark patterns to harm peoples' online privacy. As articulated by Ari Ezra Waldman, online platforms leverage dark patterns in this context to "manipulate us into keeping the data flowing, fueling an information-hungry business mode" [66], while simultaneously mollifying people through an illusion of informed choice. Bosch et al. developed a taxonomy of eight privacy dark strategies and presented case studies of them drawn from popular online services [7].

Privacy policies are one area where dark patterns have been found, although this literature largely predates the existence of the term. Observational studies of privacy policies have consistently found that they employ dark patterns like hiding hyperlinks to polices [41]; using unrealistically positive framing about privacy choices; exploiting time gaps between notice and choice [2]; or simply failing to disclose practices that have a material impact on peoples' privacy [44, 68]. Arguably, the dense, long, legalistic language used in many privacy policies is also "dark" in that it discourages people from reading and hinders understanding [22, 41].

Another well-studied application of dark patterns are online *privacy notices*, including *cookie consent notices* that have proliferated in response to privacy laws like the EU General Data Protection Regulation (GDPR). Privacy notices are ubiquitous across websites [18, 48] and mobile apps [60], and there is a strong incentive for service providers to nudge people to consent to extensive data collection and sharing. Several observational studies have measured the presentation and behavior of cookie consent notices on major websites and found that well over 50% contained dark patterns [53, 58, 64]. This includes setting tracking cookies in peoples' browsers before they have even been given an opportunity to consent to tracking [63]. Laboratory studies have confirmed that dark patterns have the desired effect in this context [5, 30, 64]. For example, Nouwens et al. asked participants to consent to data collection using notices drawn from popular websites, and found that dark patterns increased the percentage of participants who accepted tracking by 8–23% [53]. Interestingly, participants in a study by Kulyk et al. felt that the whole concept of cookie notices was a dark pattern [43]. Gray et al. unpack the dark patterns associated with consent notices using an interaction criticism approach [34].

A related area of concern are online behavioral advertising opt-out mechanisms. Habib et al. surveyed the data deletion and advertising opt-out functionality offered by 150 websites and argued that their usability was hindered by dark patterns [37]. As above, laboratory studies have bore these concerns out, finding that participants struggled to opt-out of advertising and marketing [29, 36].

2.2.2 E-commerce. Two studies specifically studied the use of dark patterns on e-commerce websites. Like privacy, this is another context where there are obvious motivations for merchants to leverage dark patterns to alter peoples' behavior, i.e., to maximize revenue. Moser et al. manually classified the content on 200 popular e-commerce and travel websites to look for features that encourage "impulse buying" [49] – a conceptual space that includes, but is not limited to, dark UI patterns. Mathur et al. dramatically scaled-up the search for dark patterns using a carefully crafted crawler combined with natural language processing, ultimately examining 11 K e-commerce websites [46]. Moser et al. observed dark patterns on roughly 14% of the websites they analyzed; Mathur et al. found dark patterns only on 11%, although they noted that the most popular websites (i.e., the ones examined by Moser et al.) more likely to include dark patterns. Furthermore, both studies documented many of the same specific dark design patterns, such as the use of countdown timers and indicators of customer interest to create a sense of urgency for shoppers.

2.2.3 Mobile Apps. As mobile devices become the dominant form-factor through which people access online services, the importance of studying dark patterns in mobile apps (as opposed to websites) grows. Di Geronimo et al. were the first engage this topic: they manually examined 240 of the most popular Android apps and found that 95% contained dark patterns, with an average of seven patterns per app [20].

2.2.4 Building On Prior Work. Prior work on dark patterns in privacy, e-commerce, and mobile app contexts has deeply informed our study in three ways. *First*, as we discuss in the § 3.3, the types of dark patterns identified in these studies informed our development of a dark pattern taxonomy that we use for coding in this study. *Second*, with respect to methods, we adopt the content analysis techniques used by Moser et al. and Di Geronimo et al. to identify dark patterns in real-world online services [46, 49] (see § 3). *Finally*, with respect to analysis, we compare our measurements of dark pattern prevalence to the baselines established by these prior studies in § 4.

2.3 Practitioners

There is a thread of academic discourse that seeks to understand the practical work of designers in order to unpack how (dark) UI designs are produced. Gray et al. observed UX design professional at work and found that ethical considerations were often overridden by practical matters such as legal compliance and a focus on serving clients' business needs (a situation that is likely exacerbated by the precarious, contract-oriented structure of freelance design work) [31]. Chivukula et al. performed a complementary series of structured design exercises with students and found that the framing of the design task (e.g., emphasizing the necessity of persuasion) steered the designers towards adopting darker designs [13]. The authors also observed the students using a variety of

Play Store Category	Number of Services	Services
Auto & Vehicles	2	Cars.com, Carvana
Beauty	5	Ulta, Sally Beauty, Sephora, Ipsy, Booksy
Books & Reference	5	Audible, *Dreame*, The Bible App, Webnovel, *Wattpad*
Business	4	Indeed Job Search, Jersey Mike's , LinkedIn, *USPS Mobile*
Comics	5	Webtoon, *Mangatoon*, Tappytoon, Tapas, *Comics/Comixology*
Communication	4	*Discord*, Yahoo Mail, Google Voice, BadBizz
Dating	6	Zoosk, *AsianDate*, UDates, Match Dating , Rondevo, OKCupid
Education	3	Duolingo, Google Classroom , PMP Exam Prep
Entertainment	4	*TubiTV*, Amazon Photos, *Twitch*, PlutoTV
Events	3	Ticketmaster, *GreetingsIsland*, SeatGeek
Food & Drink	5	DoorDash, Subway, Grubhub, Burger King, BeyondMenu
Games	2	*Roblox*, *ChessKid*
Health & Fitness	4	Calm, AllTrails, *Headspace*, MyFitnessPal
House & Home	5	Zillow, HomeAdvisor, Realtor.com, Redfin, Apartments.com
Lifestyle	4	Pinterest, *Tinder*, GreatClips, *Life360*
Maps & Navigation	1	*onX Offroad*
Medical	3	GoodRx, RxSaver, Leafly
Music & Audio	4	Spotify, YouTube Music, iHeartRadio, Audiomack
News & Magazines	5	NewsBreak, Twitter, Reddit, Quora, CBS News
Parenting	1	Pregnancy Tracker
Photography	2	Yogile, Amazon (Shopping)
Productivity	1	Outlook
Shopping	4	Wish, Amazon Prime Video, Wayfair, eBay
Social	6	*TikTok*, Kannada Matrimony, PlentyOfFish, Facebook, Instagram, MeetMe
Sports	5	*onX Hunt*, ESPN, OnGait, Gamechanger Scorekeeper, GolfNow
Tools	1	Google Translate
Travel & Local	6	VRBO , Tripline, Airbnb, Priceline, Expedia, Booking.com
Video & Editing	2	Youtube, Cartoon Network
Weather	3	The Weather Company/Channel, WeatherBug, AccuWeather

Table 1. The services in our corpus, organized by Play Store category. *Italicized* services are part of the 18 we labeled as partially equivalent features-wise during the coding procedure as described in § 3.3.

rationalization strategies to justify design decisions that were not user-centered, despite being educated in ethical design practices [11, 12].

Narayanan et al. hypothesize that an alternate pathway through which dark UI designs may be developed involve the misuse of *online behavioral experiments*, commonly known as *A/B tests*. In this theory, dark patterns are not intentionally engineered per se—they emerge organically through poorly designed and naïve experiments that iteratively converge towards exploitative designs [50]. Jiang et al. observed tens of thousands of websites leveraging in A/B testing in-the-wild, which provides a lower-bound estimate on the ubiquity of this practice [42].

Taken together, this body of work provides some explanation for how ethically-conscious designers can still produce unethical user interfaces. We further this discussion in this work by leveraging the body of artifacts produced by an online service as a lens through which to observe how different design teams working towards shared goals arrive at different, potentially dark UI implementations.

3 METHODOLOGY

In this study, we aim to investigate the relationship between technology platforms and dark patterns through the lens of modality: does dark pattern usage differ across the desktop web, mobile web, and mobile app versions of online services? Driven by this overarching question, we now discuss the methodology that we used for our study. This includes how we selected the corpus of 105 services that we focus on, how we developed our codebook of dark patterns, and how we interacted with and labeled the services. We present validation results for our labeling procedure before delving into analysis in the next section.

3.1 Preliminary Exploration

Before launching into formalized investigation of dark patterns, we first conducted an exploratory analysis. The purpose of this exploration was threefold: (1) to give us a sense for what kinds of online services might be amenable to our study, (2) to help inform our development of a codebook of dark patterns for use in labeling apps and websites, and (3) to assess approaches for investigating services that would be replicable, scalable, and likely to elicit a wide breadth of dark patterns.

We conducted our iterative exploratory analysis between September 2019 and June 2020. We manually investigated services that appeared in the Dark Patterns Hall of Shame on Twitter[3] and apps from the "Top Free" list in the Google Play Store. These sources were chosen to cover services that were known to employ dark patterns, as well as services that were popular overall. During each round of investigation the first author exercised the selected services, identified dark patterns, and then reported the methods and observations back to the group for discussion. The product of these discussions were iterative refinements to our approach for exercising apps and our working taxonomy of dark patterns.

We drew our initial set of dark patterns from prior work [7, 20, 33, 46] and expanded this over time by relying on Mathur et al.'s definition [46] to identify additional, previously undocumented patterns. Specifically, we looked for cases of coercion, steering, deception, and/or strategic omission that appeared to benefit the service at the expense of the human using the service. Note that we did not consider designer intent when identifying novel dark patterns—as noted by Di Geronimo et al., "[u]nderstanding designers' intentions and ethical decisions is subjective and may lead to imprecision" [20]. With respect to identifying dark patterns, we adopted Di Geronimo et al.'s stance of judging services solely by what was presented in the UI and whether the design privileged the service or the user, rather than attempting to infer whether designers had ill-intent.

3.2 Corpus Selection

The second step in our study was constructing a corpus of services that were amenable to our research goals. Specifically, we focused on online services that met the following criteria:

(1) The service must be popular, e.g., trending within the service's Google Play Store category;
(2) The service must be available through a desktop browser, mobile browser, and the Google Play Store;
(3) The service must offer roughly equivalent functionality across all three modalities;
(4) The service must be usable without a paid subscription, i.e., it is free or it provides a free trial without requiring a credit card during registration;
(5) The service must not require proof of identity beyond email or phone number verification.

Criteria (1) was motivated by our desire for impact, i.e., we choose to focus mainly on services that impact many people's lives. Additionally, the Play Store category element of criteria (1) was motivated by our desire to capture greater variety in service types. Criteria (2) and (3) derived from the requirements of our study: to compare dark patterns across modalities, a service must exist and offer similar functionality across the modalities.[4] Criteria (4) and (5) were necessary for practical reasons: we could not test a service that we could not reasonably gain access to.

