(303) 573-7474
CoPIRGFoundation.org
Center@CoPIRG.org

COMMENTS OF THE COLORADO PUBLIC INTEREST RESEARCH GROUP FOUNDATION
to the
COLORADO DEPARTMENT OF LAW
On Proposed Rulemaking Under the Colorado Privacy Act of 2021
August 5, 2022

The Colorado Public Interest Research Group Foundation (CoPIRG) is a state-level, citizen-funded advocacy group. We stand up for Colorado consumers and the public interest.

CoPIRG submits these comments in response to the Colorado Department of Law's (hereinafter "Department") call for input on the Colorado Privacy Act ("CPA") rulemaking. We support the Attorney General's efforts to establish strong protections for Coloradans related to consumer privacy, and consumer autonomy and choice when it comes to our data and online lives.

CoPIRG offers comments on three subjects: dark patterns, consumer consent and the importance of implementing a strong brower signal mechanism without delay.

Dark patterns

In today's world, a large number of interactions between consumers and companies happen online. While digital commerce is often convenient for consumers, it also creates a suite of opportunities to shape and manipulate consumer behavior in new ways - ones that either aren't possible, as pervasive, or as easily deployed in brick-and-mortar environments.

Deceptive designs, or "dark patterns", are the deployment of online design elements to trick consumers into taking actions they wouldn't have otherwise taken, even actively against their

interests.[1] Dark patterns can also be deployed to keep consumers locked into decisions using confusing and misleading design elements. These dark patterns can substantially affect how consumers interact with online companies - from influencing how much information consumers give up through mechanisms like default privacy settings or pop-ups that employ confusing colors and complex language[2], to elaborate and unintuitive cancellation processes that may frustrate a consumer's ability to end a monetary subscription.[3] Consumers come into contact with dark patterns online frequently, and have no real way to avoid them, making the state's role as regulator crucial for meaningful protection.

Many substantial interactions consumers have with platforms online are susceptible to the deployment of dark patterns, including, but not limited to: creating accounts and signing up for online subscription services; selecting or changing privacy settings on online platforms; browsing and making purchases online; and deleting accounts or subscriptions. CoPIRG encourages the Department's rulemaking to account for the range of scenarios in which dark patterns can impact consumers, including, but not limited to, the examples above.

Many types of dark patterns are in use today. Common ones include forcing users to create accounts to enable the collection of unnecessary data by the platform; using countdown timers to create a sense of urgency in consumers to take advantage of a deal that doesn't actually expire; and requiring exceedingly burdensome steps to end a relationship with part or all of a platform's services. Dark patterns are also often used for gathering consumer consent, or making it difficult for consumers to exercise real choices about their data. For example, TMobile subscribers who wish to opt-out of the phone carrier's data collection and targeted advertising program must download a special app - one that offers no other functionality or purpose than being the opt-out portal consumers have available to them if they wish to end their enrollment in a program that was done for them automatically by the company.[4] Opt-out mechanisms such as this serve as barriers to genuine consumer choice, serving instead the interests of the controlling entity.

The use of dark patterns can cause real harm for consumers. They can cause financial harm, by manipulating consumers into making purchasing or subscription choices they may not have

---

[1] Harry Brignull, "What is deceptive design", Deceptive Design (web page). Available at: https://www.deceptive.design/

[2] *Deceived By Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,* Norwegian Consumer Council, 27 June 2018. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

[3] *In re Amazon*, Electronic Privacy Information Center complaint, 23 February 2021. Available at: https://epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf

[4] "Mobile Advertising ID Opt Out", TMobile Advertising Solutions (web page). Accessed on 4 August 2022 at: http://www.pushspring.com/optout.html?INTNAV=fNav%3ALegal%3AAdvertisingChoices

otherwise made, or creating a cancellation process that is unduly difficult, and therefore more likely to result in a consumer making additional payments, as they must set aside time in their schedules to sit down and figure the process out. Consumers are forced to expend time and energy even in one-off interactions, studying complex interfaces or reading confusing disclosures or consent every time they download a new app or visit a new site if they wish to exercise control over their data. Dark patterns can also be used to trick consumers into sharing information they may wish to keep private.

