Comments of the International Digital Accountability Council (IDAC) to the Federal Trade Commission in the Inquiry into Dark Patterns

May 25, 2021
info@digitalwatchdog.org

The International Digital Accountability Council ("IDAC"), an independent privacy watchdog with a mission to advance accountability, integrity and trust in today's increasingly complex digital ecosystem, submits the following comments to the Federal Trade Commission's inquiry into dark patterns.

We aim to create a digital ecosystem where all actors have strong accountability measures built into their practices, policies and design, and users have full trust in the applications and platforms that they are using. IDAC has conducted investigations into mobile apps including those related to COVID-19, ed-tech, and political elections. Our research demonstrates that a wide range of tools and techniques are employed to subvert user privacy choices.

Dark patterns, a term first coined by Harry Brignull in 2010, are user interfaces in websites or apps that are intentionally designed to trick, confuse, manipulate, or shame users into taking unintended and unwanted actions or, in the case of privacy, thwart users' ability to decide whether and to what extent their personal information is collected and shared. Design decisions that constitute dark patterns are not the result of "sloppy" design, nor are they intended to gently nudge the consumer toward a preferred outcome. Rather, dark patterns are intentionally designed to exploit users' cognitive biases and take advantage of the information asymmetry between the user and the company. For those consumers who have less experience with navigating digital technologies, lower levels of digital literacy or language barriers, dark patterns have a particularly insidious impact. While a user might find an interface frustrating or difficult to navigate, the true impact of these design choices on an individual's autonomy and agency are largely invisible. User interfaces for opting out of data sharing are often impossible to navigate, leaving users either unaware of their privacy options or frustrated in their effort to exercise their rights. While user interfaces may give users "an illusion of control," they in fact "[hide] away privacy-friendly choices" or make it challenging for users to exercise their privacy. As the French

data protection agency CNIL explained, "dark patterns can lead to invalidating consent patterns [that do] not qualify as valid consent freely given."

The use of dark patterns to erode users' ability to safeguard their personal data may also evade legal obligations to provide users with the opportunity to opt-out of tracking and data sharing. For example, a study by the Consumer Reports Digital Lab found that dark patterns were used to circumvent the Do Not Sell provision in California Consumer Privacy Act (CCPA) that required data brokers to provide an opportunity to opt-out of the sale of their personal data. Consumer Reports' testers found that the dark patterns posed significant obstacles to users' exercise of their rights under the CCPA.

The Norwegian Consumer Council's landmark 2018 report, "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy" makes clear that these practices are widespread. The study, which analyzed a sample of settings in Facebook, Google and Windows 10, revealed that "default settings and dark patterns, techniques and features of interface design meant to manipulate users, are used to nudge users towards privacy intrusive options." These include "privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy-friendly option requires more effort for the users."

While consumer manipulation is not unique to the digital space, the ability to manipulate consumers in digital environments risks far greater harm to consumers than practices honed in 20th Century brick and mortar commerce. In the digital environment, not only can dark patterns be deployed to thwart consumer exercise of privacy choices, the unwanted tracking, collection and sharing of personal information that follows permits the leveraging of that data against the consumer in ways that were unimagined before the rise of digital commerce. As Ryan Calo presciently predicted, today's digital market "permits the constant monitoring, collection and processing of data allowing so-called data informed marketing which uses large data sets to identify consumer vulnerabilities and behavioral biases to manipulate consumers into taking actions against their best interests."

Dark patterns have only one purpose: to serve as a digital trap door to deter consumers from making rational choices about their personal data *at the point where it is most impactful to do so*. Once personal data is unwittingly shared without consent or knowledge, there is no way back. Consumers cannot call back the data already shared if they later figure out how to opt out of data sharing. It is also likely that the user can still be identified and tracked based on the multiple device identifiers that have been collected and linked to the device. In our investigations, IDAC has identified hundreds of mobile apps that share multiple device identifiers for the same user, with some potentially engaging in ID bridging, the linking of multiple identifiers for the same user on different devices and across multiple apps, which permits tracking over time across

platforms. ID bridging circumvents user privacy preferences by using the link to maintain the association with a user *even after the user or platform has set privacy preferences and/or reset a past identifier.* The data collected through the practice of organizing and linking information gathered through unique identifiers can then be used to create a "shadow profile."

While it is unclear how often dark patterns and ID bridging can be found together in mobile apps, the presence of both elevates the risks to consumers. For example, during the 2020 United States presidential election, the Trump campaign's mobile app was found to use dark patterns to trick supporters into donating millions more than intended. At the same time, an IDAC investigation found that the Trump app also collected and shared users' device identifiers, which most likely was used for extensive tracking collection of data on users' online behavior across the Internet.

IDAC's recommendations are:

1. Congress should enact comprehensive privacy legislation that specifically prohibits dark patterns and gives the FTC regulatory authority over the statute.

2. The FTC should use the full measure of its authority to put the digital ecosystem on notice that dark patterns that undermine, deter, and mislead consumers' ability to make choices about their personal information will be closely scrutinized for violations of Section 5.

> A.The FTC should issue clear prescriptive guidelines for companies with respect to the design of user interfaces for privacy choices, drawing on the extensive research and investigative findings on dark patterns and the agency's prior decisions on deceptive or unfair design.
>
> B. The FTC should encourage investigators, researchers and civil society groups to share their findings with the Commission in order to develop the record for bringing actions and issuing guidance.
>
> C. The FTC should investigate and take action against companies that use dark patterns to thwart consumers' ability to opt-out of tracking and data collection. There are unique challenges to enforcement posed by these practices, including the diversity and complexity of how dark patterns may appear, which make it difficult to capture these practices at scale. Nevertheless, the Commission should draw on its significant experience with deceptive design cases and the findings of external investigators to take targeted action.

In sum, the fundamental power and information imbalance between consumers and data collectors is exploited at every point in digital commerce. The burden of safeguarding personal

information from the Internet's rapacious appetite for personal data lies almost exclusively with consumers.

Dark practices are designed to manipulate, frustrate and thwart consumers' ability to make rational decisions about their privacy. There is simply no way to reconcile the competing interests of the consumer with those of the digital marketplace without new law and robust enforcement using existing authorities. The FTC must use the full measure of its current authorities to put companies on notice that these practices will not be tolerated.