To search for candidate services, we manually investigated the top fifteen free Android apps listed in App Annie's Top Charts[5] per Play Store category on June 15, 2020, for a total of 495

[3] https://twitter.com/darkpatterns
[4] Note that we restricted our study to Android apps because they are amenable to automated UI exploration in ways that iOS apps are not due to Apple's security restrictions. We plan to meld data from these automated methods with our data from manual testing in future work.
[5] https://www.appannie.com/

potential services across 33 categories.[6] We opted to search through each category instead of using the aggregate Top 200 most-popular list to ensure that we selected services across a breadth of different categories (e.g., e-commerce, social media, and games).

We did not fully investigate services in detail during this phase of the study; rather, we visited the relevant websites and Play Store pages for each potential service to determine if they would meet criteria (2–5). We filtered out popular services like Zoom, which at the time of our corpus selection failed criterion (2) as the desktop service was delivered through a desktop application, not a browser. We removed services like Netflix and Hulu that required credit card information to activate free trials, thus failing criterion (4). We filtered out some banking and health applications for failing criterion (5)—for example, MyChart by EPIC Systems required login information provided specifically by a person's healthcare provider. Ultimately we had to remove all services that we sampled from the Personalization, Libraries & Demo, and Finance categories from our corpus for failing our criteria.

After identifying 174 promising candidate services, we attempted to record screen-capture videos while interacting with each service on all three modalities (desktop website, mobile website, and mobile app; see § 3.4). During these in-depth examinations we discovered additional services that failed to meet our criteria and we filtered them out. To avoid disproportionate representation from any one category, we ultimately chose to retain at most five services from each remaining category.

Lastly, we added ten additional services to the corpus that we randomly selected from a joined and de-duplicated list composed of the Alexa Top-1M domains and app packages that were available on the Google Play Store as of August 14, 2020 [3]. We included these services to add diversity to our corpus with respect to service popularity. They bring the tally of services in our corpus to 118 total prior to the coding procedure.[7] Table 1 shows the services in our corpus.

3.3 Codebook Development

Before attempting to identify and label dark patterns in services, we required a codebook of dark patterns so that our manual labeling process would be as consistent as possible. To bootstrap our codebook and make our study comparable to existing dark patterns literature, we compiled specific examples of dark patterns from prior work. Given that Di Geronimo et al.'s [20] study of dark patterns in mobile apps from the Play Store was (1) most recent and (2) used a pattern library that was grounded in earlier work by Harry Brignull [8] and Gray et al. [33], we adopted their library of dark patterns as our starting point. We augmented it with additional patterns that they had excluded (e.g., gamification), as well as industry-specific patterns from Mathur et al. (e-commerce patterns) [46] and a variety of privacy-related studies [7, 41, 53, 58, 64].[8] Overall, our initial, synthesized codebook contained 37 distinct dark patterns.

During our preliminary examination of services (see § 3.1) we observed many examples of dark patterns that fell within existing general categorizations of dark patterns, but had not been specifically documented in prior work. In total, we added 12 novel dark patterns to our codebook, bringing the total number of patterns up to 50. These dark patterns are **bolded** in Table 2. We describe these dark patterns in detail and provide examples in the Appendix, § 6.

Table 2 lists the dark patterns in our codebook. To streamline our labeling process and facilitate later analysis, we categorized the dark patterns into nine *themes*. Some themes gather patterns based on the user actions that may elicit them, e.g., during *Initial Usage* of a new service, *Account*

[6]For simplicity, we count the Games parent category as one single category.
[7]As we describe in § 3.5, we discovered additional services from the corpus that failed to meet our criteria once we began detailed coding—this brought the final size of our corpus down to 105 services.
[8]Jensen et al.'s study of problematic privacy policy-related practices [41] predates the introduction of the term "dark patterns." That said, we argue that the problems they identify fit seamlessly among designs that would be considered "dark" today.

Thematic Category	Dark Pattern Description	Correspondence to Taxonomies from Prior Work	Privacy
Initial usage	Account is required to use service at all	Forced Action [33], Forced Registration [7], Forced Enrollment [46]	
	Cookie consent notice only allows "Accept" or "Close" without options to edit	Privacy Zuckering [7, 8, 33]	✓
Account Registration	**ToS/PP not mentioned during registration**	Privacy Zuckering [7, 8, 33]	
	If ToS/PP are mentioned, no visual cues that these are links	Privacy Zuckering [7, 8, 33], Hidden Information [7, 20, 33], Hidden Legalese [7]	✓
	If ToS/PP present, no consent checkbox is provided, i.e., agreement is implied	Privacy Zuckering [7, 8, 20, 33], Hidden Legalese [7], Preselection [20]	
	Consent notice for ToS/PP has a preselected opt-in checkbox	Preselection [20, 33], Hidden Legalese [7]	
	Consent notice includes email/SMS subscriptions with no opt-out	Preselection [33], Bad Defaults [7], Sneaking [33], Forced Registration [7]	
	Consent notice includes email/SMS subscriptions with a preselected opt-in checkbox	Preselection [20, 33], Bad Defaults [7]	
	Free trial with paid subscription required†	Forced Continuity [8, 33], Hidden Subscription [46], Forced Registration [7]	
	New accounts "follow" specific content producers by default	Sneaking [33]	
Monetization	Free and premium/app-only content are visually indistinguishable	Disguised Ads [8, 33], Bait & Switch [8, 33], Hidden Subscription [46]	
	Cannot sort or filter free from premium content	Aesthetic Manipulation [20, 33]	
	Native ads (including sponsored ads)	Disguised Ads [8, 20, 33]	
	Service uses fictional currency that is paid for with real money	Intermediate Currency [20, 33]	
	Ads that mimic UI of service	Disguised Ads [8, 20, 33]	
	Tiny close buttons/difficult to close ads	Aesthetic Manipulation [20, 33]	
	Moving/inconsistent close buttons on ads	Aesthetic Manipulation [20, 33]	
	Interact with ads to unlock content (w/ or w/o countdown timer on ad)	Forced Action [20, 33]	
	Pay to avoid ads	Hidden Costs [8, 33, 46], Nickel-and-Diming [32]	
Engagement	Gamification with achievement badges or per login/daily rewards	Gamification [33], Forced Action [20]	
	Service offers rewards with individual countdown timers	Toying with Emotion [20, 33], Countdown Timer [46]	
	Extraneous notification badges on features	Nagging [33], Aesthetic Manipulation [33]	
	Inboxes/message centers for services that don't primarily offer chat functions	Nagging [33]	
	Invite buddies or import contacts for rewards	Friend Spam [8], Social Pyramid [20, 33], Address Book Leeching [7]	
	Inviting buddies or importing contacts is or appears to be mandatory for use	Friend Spam [8], Social Pyramid [20, 33], Address Book Leeching [7]	
Shopping	No guest checkout possible, account registration required to make purchase	Roach Motel [8], Forced Action [20, 33], Forced Enrollment [46]	
	Items not chosen appear in basket	Sneak into Basket [8, 20, 33, 46]	
	Optional add-on items are preselected	Sneak into Basket [8, 20, 33, 46]	
	Opting out of add-on items results in shaming language	Confirmshaming [8], Toying with Emotion [33]	
	Item in basket differs from item added (e.g., in price, color, etc.)	Bait & Switch [8, 33]	
	Prices do not include taxes/fees/etc.until checkout	Hidden Costs [8, 33, 46]	
Location	Location permissions are required to use service	Forced Action [33], Bad Defaults [7], Privacy Zuckering [7]	
	Location permissions appear to be required, but are not	Nagging [33], Aesthetic Manipulation [33], Visual Interference [46], Privacy Zuckering [7]	
	Location sensed by default without asking consent (e.g., via IP address, etc.)	Privacy Zuckering [7, 8, 33]	
Settings	**No bulk options for settings**	Aesthetic Manipulation [33], Privacy Zuckering [7, 8]	
	No notification settings provided	Forced Action [33], Bad Defaults [7]	
	No privacy settings provided	Forced Action [33], Privacy Zuckering [7, 20], Bad Defaults [7]	
	Any Notification setting opted-in by default	Preselection [20, 33], Bad Defaults [7]	
	Any Privacy setting opted-in by default	Preselection [20, 33], Privacy Zuckering [7, 20], Bad Defaults [7]	
	Settings changes do not actually save	Bait & Switch [8, 33], Privacy Zuckering [7, 20]	
Leaving	No logout option if login was possible	Roach Motel [20, 33], Hard to Cancel [46], Immortal Accounts [7]	
	No account deletion option if account creation was possible	Roach Motel [20, 33], Hard to Cancel [46], Immortal Accounts [7]	
	Unclear deactivation/deletion options	Roach Motel [20, 33], Hard to Cancel [46], Immortal Accounts [7]	
	Account deletion options are time delayed	Forced Action [33], Hard to Cancel [46], Immortal Accounts [7], Roach Motel [20]	
General usage	Nags app use or installation	Nagging [20, 33], Forced Action [33]	
	General pop-up nags	Nagging [20, 33]	
	Provocative text to shame or guilt people into certain behavior	Confirmshaming [8], Toying with Emotion [20, 33]	
	Confusing text, like double negatives, or verbally confusing toggles	Trick Questions [8, 20, 33, 46]	
	Some options are given visual precedence over others, e.g., larger buttons	False Hierarchy [20, 33], Visual Interference [46]	
	Checkbox options are preselected	Preselection [20, 33], Bad Defaults [7]	

Table 2. The codebook of dark patterns we use to label websites and apps. **Bolded** dark patterns are novel pattern cases identified by the authors during our initial exploratory study; all other cases were drawn from prior work. We map the dark patterns in our codebook to categories of dark patterns developed by prior work. The "Privacy" column denotes dark patterns that have been previously identified in studies of privacy polices and privacy consent notices [41, 53, 58, 64]. The † on the "free trial" dark pattern denotes special cases where we could explore the primary features of services, but not some of their ancillary, paywalled features.

Registration, while *Shopping*, when changing *Settings*, or when *Leaving* a service. Other themes gather patterns that are related to a specific goal of the designer, such as the *Monetization* of a service or increasing *Engagement*. Dark patterns in the *Location* theme pertain specifically to location privacy. Lastly, the *General Usage* theme captures dark pattern types that are not tied to specific usage contexts or designer goals, and thus may be found throughout a UI. Table 2 also provides mappings from our dark pattern types to taxonomies and categorizations from prior work.

3.3.1 Service vs. Platform Settings. For the purposes of our study, we only investigated settings that were available within a service's interface, not device-wide, OS, or browser-level settings. We did this partly for fairness reasons, since the availability of platform-wide settings varies across modalities. But more importantly, we considered the availability of granular settings related to issues like notifications and privacy within a service to be more important than platform-level settings. For example, in Android and iOS a person may disable all notifications from an app in the OS, but this is a blunt instrument. In contrast, only the settings within an app can potentially provide granular control, allowing a person to enable desired types of notifications (e.g., shipping notifications from an e-commerce app) while disabling undesired notifications (e.g., unsolicited product recommendations). Similar logic applies to platform-level privacy settings: they typically block a narrow class of data collection (e.g., third-party cookies in web browsers), but leave other forms of data collection open. Only settings within a service can empower people with a full range of options concerning what data is collected about them.

Ultimately, we consider platform-level settings to be outside the scope of our study. That said, we recognize that there may be dark patterns present in the settings UI for platforms themselves, and that this may be a good target for future studies.

3.3.2 Limitations. One notable limitation that surfaces from our codebook concerns the "Forced Enrollment" pattern, specifically "free" trials that require payment information (e.g., a credit card) to activate. We argue that this is clearly a dark pattern—people could just as easily enter their payment information at the end of the trial period. Practically speaking, however, the presence of this pattern in a service impacts our ability to investigate it, given criteria (4) in § 3.2. If a service required us to provide payment information at the outset, we excluded it from our study for failing to meet inclusion criteria (4). We did include services in our study that put some or all content behind a free trial wall or paywall, so long as the primary features of the services were accessible to us without providing payment information up-front.

Another noteworthy limitation of our codebook concerns cookie consent notices. While we included a dark pattern related to the presentation of options in cookie consent notices, we did not include the absence of tracking/cookie notices as a dark pattern. In concurrence with prior work [53, 58, 64], we also saw cases where websites provide notices in browser modalities, but the notices were dark by offering no meaningful options beyond prompts like "Accept" or "Close". In contrast, we observed that apps largely avoided the problem of having notices with dark options, but they did so by providing no notice at all.

Whether we should consider the omission of tracking/cookie notices to be dark was a matter of considerable debate among the authors. On one hand, we considered other omissions related to privacy disclosure (e.g., not mentioning the privacy policy during account registration) as dark, so it seemed inconsistent to not label lack of tracking/cookie consent as dark. Further, it is reasonable to argue that people have a right to be notified about tracking that may impact their privacy (as regulators in Europe and California have done with the GDPR and CCPA). Indeed, prior work has found that people considered cookie consent banners to be a dark pattern [43]. On the other hand, cookie consent notices are typically not contextually relevant, i.e., they pop-up during unrelated activities, and are thus unexpected, whereas the dark patterns we included in our codebook were all contextually relevant. Additionally, the information contained in tracking/cookie notices is typically available to people in the service's privacy policy. For these reasons, we decided not to consider the omission of cookie consent notices to be dark, but we concede that other researchers may not agree with this decision.

3.4 Recording Methodology

The next step in our study was generating recordings of interactions with the 118 services in our corpus. We adopted the methodology used by Di Geronimo et al., i.e., our goal was to create a screen capture video of each service on each modality that we could later examine in detail for evidence of dark patterns [20]. In this section, we discuss how we maintained uniform testing and interaction procedures while generating these recordings.

3.4.1 Test Environment. For testing mobile websites and apps, we utilized two Google Pixel 3a smartphones running stock Android version 9. We equipped each phone with a valid and active SIM card to facilitate phone number-based account verification. To facilitate signing up for accounts with services, we created two new Google accounts with unique email addresses. Each Google account used the profile of an ungendered Jamie Doe born January 1, 1990. We used one phone for installing and testing mobile apps from the Play Store, and the other for testing the corresponding mobile websites in Chrome.[9] We uninstalled each app after testing it, and cleared all browsing history and data from Chrome after testing each mobile websites.

For testing desktop websites, we used an up-to-date Chrome browser in Guest Mode on a Surface Book 2 running Windows 10. Because Guest Mode for desktop does not store history or browser data by default, we did not need to manually clear browser data after each service. Instead, we closed the browser after testing each service, opened a new browser window for the next service, and logged into a Gmail tab for email verification purposes before opening the service's website.

We recorded mobile interactions using LetsView over Wi-Fi, and recorded desktop interactions using Windows GameBar.

3.4.2 Interacting with Services. To mimic a new user's experience with a service, we interacted with each service for approximately five to six minutes, then attempted the following tasks when possible in the service. *First*, we attempted to interact with a service for its intended use (e.g., playing music in Spotify, buying an item from Amazon) without creating an account or providing permissions.[10] *Second*, if the service supported account creation, we did so and continued attempting to exercise the service's intended functionality. *Third*, we visited the service's settings pages and attempted to modify options related to accounts, notifications, and user privacy. Examples of relevant options include opting-out of marketing communications and data collection for targeted advertising. *Fourth*, we attempted to delete or deactivate our account if the option was available, or sign out.

In addition to our general interaction "script" that we followed for every service, we followed more specialized scripts in specific scenarios. For shopping services, we completed as many purchase steps as possible short of finalizing check-out for a product or subscription, using both a guest account (if available) and a logged-in account. For chat and dating apps, we did not interact with other people as we considered this to be unethical. For account creation, we always used a basic profile of Jamie Doe, born January 1, 1990. If a service requested location information, we provided the 90210/Beverly Hills Zip Code. If additional information was required, we opted for less identifiable options (like "Prefer Not to Say" or "Other") if possible, and otherwise chose randomly from available options. If a service required a phone number for phone verification, we used the prepaid SIM card with a 424 (Beverly Hills) area code to match the profile's Zip Code. We processed single-ecosystem services using the same account that we created for that ecosystem's primary account. For example, for Amazon-owned services we first created an account on `amazon.com` then investigated services like Audible, Kindle, ComiXology, etc..

We tested one service at a time across all three modalities, attempting to perform the same flow of tasks across modalities wherever possible. We prioritized achieving interaction equivalence across modalities and adjusted interaction time in instances of slow network connectivity and similar situations, and do not find that recording time outliers impact dark pattern expression. All testing was performed by the first author to minimize variations in interaction across services and time. In total, producing recordings took over 30 hours.

We found that spending approximately five to six minutes interacting with each version of the services was sufficient to complete the scripts outlined above. With respect to realism, our scripts most closely resemble a curious person testing a service for the first time. With that in mind, our testing method has clear limitations: it cannot capture dark patterns that arise after repeated or

[9]We did not log in to our Google account from Chrome, to help mitigate concerns about the impact of third-party cross-domain tracking on the behavior of mobile websites.
[10]Note that many apps in our corpus require account creation, in which case we proceeded directly to the next step.

extended use of a service, nor does it fully emulate the experience of a person interacting with a service as an expert.

3.5 Coding Procedure

The final step in our methodology was labeling dark patterns in specific services by viewing our video recordings and applying our codebook. In keeping with prior work [20], we label dark patterns as present or not present in each (service, modality) pair, rather than counting the number of specific instantiations of each dark pattern. As we noted in § 3.3, we limited our dark pattern labels to UI designs and elements that (1) appeared in our codebook and (2) seemed to benefit the service over the user.

The initial labeling was performed independently by the first author of this paper. One service was labeled at a time, starting with the mobile app, then mobile website, and finally the desktop website. The researcher then inspected the labels for discrepancies across the three modalities and reviewed all three recordings for differences in user interaction that could have impacted dark pattern discovery, omitting dark pattern labels that could not be fairly judged. For example, if a dark pattern in the mobile website seemed dependent on a specific settings submenu, but the recording showed that the researcher did not open the corresponding submenu in the mobile app, then we did not label that dark pattern in any modality for that service in the interest of comparative fairness. In other words, for us to label a specific version of a given service as containing a specific dark pattern, all three of our recordings must have included footage of the researcher attempting to interact with the context in which that dark pattern was observed, taking into account whenever a modality's unique UI design or affordances could impact or limit the attempted interaction.

While reviewing the videos, we noticed that the recording software inconsistently captured visual touch feedback. When we observed potential dark patterns that relied on human interaction, like pop-up nags, but could not confidently determine whether the pop-up was triggered by researcher input or not, we did not label the pattern as dark to offer the service the benefit of the doubt.

During the labeling process, we found 13 additional services that were not equitably observable either due to recording failures, newly discovered inclusion criteria failures, or other reasons that prevented us from comparing the three modalities. We removed these services from our corpus, leaving us with 105 services for the remainder of our analysis. Among these 105 services we retained 18 that offered extra features in some modalities as long as the services' primary or core features were equivalently accessible and observable across all modalities. For these services, we noted their partial feature parity and where shared features ended.

3.5.1 Validation. To validate the labels produced by the first researchers, we asked a second researcher to independently label a subset of the services from our corpus. The second researcher was primed on dark patterns in general, and our codebook in particular, before labeling. We selected the top-ranked app from each category for secondary labeling plus two of the randomly selected apps, which accounts for 31 services (29% of the corpus). The second researcher labeled all three modalities of these 31 services. For the purpose of this validity testing, each researcher produced $31 * 3 * 50 = 4650$ binary labels, i.e., the presence or absence of each dark pattern in the codebook in each modality of 31 services.

The researchers respectively produced 634 and 601 positive labels, and 4016 and 4049 negative labels. The overall percentage agreement between the labels produced by our researchers was 90%, with the positive and negative agreements being 61% and 94%, respectively.[11] Thus, we observe that negative labels were more common overall (i.e., a dark pattern did not appear in a given context)

[11] The Cohen's κ measure of inter-annotator agreement between our researchers is 0.55. However, we caution that κ is difficult to interpret in situations with two labelers and binary labels [25, 26], so we do not emphasize this metric.

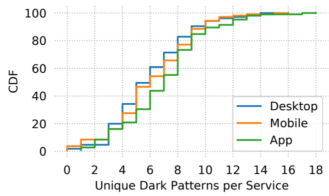

Fig. 1. CDF of unique dark patterns per service, broken down by modality.

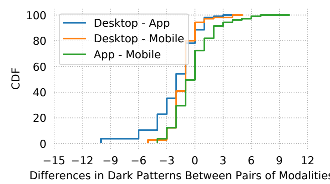

Fig. 2. CDF of the difference in unique dark patterns between two modalities for a given service. Zero indicates that both versions of the service had the same number of unique dark patterns.

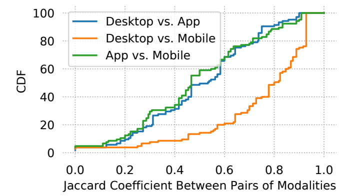

Fig. 3. CDF of the Jaccard coefficient between the set of unique dark patterns in two modalities for a given service. Zero means no overlap; one means complete overlap.

and that the researchers had greater agreement on these absences. Positive labels were rarer and had relatively less agreement. While these results demonstrate sufficient agreement overall to proceed, we return to the issue of identifying dark patterns in-the-wild in § 5.2.

4 ANALYSIS

In this section, we analyze the labeled dataset of dark patterns from the 105 services in our final corpus. We identified 2320 total instances of dark patterns across all services, with the per-modality breakdown being 834 patterns for the app modality, 756 for the mobile browser, and 730 for the desktop browser.

4.1 Differences Across Services

We begin by focusing on differences in dark pattern adoption across services. We analyze differences in dark pattern adoption overall, comparatively across modalities for each service, and differences with respect to app popularity.

4.1.1 Dark Pattern Adoption by Services. We begin with the raw counts of total unique dark patterns per service, per modality. Figure 1 shows the cumulative distributive function (CDF) by modality, where the x-axis denotes the number of unique dark patterns found per service, and y-axis denotes the percentage of the 105 services in our corpus that included exactly that number of unique dark patterns. Overall, we see that the trends for dark pattern adoption across modalities are similar. Based on Mann-Whitney U (MW U) and Kruskal-Wallis H (KW H) tests, we cannot reject the null hypotheses that these distributions are the same (all $p \geq 0.46$). Further, we observe that the median services in our corpus tend to have 7–8 dark patterns, while the "darkest" services include up-to 18 unique dark patterns, out of 50 possible patterns in our corpus. Every service in our corpus contained at least one dark pattern across its three modalities. This result aligns with work by Di Geronimo et al. [20], who reported that 95% of mobile apps in a corpus of 240 apps contained at least one dark pattern.

Despite the overall similarity of the distributions in Figure 1, it does give us our first hints of differences across the modalities. First, the app modality produced the longest tail, with apps like Match Dating and Wish containing 18 and 17 dark patterns respectively. Second, the service in our corpus with the fewest dark patterns overall (USPS Mobile) only contained one pattern in the app modality and none in the two browser modalities, which contributes to the browser modalities starting at 0.

Service	Uniq. DP
Wish	19
Match Dating	19
iHeartRadio	17
MeetMe	17
GoodRx	17
Dreame	17
MyFitnessPal	17
Webnovel	16
Duolingo	16
Facebook	16

Table 3. Top 10 services sorted by most unique dark patterns across modalities.

Service	Uniq. DP
USPS Mobile	1
Google Translate	4
OnGait	4
Burger King	4
Sally Beauty	5
Cartoon Network	5
Ticketmaster	5
Amazon (Shopping)	5
RxSaver	5
GreetingsIsland	6

Table 4. Top 10 services sorted by least unique dark patterns across modalities.

Service	D	M	A
Mangatoon	4	4	14
onX Offroad	5	1	8
Wish	15	10	17
Dreame	8	8	14
Tapas	5	6	11
Sephora	7	10	13
Twitter	8	7	12
Twitch	6	1	4
NewsBreak	6	11	7
Headspace	6	6	10

Table 5. Top 10 services, sorted by greatest disparity in unique dark patterns across **D**esktop, **M**obile, and **A**pp.

Table 3 and Table 4 show the services in our corpus with the most and least unique dark patterns combined across their three respective modalities.

4.1.2 Modality-to-Modality Comparisons. Next, we investigate comparative differences between pairs of modalities for a given service.

Figure 2 shows the distribution of differences in unique dark pattern usage between pairs of modalities. Given two versions of a service where s_i and s_j are the sets of dark patterns in modalities i and j, the x-axis is the difference $|s_i| - |s_j|$ between the two cardinalities. If $|s_i| - |s_j| = 0$ for the given modalities of a particular service then they contained the same number of unique dark patterns. The y-axis is the CDF of modality pairs with exactly that count of differences. We plot lines that compare the desktop web to app modality, desktop web to mobile web modality, and app to mobile web modality.

We draw several conclusions from Figure 2. First, more than 70% of the pairs fall within the $[-3, 3]$ range, meaning that for most services in our corpus the number of unique dark patterns across modalities rarely diverges by more than three patterns. Second, we observe that the overall trends for each pair of modalities are not significantly different (all MW U and KW H $p \geq 0.34$). Third, we note that the distributions for "Desktop - App" and "App - Mobile" have the longest tails, indicating that the app versions of services tend to have the greatest differences in unique dark patterns versus their desktop and mobile web counterparts. In contrast, the "Desktop - Mobile" distribution is more vertical, indicating less variation between these versions of services (although the distribution is slightly negative overall, meaning that the mobile web versions tend to consistently have one or two more unique dark patterns).

Table 5 lists the top ten services with the highest total difference in unique dark patterns from Figure 2. These services exemplify unusual UI design choices, where one modality might have two or three times the number of dark patterns of another modality. That said, these results do have one caveat: recall from § 3.3 that we could not explore at least one modality of 18 services to the full extent that we could for the rest of the 105 due to partial feature parity. Four of these services (Mangatoon, onX Offroad, Dreame, and Twitch) appear in Figure 2. Thus, we caution that results for these four services are an upper-bound on the amount of disparity between their modalities, i.e., it is possible the disparity could be lower if all features in all modalities were explorable. Still, we consider these cases important to retain in this figure as they highlight the design challenges of assessing feature parity, which we discuss in § 5.1.

While Figure 2 is useful for comparing the overall frequency of dark patterns between pairs of modalities, it does not tell us anything about whether services use specific dark patterns consistently

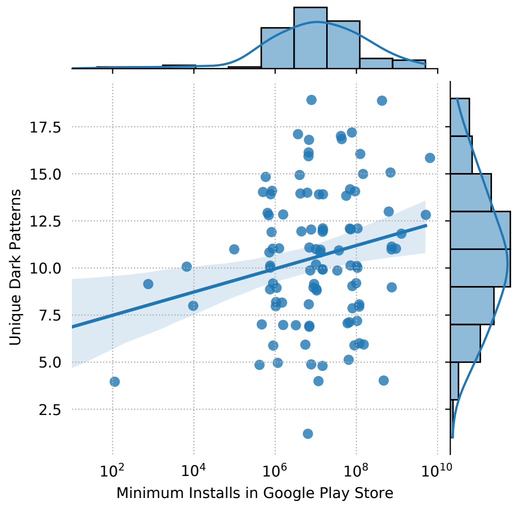

Fig. 4. Scatter-plot showing minimum installs in the Google Play Store versus unique dark patterns per service. Points are jittered along the x- and y-axes to improve readability. Frequency histograms in the x- and y-dimension are shown, as is a linear regression best-fit with confidence intervals.

across modalities. For example, a service might include three dark patterns in its desktop website and mobile app, yielding no difference in Figure 2, but each modality might incorporate three completely different dark patterns.

To investigate the issue of consistency across pairs of modalities, we plot the distribution of Jaccard coefficients between pairs of modalities in Figure 3. Given two versions of a service where s_i and s_j are the sets of dark patterns in modalities i and j, the Jaccard coefficient is defined as Jaccard $= \frac{|s_i \cap s_j|}{|s_i \cup s_j|}$, i.e., the size of the set intersection divided by the size of the set union. The x-axis are the Jaccard coefficients from zero to one, with the former meaning the pair of modalities used totally disjoint sets of dark patterns, and the latter meaning the sets where identical. The y-axis is the CDF of modality pairs with that exact Jaccard coefficient. As with Figure 2, we plot three lines comparing all combinations of modalities.

Figure 3 reveals that the sets of dark patterns included in the web modalities of services in our corpus tend to be much more similar than the set of patterns included in the mobile app modality. The “Desktop vs. App” and “App vs. Mobile” distributions are significantly different from the “Desktop vs. Mobile” distribution (all MW U and KW H $p < 0.05$), but not from each other ($p = 0.37$). The median pair of desktop and mobile websites in our corpus have a Jaccard coefficient of 0.8, e.g., they share eight out of ten observed dark patterns, while the median website and app only have a Jaccard coefficient of 0.5. We hypothesize that one explanation for these observations may be that the web versions of a given service share the same underlying source code. In contrast, the app version of a service may be written in a different programming language (e.g., Objective C, Swift, or Kotlin) than the website, possibly by a different team of developers.

4.1.3 Dark Pattern Usage versus Service Popularity. Next, we briefly examine the relationship between dark pattern adoption and service popularity. Figure 4 is a scatter-plot showing the number of app installations reported by the Google Play Store for apps in our corpus on the x-axis, and unique dark patterns per service on the y-axis. Note that the Play Store does not report the exact installation counts for apps—rather it reports a count that is rounded down to the nearest power of ten or power of ten times five, whichever is larger. This rounding explains why the points in Figure 4 are situated in vertical bands. To improve clarity, we jitter the points on the x- and y-axes, and show frequency histograms of the points along each axis.

We find a weak correlation between app popularity and dark pattern adoption (Spearman's $r = 0.15$, $p = 0.11$).[12] To illustrate this relationship, Figure 4 shows the linear-regression best-fit line with confidence intervals.

Unfortunately, we are unable to analyze dark pattern adoption versus popularity stratified by modality for two reasons. First, top lists of popular websites like Alexa[13] and Tranco [57][14] do not contain several of the services we examined, especially services that use subdomains. For example, these lists rank Google, but do not provide a ranking for Google Translate (which uses `translate.google.com`). Second, rankings like Alexa and Tranco that are accepted in the research community do not differentiate between the popularity of desktop and mobile websites of services. We note, however, that our high-level findings roughly match those from Mathur et al. [46], who found that popular websites (sorted by Alexa rank) tended to include more e-commerce-related dark patterns.

4.1.4 Summary. Overall, we observe that all of the services in our corpus include at least one type dark pattern, with the majority including seven or more types (Figure 1). Our results are consistent with previous work [20] that find dark patterns in at least 95% of apps in a corpus of 240. Further, we find that dark pattern usage frequently differs across the versions of a given service: quantitatively, we observe that apps tend to have more unique dark patterns than their web counterparts (Figure 2), and qualitatively, we observe that apps tend to include different patterns than the corresponding websites (Figure 3). Lastly, we find that popular apps tend to include slightly more types of dark patterns overall (Figure 4).

4.2 Differences Across Dark Patterns

In this section, we shift our focus towards examining how dark pattern usage differs across modalities with respect to different types of dark patterns. We examine dark pattern frequency organized by category and individually.

4.2.1 Dark Pattern Category Comparisons. We begin by focusing on the adoption of different categories or taxonomies of dark patterns across modalities. Recall from § 3.3 and Table 2 that we organize the 50 dark patterns in our codebook into nine themes. Figure 5 presents the percentage of services that contained at least one dark pattern from each theme, broken down by modality.

We note several takeaways from Figure 5. First, more than half of the services in our corpus have adopted dark patterns from five of our nine themes, with dark patterns that hinder autonomy and choice in *Settings* being the most popular theme overall. We hypothesize that these differences in overall adoption are intrinsically linked to the purposes of different services. For example, only services that implement storefronts or are ad-supported are likely to adopt dark patterns from the *Shopping* and *Monetization* themes, respectively. In contrast, dark patterns from the *Account Registration*, *Settings*, and *General Use* themes are applicable to a wide variety of services, and dark patterns pertaining to these themes are, understandably, more widely adopted by services in our corpus. Note, however, the dependency evident here on corpus construction: for example, other observational studies of dark patterns have found a greater prevalence of certain types of pattern, e.g., related to *Shopping*, due in part to different corpus construction strategies [20, 46].

[12] Given the logarithmic scaling of installation counts, Spearman's rank correlation r is a more appropriate measure then Pearson's r.
[13] https://www.alexa.com/
[14] https://tranco-list.eu/

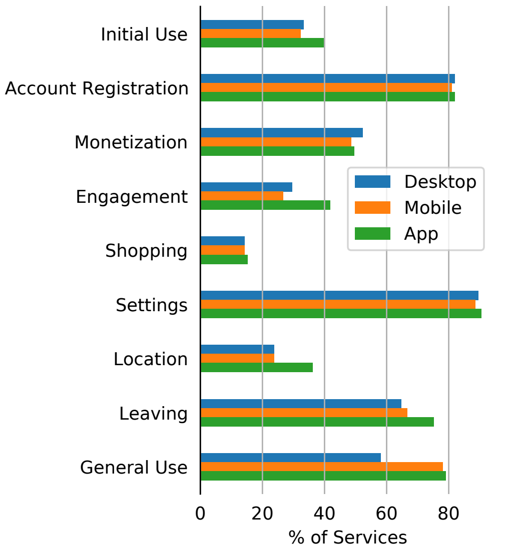

Fig. 5. Bar chart of the percentage of services that contain at least one dark pattern from different categories, broken down by modality.

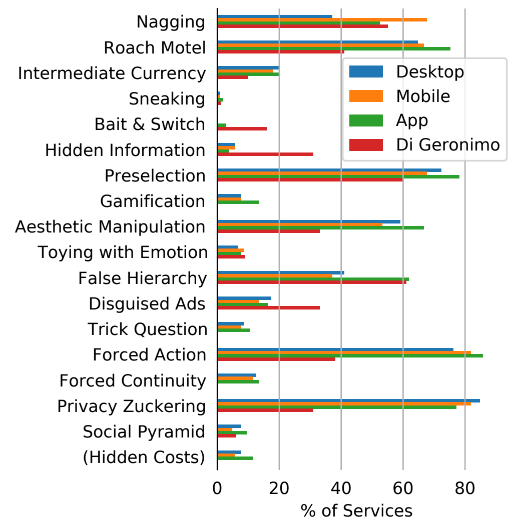

Fig. 6. Bar chart of the percentage of services that contain at least one dark pattern from different subcategories from Di Geronimo et al. [20], broken down by modality. For comparison, we also show the percentages observed in the original study.

Second, we observe that in four of our nine themes (*Account Registration*, *Monetization*, *Shopping*, and *Settings*), the percentage of services adopting dark patterns across modalities are very similar (i.e., less than 5% difference across modalities). In four of the five remaining themes, we observe that a greater percentage of services adopt dark patterns in their app modalities, with especially stark differences in the *Location* and *Engagement* themes (for example, 24% of mobile websites included *Location* patterns, versus 36% of mobile apps). The remaining *General Use* theme skews towards greater adoption of dark patterns in both mobile modalities than on the desktop web.

Rather than organize dark patterns by interaction themes, prior observational studies have organized dark patterns according to the taxonomy developed by Gray et al. [33]. To situate our study within this literature and offer a direct comparison to prior work, we next (1) analyze the adoption of dark patterns organized according to this taxonomy (using the mapping given in Table 2), and (2) directly compare our findings to those presented in Figure 1 of Di Geronimo et al. [20], in which they studied the adoption of dark patterns across 240 mobile apps.

Figure 6 presents the results of this comparative analysis. Overall, as with Figure 5, we observe that some categories of dark patterns are far more prevalent than others, with *Nagging*, *Roach Motel*,[15] *Preselection*,[16] *Aesthetic Manipulation*,[17] *False Hierarchy*,[18] *Forced Action*, and *Privacy Zuckering*[19]

[15] *Roach Motel* is defined as an asymmetrical UI that "makes it very easy for you to get into a certain situation, but then makes it hard for you to get out of it (e.g., a subscription)." [33]
[16] For example, of checkboxes related to opt-in choices about privacy and marketing subscriptions.
[17] Defined by Gray et al. as "design choices that focus the user's attention on one thing to distract them from or convince them of something else (e.g., Brignull's "Misdirection")." [33]
[18] "[G]iv[ing] one or more options visual or interactive precedence over others, particularly where items should be in parallel rather than hierarchical." [33]
[19] To paraphrase, Harry Brignull defines *Privacy Zuckering* as tricking someone into sharing more information about themselves than they intend to [8].

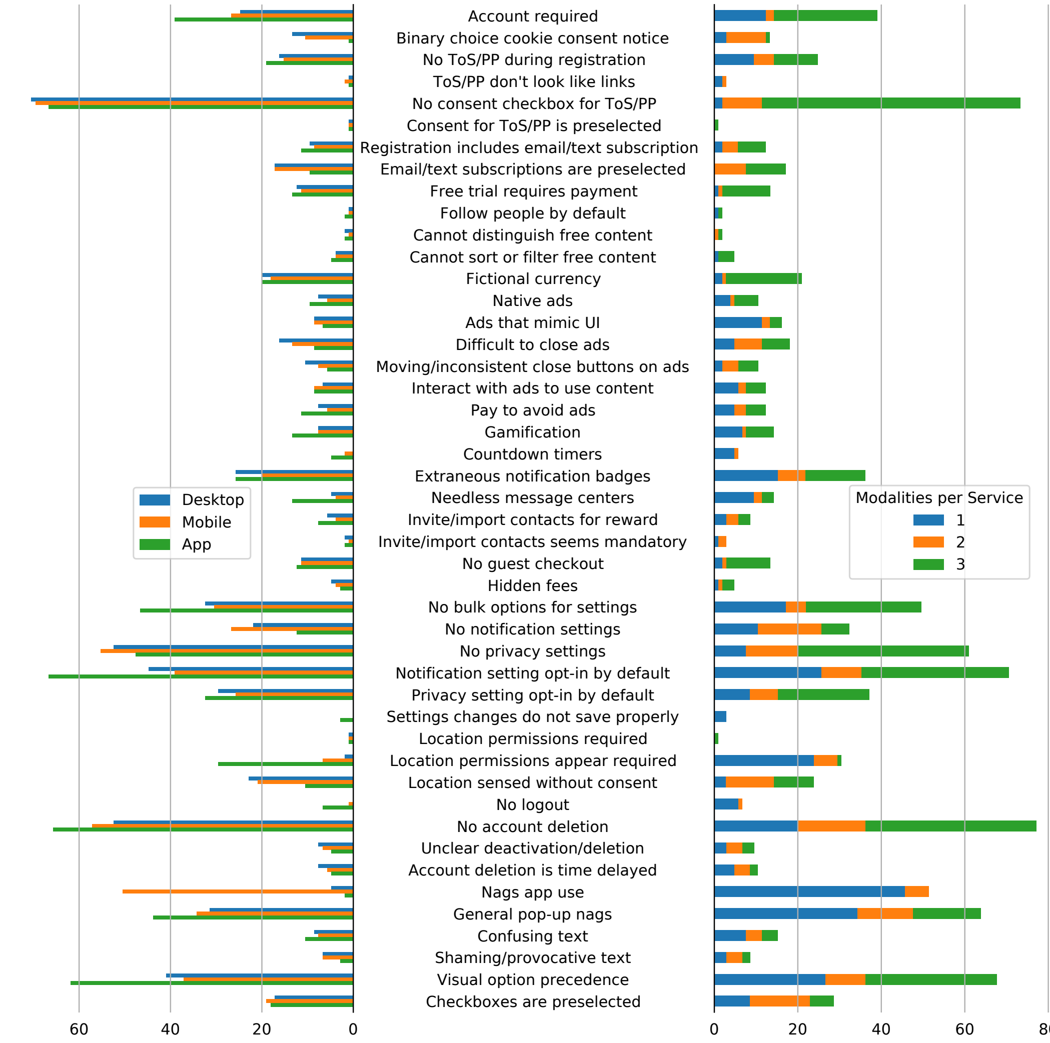

Fig. 7. Bar chart of the percentage of services that contain dark patterns, broken down by modality.

Fig. 8. Stacked bar chart showing, for each dark pattern, the fraction of services in which it appears across zero, one, two, or three modalities.

being the most prevalent. However, we caution that these overall prevalence results must be interpreted with caution, given the dependency on corpus construction.

We observe several disparities between our results and those from Di Geronimo et al. in Figure 6. The categories where we consistently observe more dark pattern usage in our corpus include *Roach Motel*, *Intermediate Currency*, *Preselection*, *Gamification*, *Aesthetic Manipulation*, *Trick Question*,[20] *Forced Action*, *Forced Continuity*, and *Privacy Zuckering*. Conversely, Di Geronimo et al. observed more *Bait & Switch*, *Hidden Information*, and *Disguised Ads*. Some of these disparities may originate

[20]For example, the use of double-negatives to obfuscate the intent of UI choices.

Dark Pattern	%
No consent checkbox for ToS/PP	70
No account deletion	52
No privacy settings	52
Notification setting opt-in by default	45
Visual option precedence	41
No bulk options for settings	32
General pop-up nags	31
Privacy setting opt-in by default	30
Extraneous notification badges	26
Account required	25

(a) Desktop Websites

Dark Pattern	%
No consent checkbox for ToS/PP	70
No account deletion	57
No privacy settings	55
Nags app use	50
Notification setting opt-in by default	39
Visual option precedence	37
General pop-up nags	34
No bulk options for settings	30
Account required	27
No notification settings	27

(b) Mobile Websites

Dark Pattern	%
No consent checkbox for ToS/PP	67
Notification setting opt-in by default	67
No account deletion	66
Visual option precedence	62
No privacy settings	48
No bulk options for settings	47
General pop-up nags	44
Account required	39
Privacy setting opt-in by default	32
Location permissions appear required	30

(c) Mobile Apps

Table 6. Top 10 dark patterns sorted by percentage containing the pattern.

from the selection criteria used to build the two studies' respective corpora: Di Geronimo et al. focused on eight primary Play Store categories with 30 apps each, whereas our corpus investigated 29 Play Store categories with at most six services each. Other disparities highlight differences in the studies' respective codebooks:

- We chose to consider "login for rewards" patterns and achievement badges as *Gamification* instead of *Forced Action*, following the Gray et al. definition of "situations in which certain aspects of a service can only be earned through repeated... use of aspects of the service." [33] In contrast, Di Geronimo et al. elided the *Gamification* category entirely.[21]
- Our codebook contains 13 privacy-related dark patterns that get grouped under *Privacy Zuckering*, versus only two for Di Geronimo et al.
- Di Geronimo et al. do not include a *pay to avoid ads* in their corpus, so we map this to the Gray et al. *Hidden Costs* pattern [33] and denote this additional category in parentheses.

These comparative results highlight that the work of identifying dark patterns is complicated by the evolving discourse around what is and is not a dark pattern, and how to systematize these patterns into a coherent taxonomy. We discuss this further in § 5.2.

4.2.2 Individual Dark Pattern Comparisons. We now proceed to examining the prevalence of individual dark patterns from our codebook across modalities. Figure 7 shows the percentage of services containing each dark pattern, broken down by modality, while Figure 8 shows the percentage of services that include each dark pattern in one, two, or all three of their modalities. These two figures are complementary: Figure 7 is useful for understanding the relative prevalence of patterns, while Figure 8 is important for understanding whether each dark pattern is being adopted consistently across modalities of a given service.[22]

Focusing on the two dark patterns in the *Initial Use* theme, we observe an inversion in adoption: the *account required* pattern is more frequently implemented in apps, while the *binary cookie consent notice* pattern is more frequently implemented in websites. With respect to the latter, we hypothesize that laws like the EU ePrivacy Directive (a.k.a. the "cookie law") and the EU General Data Protection Regulation (GDPR) have pushed websites to adopt cookie consent notices, while mobile apps can instead rely on APIs like the Android Advertising ID for stateful tracking.

The adoption characteristics of dark patterns in the *Account Registration*, *Monetization*, *Shopping*, and *Leaving* themes are remarkably consistent across modalities, in contrast to the other themes in our codebook. In the vast majority of cases, these dark patterns are unpopular, e.g., they are adopted

[21] Like Di Geronimo et al., we chose not to label "grinding" patterns used in video games as dark patterns.
[22] For four of the dark patterns in our codebook we did not observe any instances in-the-wild. Thus, we omit them from Figure 7 and Figure 8. All four patterns were shopping-related.

by <20% of services. Given the rarity of these patterns, we refrain from drawing conclusions about adoption trends. That said, there are two exceptions. First is the *no consent checkbox for ToS/PP* dark pattern, which is the most prevalent pattern in our corpus across all modalities (see Table 6). This dark pattern corresponds to account creation interfaces that (1) notify the person about the services' ToS and/or PP with relevant hyperlinks, but (2) assume that the person accepts these terms if they complete the account creation process or otherwise proceed (Figure 11 in the Appendix shows an example of this dark pattern). We observe that this presumptive approach is far more common than alternative designs that ask the user to explicitly consent to the terms separately from other actions. Further, 62% of services that adopt this pattern do so across all three of their modalities. In some services, only one or the other policy type was provided (e.g., PP or ToS, but not both) with or without links—in these cases, a service can have both the *no checkbox for ToS/PP* and the *no ToS/PP during registration* patterns as we considered any missing information to be disadvantageous for the user.

The second exception is the *no account deletion* dark pattern, which is also widely adopted overall (appearing in 77% of services) and appears more often in the app modality (more than 65% of apps in our corpus versus ≤58% of websites).

For the six dark patterns in the *Engagement* theme we make several observations. We find that *extraneous notification badges* are adopted in roughly similar amounts across modalities, with 15% of services adopting them in a single modality and 14% adopting them in all three modalities. In contrast, the conceptually similar *needless message centers* dark pattern mainly appeared in a single modality: mobile apps. We hypothesize that designers may adopt this pattern more frequently in mobile apps because people have been habituated to use apps on their smartphone for messaging, whereas services like SMS and Whatsapp are not typically available via the web. Additionally, the *invite or import contacts for rewards* pattern is more common in mobile apps, but the overall prevalence of this pattern in our corpus is low.

Next we discuss dark patterns in the *Settings* theme. As we note in § 4.2.1, this is the most prevalent theme of dark patterns in our corpus overall: with the exception of the *settings changes do not save properly* dark pattern, all of the other patterns in the theme appear in ≥32% of services. We observe that the *no bulk options for settings*, *notification setting opt-in by default*, and *privacy setting opt-in by default* dark patterns are all more prevalent in the app modality in our corpus, while the *no notification settings* and *no privacy settings* patterns are more prevalent in web modalities. Among these five, the *no privacy settings* dark pattern appears most consistently across all three modalities of services, with 41% of services in our corpus adopting this posture. We hypothesize that services opt people into notifications more aggressively in the app modality, and have fewer notification settings available in web modalities, because mobile apps have more robust notification APIs than web browsers.

We observe that dark patterns in the *Location* theme exhibit a disparity between the web and app modalities. The *location permissions appear required* dark pattern appears in 29% of mobile apps in our corpus but ≤7% of websites. Although both web and app platforms offer location-sensing APIs that services must request access too, it is interesting to observe that more services adopt pressure tactics to try to coerce people into approving location API requests within mobile apps. We find that the *location sensed without consent* dark patterns has the opposite adoption characteristics, appearing in 21–23% of websites in our corpus but only 10% of mobile apps. We hypothesize that this inversion exists because of the fundamental limits of the JavaScript location-sensing API: in desktop browsers, this API relies on IP address-based geolocation to sense a person's location, which is (1) inaccurate relative to the precise sensors available on smartphones and (2) a technique that a service can employ on their own (i.e., without a person's permission) on the server-side. Thus, services have less incentive to request access to the JavaScript location-sensing API versus the Android location-sensing API, and instead opt to perform IP address-based geolocation in modalities that do not have access to the Android APIs.

The six dark patterns in our *General* theme are, unsurprisingly, eclectic compared to the dark patterns in our other themes, which are more narrowly tailored. As such we observe a wide range of adoption behaviors from patterns within the *General* theme. We highlight cases of note:

- We see that nags that push people to use the app version of a service appeared in more than 43% of the mobile websites in our corpus, versus <5% of desktop websites and apps.[23] While we expect a low percentage from the app modality, the disparity between the two browser versions is notable. Conversely, *general pop-ups nags* appear more frequently in mobile apps and websites than desktop websites, and this behavior is inconsistent across services in our corpus: as shown in Figure 8, 34%, 13%, and 16% of services only adopted these nags in one, two, and three modalities, respectively.
- We observe that the *visual option precedence* dark pattern is popular overall, but especially for mobile apps. 27% of services adopted this pattern in a single modality while 31% adopted it in three modalities.

4.2.3 Summary. Of the 46 dark patterns in our codebook that we observed in-the-wild, 30 appeared more frequently in the app modality (Figure 7). While we find that some patterns, like *account required*, *no consent for ToS/PP*, *visual option precedence*, *no bulk options for settings*, *no privacy settings*, *privacy settings opt-in by default*, *notification settings opt-in by default*, and *no account deletion* are utilized consistently across all three modalities by more than 20% of services in our corpus, the majority of dark patterns in our codebook are not adopted as consistently across modalities (Figure 8). These trends persist when examining dark patterns organized by our thematic categories (Figure 5), with patterns in the *Initial Use, General Use, Location,* and *Leaving* categories being more prevalent within the mobile modalities. Additionally, we compare our findings to the dark pattern categories used by Di Geronimo et al. [20] (Figure 6) and observe disparities in dark pattern frequency between the two studies, which accentuate challenges in dark pattern measurement based on codebook and corpus differences.

5 DISCUSSION

In this study, we examined the prevalence of 50 types of dark patterns across the desktop web, mobile web, and mobile app modalities of 105 services. We now explore implications for practitioners, researchers, and policymakers, and discuss the limitations of our work.

5.1 Implications

Analyses restricted to one modality may find that a given service contains few dark patterns, or, conversely, many—but approaches that take modality into account can help construct a more complete picture of a service's darkness. Table 5 highlights the services in our corpus with the highest disparities of dark pattern count between modalities—these results suggests two outcomes: first, that people exclusively using one modality will not experience a service's darkness equally, and secondly, that reviewing a service through a modality with few dark patterns may incorrectly imply that the service is relatively benign.

Ensuring feature parity across versions of a service may offer a partial solution to these issues. We are not claiming that designers must offer every possible feature in every version of a service, but we believe that some features, especially those pertaining to user privacy and rights, should

[23] We did observe cases where a mobile app used an embedded web browser to display content from the corresponding mobile website, which led to the bizarre situation where a nag to install the mobile app would appear within the mobile app.

be available equally across modalities. In our opinion, there are few reasons that justify omitting these features from one modality or another.

We now consider the implications of our findings for designers, researchers, and policymakers.

5.1.1 For Design Practitioners. We recognize that designers do not operate in a vacuum, but in complex decisionmaking systems that combine the efforts of marketing teams, business development teams, engineering teams, and other stakeholders. Like Di Geronimo et al. [20], we did not attempt to intuit designer intent when examining dark patterns, and are aware that even the best designs can result in unintended outcomes. Previous dark patterns research has largely focused on increasing awareness within the design community, particularly in improving and enabling ethical design or value-sensitive design (VSD) [20, 33]. We agree that value-sensitive and ethical design is incredibly important, and believe that the contributions of this paper provide some guidance for making VSD applications more concrete in practice.

Feature Parity Across Modalities. We argue that feature parity across modalities is an issue of equity, especially when it concerns fundamental controls like privacy settings or account deletion options. Our comparative findings may help designers audit omissions across different versions of their service, improving the experience in a way that empowers people and protects their agency regardless of how they accessed the service. Early efforts to ensure feature parity for these fundamental controls may help reduce the amount of technical labor required to enable these features across all modalities—it is potentially less work to include these features or options up-front, than to include them after a service has been built. This presents an opportunity for designers to influence equitable experiences for the end product, and helps prevent feature parity from becoming an afterthought. Similarly, we recognize that development may occur across different groups within an organization, like app-focused and web-focused software development teams. Our findings suggest that feature parity should be brought to the forefront for VSD across teams building parallel versions of a service.

5.1.2 For Researchers. Like DiGeronimo et al. and Mathur et al. we note that more empirical research is needed, especially targeted studies per dark pattern and dark pattern category [20, 47]. We hope that the results of this study help sharpen these future research efforts, by highlighting the critical importance of examining dark patterns across modalities, writ-large and within different versions of specific services. In particular, we suggest two modality-based focus areas as targets for future study: dark pattern causality and dark pattern impact.

Dark Pattern Causality. The three modalities included in this study differ in capabilities, affordances, and features. Each modality's unique traits will impact the design of their interfaces; for example, screen size limitations for mobile devices require more compact designs than desktop sites out of necessity. Our study only observed dark patterns within the Android and Windows 10 operating systems and Chrome browser—other operating systems and device types may impact the expression of dark patterns in unforeseen ways. Future work can inspect dark patterns across several versions of each modality of the same service to learn what OS, device, or browser constraints and/or capabilities might impact dark pattern adoption. Other work could collect samples of mobile/web development design guidance (from documents or interviews) that encourage the use of nudges and persuasive technologies, and investigate how industry norms may result in dark patterns.

Dark Pattern Impact. Surveys on device-type usage (like the US-based surveys cited here) point to disparities in device adoption and ownership across demographic lines [56] or across people overall [4], and highlight upward trends in mobile device ownership [10]. Future dark patterns research should similarly consider how manipulative interfaces impact different groups of people. For this study, we interacted with services as if we were novice users and standardized our actions where possible, but the lived experiences of people in their preferred modality may differ greatly from controlled interactions conducted by computer scientists. User studies can capture how people interact with dark patterns in-the-wild, at different experience levels like novice or superuser, and across preferred modalities or owned devices. Additionally, we are concerned that dark pattern variability across modalities may exacerbate existing social inequalities and exploit vulnerable populations, especially for people whose primary (or only) internet-capable device is mobile. To investigate these concerns, we hope that future work will explore the intersections between the welfare categories outlined in Mathur et al. [47], different modalities, and different demographic populations.

5.1.3 For Policymakers. Based on our study's results we make three suggestions for policymakers.

Truthfulness of Legal Disclosures. Companies frequently make legal disclosures about how people can engage with their service regarding account creation, account deactivation, privacy settings, and other options. Terms of use and privacy policies may articulate the choices and controls available to people at a service- or company-level, which may be sufficient for compliance to existing legal standards. But disparities in user agency with features across modalities raise concerns over the truthfulness and accuracy of legal disclosures. When terms of use and privacy policies promise certain kinds of options and choices for all people, but the way that a person experiences these choices differs significantly between modalities (with some people being practically obstructed or even denied from taking advantage of certain features), regulators like the US Federal Trade Commission and state consumer protection agencies might find that the mismatch between a company's representations and a particular subgroups' experience using the service gives rise to an unfair or deceptive trade practice.

Parity Requirements for Dark Pattern Frameworks. Although there are not many specific regulations targeting dark patterns, the few that do exist have prioritized feature parity as a consumer protection value to mitigate companies' attempts to make commitments easy and withdrawals difficult. For example, additions to the CCPA in Section 999.315(h) require the number of steps to opt out of the sale of personal information to be equal to or less than the number of steps to opt in. Inequable omissions, by requiring people to switch modalities in order to leave a service or adjust settings, would violate this principle. Policymakers may consider extending this parity principle to other rules. For example, Section 995.305.(a)(3) of the CCPA outlines where business should place notices for the collection of personal information in browser, app, and offline interaction settings. Conversely, requests to delete information are not as strictly defined, merely requiring a minimum of two methods of offering this option, only one of which is built into a user interface (the service's website) (999.312(b)). By requiring parity beyond opt-in/opt-out requests, and across modalities, policymakers can construct rules that equalize experiences and improve agency for all people across multiple modalities.

Holistic Investigation for Enforcement. Our findings that user experiences and levels of agency cannot be assumed as equivalent across modalities counsel enforcement authorities like the FTC to ensure thorough, holistic investigations that consider different modalities. When investigating compliance with rules that may be impacted by dark patterns, simply checking one modality of service such as a website for compliance might fail to detect dark patterns relevant to consent, notice, or fairness requirements in a different modality such as a mobile app.

5.2 Limitations

Prior work has discussed challenges to dark pattern identification: Mathur et al. [46] provide a robust mapping of dark patterns to cognitive biases, but warn that individual susceptibility to these cognitive exploits may vary. Di Geronimo et al. [20] called this "DP-blindness" and found that the majority of participants in a laboratory study were unable to correctly identify malicious designs, let alone specific dark patterns. Even for researchers, dark patterns still prove difficult to classify. Di Geronimo et al. report encountering DP-blindness during their classification work even when two researchers labeled patterns together. Although our approach to inter-annotator agreement differed from Di Geronimo et al., we also found that our labelers were more successful at identifying the absence of dark patterns than the presence of dark patterns (see § 3.5.1). Taken together, these studies highlight the difficulties that researchers and the public face when trying to accurately identify dark patterns. Additional research is needed to develop the theory of DP-blindness and potential mitigation strategies.

Codebook Construction. Like Di Geronimo et al. [20], we felt that certain adaptations to existing taxonomies and lists of dark patterns were necessary for our codebook. We also did not include all of the dark patterns discussed by Mathur et al. [46] or match all of the behaviors investigated by Di Geronimo et al.. Thus, our results are not entirely comparable to those from prior work, nor capture all possible nuances in dark patterns adoption. Additional research is needed to improve codebook consensus across taxonomies that span dark pattern categories, dark strategies, and dark pattern characteristics, while accounting for newly identified patterns in future work. Suggestions by Gray et al. for holistic, n-dimensional dark patterns analysis provide a promising route for dark patterns research [34], especially for developing a unified taxonomy across academic disciplines.

Corpus Composition. To increase the breadth of our study across Play Store categories, we sacrificed per-category depth. In comparison, Di Geronimo et al. [20] examined 30 apps per category across eight categories, whereas we have six or less services per Play Store category across 29 categories. This may impact the expression of some dark patterns in our data, like shopping patterns, since we examined few services from the shopping category. Additionally, we examine fewer total services than prior work because (1) we relied on manual, not automated, labeling, and (2) we had to examine three modalities per service.

Modality Usage and Familiarity. The comparative nature of our study required consistency between our usage of each service by modality. To ensure that the tasks we completed in each modality were as similar as possible between modalities, we recorded each service three times in the same order of app first, then mobile browser, then desktop. Thus, this process only mimicked true first-time user behavior for the app versions of each service, as we were primed for the types of behaviors we might expect from the service in the following recordings. UI differences between modalities also make it difficult to ensure complete equivalence between recordings: menu placements, dynamic screen-size scaling, and other modality-specific elements made some features more or less prominent than others. However, we believe our set of tasks still allowed us to capture how a person might interact with a service within each modality. Further, we did not find that having the app recorded first resulted in fewer patterns found in the app modality.

Methodology Constraints. Time, software, account age, and scope restraints in our methodology may potentially prevent us from discovering all dark patterns that exist in services. For example, new user accounts can elicit dark patterns in account creation, but may not elicit dark patterns that impact longtime account holders with greater data invested in a service. In limiting ourselves to Android and Chrome, our results also do not represent all smartphone or internet users—iOS and other browsers may have features that change the expression of some dark patterns. Additionally, our desktop video recordings provided greater visual insight into user input via the mouse icon, so we only marked patterns in the mobile modalities if we were confident that the dark pattern was not influenced by non-visible user input or screen gestures.

Privacy Analysis. With regards to privacy, we did not investigate network traffic from our targeted services, and thus do not know what personal information (if any) they leaked (e.g., location to third-party trackers). We aim to conduct future studies to capture possible leaks, especially for location data and tracking information, or disparities between privacy policy promises and actual service behavior [68].

Generality. As is often the case with observational studies of online platforms, we caution that our results may not generalize over time as the 105 services change, or to other services from the 29 Play Store categories that we drew our corpus from. Additionally, our formal analysis was conducted during the peak months of the COVID-19 pandemic, which may have impacted the content we observed within the services. Similarly, the dark patterns utilized by services may change due to timebound or seasonal events, e.g., Black Friday/Cyber Monday shopping surges. However, these limitations do not alter the overall takeaways of our study.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their helpful comments. This research was supported in part by a Google ASPIRE award, an NSF SaTC Frontiers grant (#1955227), and a Sloan Fellowship grant. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders.

REFERENCES

[1] Eytan Adar, Desney S. Tan, and Jaime Teevan. 2013. Benevolent Deception in Human Computer Interaction. In *Proc. of CHI*.
[2] Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, and George F. Loewenstein. 2013. Sleights of privacy: framing, disclosures, and the limits of transparency. In *Proc. of the Workshop on Usable Security*.
[3] Kevin Allix, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon. 2016. AndroZoo: Collecting Millions of Android Apps for the Research Community. In *Proceedings of the 13th International Conference on Mining Software Repositories* (Austin, Texas) *(MSR '16)*. ACM, New York, NY, USA, 468–471. https://doi.org/10.1145/2901739.2903508
[4] Monica Anderson. 2015. Smartphone, computer, or tablet? 36% of Americans own all three. Pew Research Center. (2015). https://www.pewresearch.org/fact-tank/2015/11/25/device-ownership/.
[5] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Proc. of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*.
[6] Lindsey Barrett and Angela J. Campbel. 2018. Request to Investigate GoogleâĂŹs Unfair and Deceptive Practices in Marketing Apps for Children. https://commercialfreechildhood.org/sites/default/files/devel-generate/vad/google_ftc_complaint.pdf.
[7] 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
[8] Harry Brignull. 2019. Dark Patterns. https://www.darkpatterns.org/.
[9] Angela J. Campbell. 2018. Letter to Donald S. Clark, Secretary of the Commission, and Andrew Smith, Director, Bureau of Consumer Protection, Federal Trade Commission. https://www.commercialfreechildhood.org/sites/default/files/devel-generate/piw/apps_FTC_letter.pdf.
[10] Pew Research Center. 2018. Mobile Fact Sheet. pewinternet.org. http://www.pewinternet.org/fact-sheet/mobile/.
[11] Shruthi Sai Chivukula, Jason Brier, and Colin M. Gray. 2018. Dark Intentions or Persuasion?: UX Designers' Activation of Stakeholder and User Values. In *Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems (DIS '18 Companion)*.
[12] Shruthi Sai Chivukula and Colin M. Gray. 2020. Co-Evolving Towards Evil Design Outcomes: Mapping Problem and Solution Process Moves. In *Proc. of the Design Research Society*.
[13] Shruthi Sai Chivukula, Colin M. Gray, and Jason A. Brier. 2019. Analyzing Value Discovery in Design Decisions Through Ethicography. In *Proc. of CHI*.
[14] Shruthi Sai Chivukula, Chris Watkins, Lucca McKay, and Colin M. Gray. 2019. "Nothing Comes Before Profit": Asshole Design In the Wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*.
[15] Complaint Under Article 77(1) GDPR 2018. https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf.
[16] Gregory Conti and Edward Sobiesk. 2010. Malicious Interface Design: Exploiting the User. In *Proc. of WWW*.
[17] Norwegian Consumer Council. 2018. Deceived By Design. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[18] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proc of NDSS*.
[19] Jayati Dev, Emilee Rader, and Sameer Patil. 2020. Why Johnny CanâĂŹt Unsubscribe: Barriers to Stopping Unwanted Email. In *Proc. of CHI*.
[20] 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*.
[21] J. Elliott and L. Waldron. 2019. Here's how TurboTax just tricked you into paying to file your taxes. https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes.
[22] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-Scale Readability Analysis of Privacy Policies. In *Proc. of the International Conference on Web Intelligence*.

[23] 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*.

[24] Federal Trade Commission 2019. FTC sues owner of online dating service Match.com for using fake love interest ads to trick consumers into paying for a Match. https://www.ftc.gov/news-events/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love.

[25] Alvan R. Feinstein and Domenic V. Cicchetti. 1990. High Agreement but Low Kappa: I. The Problems of Two Paradoxes. *J. Clin. Epidemiol.* 43, 6 (1990), 543–549.

[26] Alvan R. Feinstein and Domenic V. Cicchetti. 1990. High Agreement but Low Kappa: II. Resolving the Paradoxes. *J. Clin. Epidemiol.* 43, 6 (1990), 551–558.

[27] Jon Fingas. 2019. Senate bill would ban deceptive data collection by internet giants. https://www.engadget.com/2019/04/09/senate-detour-act/.

[28] Ina Fried. 2019. Google claims it doesn't use "dark patterns" during Senate hearing. https://www.axios.com/google-dark-patterns-senate-hearing-c75afbc9-2462-4afc-bfd2-4b059c2a1d3d.html.

[29] Stacia Garlach and Daniel D. Suther. 2018. 'I'm supposed to see that?' AdChoices Usability in the Mobile Environment. In *Proc. of HICSS*.

[30] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Proc. of the Workshop on Usable Security*.

[31] Colin M. Gray and Shruthi Sai Chivukula. 2019. Ethical Mediation in UX Practice. In *Proc. of CHI*.

[32] Colin M. Gray, Shruthi Sai Chivukula, and Ahreum Lee. 2020. What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. In *Proc. of the Designing Interactive Systems Conference*.

[33] 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*.

[34] 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 *Proc. of CHI*.

[35] 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*.

[36] 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*.

[37] 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*.

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

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

[40] Adrianne Jeffries. 2019. Yelp is Screwing Over Restaurants By Quietly Replacing Their Phone Numbers. https://www.vice.com/en_us/article/wjwebw/yelp-is-sneakily-replacing-restaurants-phone-numbers-so-grubhub-can-take-a-cut.

[41] Carlos Jensen and Colin Potts. 2004. Privacy Policies As Decision-making Tools: An Evaluation of Online Privacy Notices. In *Proc. of CHI*.

[42] Shan Jiang, John Martin, and Christo Wilson. 2019. Who's the Guinea Pig? Investigating Online A/B/n Tests in-the-Wild. In *Proc. of the Conference on Fairness, Accountability, and Transparency (FAT* 2019)*.

[43] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. In *Proc. of European Workshop on Usable Security (EuroUSEC)*.

[44] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 01 Jan. 2020. The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (01 Jan. 2020), 47–64. https://doi.org/10.2478/popets-2020-0004

[45] Jamie Luguri and Lior Strahilevitz. 2019. Shining a Light on Dark Patterns. *U of Chicago, Public Law Working Paper No. 719; University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879* (2019). https://ssrn.com/abstract=3431205

[46] 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).

[47] Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar. 2021. What Makes a Dark Pattern... Dark?. In *Proc. of CHI*.

[48] Anthony D. Miyazaki. 2008. Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing* 27, 1 (2008), 19–33. https://doi.org/10.1509/jppm.27.1.19

[49] Carol Moser, Sarita Y. Schoenebeck, and Paul Resnick. 2019. Impulse Buying: Design Practices and Consumer Needs. In *Proc. of CHI*.

[50] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark Patterns: Past, Present, and Future. *ACM Queue* 18, 2 (2020).

[51] Harper Neidig. 2019. Senators spar with Google exec over use of 'persuasive technology'. https://thehill.com/policy/technology/450261-senators-spar-with-google-exec-over-its-influence-on-users.

[52] Don Norman. 2013. *The Design of Everyday Things: Revised and Expanded Edition*. Basic Books.

[53] 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*.

[54] Anshul Vikram Pandey, Katharina Rall, Margaret L. Satterthwaite, Oded Nov, and Enrico Bertini. 2015. How Deceptive Are Deceptive Visualizations?: An Empirical Analysis of Common Distortion Techniques. In *Proc. of CHI*.

[55] Luana Pascu. 2019. US Senate to End Deceptive Practices and Dark Patterns on Online Platforms. https://hotforsecurity.bitdefender.com/blog/us-senate-to-end-deceptive-practices-and-dark-patterns-on-online-platforms-21062.html.

[56] Andrew Perrin and Erica Turner. 2019. Smartphones help blacks, Hispanics bridge some – but not all – digital gaps with whites. Pew Research Center. (2019). https://www.pewresearch.org/fact-tank/2019/08/20/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/.

[57] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej KorczyÅĎski, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proc of NDSS*.

[58] 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*.

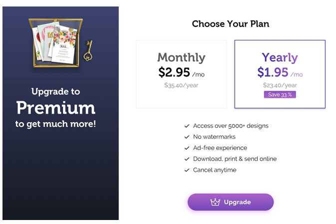

Fig. 9. An example of the *pay to avoid ads* pattern in the GreetingsIsland desktop website.

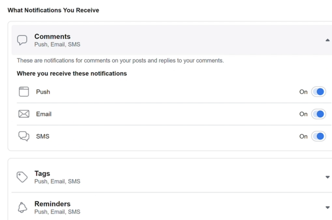

Fig. 10. An example of the *no bulk options for settings* pattern in the Facebook desktop website.

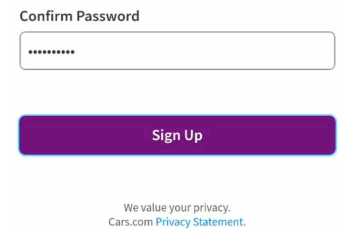

Fig. 11. An example of the *no consent checkbox* pattern in the Cars.com desktop website.

[59] Sen. Hawley Introduces Legislation to Curb Social Media Addiction 2019. Sen. Hawley Introduces Legislation to Curb Social Media Addiction. https://www.hawley.senate.gov/sen-hawley-introduces-legislation-curb-social-media-addiction.

[60] Peter Story, Sebastian Zimmeck, and Norman Sadeh. 2018. Which Apps have Privacy Policies? An analysis of over one million Google Play Store apps. In *Proc. of Annual Privacy Forum*.

[61] Richard H. Thaler. 2018. Nudge, not Sludge. *Science* 361, 6401 (Aug. 2018).

[62] Richard H. Thaler and Cass R. Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.

[63] Martino Trevisan, Stefano Traverso, Eleonora Bassi, and Marco Mellia. 01 Apr. 2019. 4 Years of EU Cookie Law: Results and Lessons Learned. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (01 Apr. 2019), 126–145. https://doi.org/10.2478/popets-2019-0023

[64] 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*.

[65] Giridhari Venkatadri, Elena Lucherini, Piotr Sapiezyński, and Alan Mislove. 2019. Investigating sources of PII used in Facebook's targeted advertising. In *Proc. of PETS*.

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

[67] Jose P. Zagal, Staffan Bjork, and Chris Lewis. 2006. Dark Patterns in the Design of Games. In *Proc. of Foundations of Digital Games (FDG '06)*.

[68] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N. Cameron Russell, and Norman Sadeh. 01 Jul. 2019. MAPS: Scaling Privacy Compliance Analysis to a Million Apps. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (01 Jul. 2019), 66–86. https://doi.org/10.2478/popets-2019-0037

6 APPENDIX

In this section we discuss the novel dark patterns that we encountered during our preliminary exploration (see § 3.1) and added to our codebook (see Table 2).

Extraneous Badges. "Badges" are design elements—often tiny, brightly colored circles—that visually highlight UI elements that require immediate user attention. A canonical example are red dots that indicate the arrival of unread messages in chat and email apps. We consider badges to be extraneous if they direct peoples' attention to UI elements that do not require immediate attention, especially if the end result of interacting with the badged UI element is content that benefits the service. For example, for newly registered users, Zoosk places notification badges over buttons leading to information for their various paid features. We categorize this dark pattern under *Aesthetic Manipulation* [33].

Needless Message Centers. Many services incorporate an inbox-like interface that serves as a centralized location for people to receive and view messages from the service provider (and potentially other users of the service). We consider a message center to be needless if, in our observation, it primarily contained spammy advertisements from the service provider, especially if the service in question was not specifically designed for messaging (e.g., within the onXHunt hunting maps service). In some cases, these are accompanied by extraneous notification badges. We categorize this dark pattern under *Nagging* [33].

Paying for Ad-Free Experiences. We observed a number of nominally "free" services that offered paid ad removal or 'premium' ad-free experiences after onboarding. We consider this pattern to be dark because we feel that asking people for payment to avoid an aggravating experience obfuscates the true cost of the service and thus tricks users. We categorize this within *Nickel-and-Diming* [32] and *Hidden Costs* [8, 33, 46]. Figure 9 shows an example of this pattern.

"Free" Trials. We observed some services that offered some features for free required credit card or payment information from people seeking free trials of additional subscription-based features. We relate this pattern to Mathur et al.'s *Hidden Subscription* pattern [46], but consider our case to be distinct because it focuses on the pre-emptive payment requirement rather than the hiding of the payment requirement. We consider this pattern to be dark because it is meant to exploit peoples' tendency to forget that free trials will expire, and may be coupled with additional dark patterns that discourage people from unsubscribing.

No "Bulk" Options For Settings. We observed cases where trying to edit multiple settings of a similar type required individually toggling each item, including cases with dozens of individual toggles. We consider this to be dark because, while granular controls may be beneficial in many contexts, forcing people to exclusively use granular controls takes time, raises the effort cost of making changes, and thus may discourage people from changing defaults that are beneficial to the service. For example, as shown in Figure 10, Facebook nests notification settings within "accordions", and has individual toggles for communication via push notification, email, and SMS. There is no way for a person to easily disable all notifications of a given type (e.g., comments or tags), or to easily disable an entire communication channel (e.g., email or SMS). We argue that the lack of bulk controls may be especially problematic with respect to opt-out privacy regimes, since this pattern may discourage people from exercising their rights. We categorize this pattern under *Aesthetic Manipulation* [33] and (in some cases) *Privacy Zuckering* [7, 20].

Missing Consent Notices, Consent Checkboxes, or Settings Options. This umbrella encompasses four dark patterns in our taxonomy, covering cases where people may reasonably expect key features to be available in a UI, but they are not. Two cases cover account registration flows that (1) fail to mention the service's ToS/PP at all or (2) simply present a link to the ToS/PP but do not offer a checkbox to consent (i.e., consent is implied by registering an account). Figures 11 and 12 show examples of these patterns. The other two cases concern services that use notifications and/or collect private data, but do not offer options to control these aspects of the service at all. These four dark patterns fall under a number of existing taxonomies, as shown in Table 2.

Settings Do Not Save Properly. We observed instances where services failed to save changes we made to settings or otherwise saved settings improperly. For example, we toggled several data and notification settings "off" in the GoodRx app prior to registration, but found these settings toggled back on after logging in, thus failing to honor in-app selections. While this behavior may be a bug, whether it is intentionally included or not bears no difference on the outcome for the end user: an experience other than the one a person sought. We categorize this dark pattern under *Bait & Switch* [8, 33] and (in some cases) *Privacy Zuckering* [7, 20].

Account Deletion Roadblocks. This umbrella includes two dark patterns in our codebook. *Unclear deactivation/deletion options* covers cases where a service insufficiently communicates what will happen if a person deactivates or deletes their account. We consider this pattern to be dark because it makes it difficult for people to understand if their account and data are actually removed and closed, if the service will still retain and use their information, or understand what deactivation entails. *Account deletion options are time-delayed* covers cases where a service will only initiate the account deletion process after a cool-off period, rather than instantaneously. We

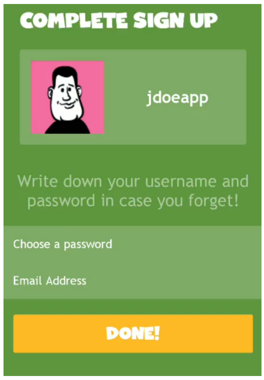

Fig. 12. An example of the *ToS/PP not mentioned during registration* pattern in the Chesskid app.

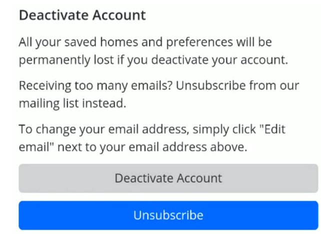

Fig. 13. An example of the *unclear deactivation/deletion options* pattern in the Zillow mobile website. Zillow describes what will happen to bookmarks and preferences if the account is deactivated, but not other types of data. The scary warning is paired with a *visual precedence* dark pattern that highlights Zillow's preferred user action.

consider this pattern to be a form of *Forced Action* [20, 33] since it subverts a person's autonomy by imposing mandatory wait times. For example, attempting to delete a Duolingo account results in a lengthy screen of text explaining that the user must confirm the deletion request via email, then the account will first be deactivated for a 7-day grace period before the service will begin deleting user data. Additionally, we place both of these dark patterns under the *Roach Motel* [20, 33], *Hard to Cancel* [46], *Immortal Accounts* [7] categories.

Received October 2020; revised April 2021; accepted July 2021