Given the range of uses of dark patterns and the harms they pose to consumers, the Department should create rules that prohibit platforms from using dark patterns in any consumer interaction. Specifically, a prohibition on the use of dark patterns to collect consumer data, or consent for data collection and processing, should be enumerated. The Department should consult the comments submitted by the Electronic Privacy Information Center for possible language, and continue to work with consumer-focused stakeholders in crafting the rules around dark patterns.

Rules must be designed to address the wide array of types of dark patterns used today, and crucially also ensure the flexibility to regulate dark patterns of the future. Web-enabled platforms and services are continually developing technologies, and regulation too often lags significantly behind, leaving consumers exposed to new harms they must face with largely outdated regulations and few meaningful protections to support them. As currently nascent technologies - like augmented and virtual reality that will likely increase the personalized commercial interactions between consumers and companies[5] - are adopted by Coloradoans and the broader public, the importance of flexible consumer protections will only grow. The rules the Department writes to answer the current moment will be the rules consumers will rely on as these and other technologies come to market. Dark patterns will continue to evolve, and the rules that regulate them must be flexible enough to meet that challenge.

Consumer consent and global opt-out mechanism

Consumer consent is a concept that is often abused by online entities - particularly those in the business of harvesting and selling user data. Today, collecting a consumer's consent is rarely carried out in a way that meets an adequate interpretation of affirmative, informed, freely given, or unambiguous consent.

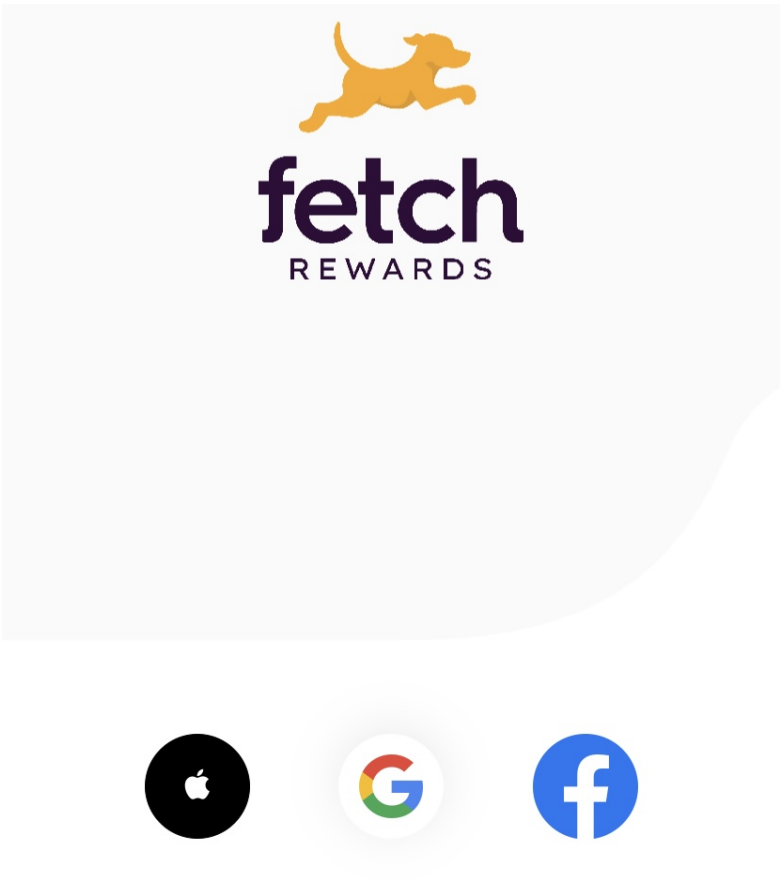
[5] Matt Johnson, "The Effects on Consumers of Augmented and Virtual Reality", *Psychology Today*, 27 April 2022. Available at: https://www.psychologytoday.com/us/blog/mind-brain-and-value/202204/the-effects-consumers-augmented-and-virtual-reality.

Currently, for Colorado consumers, consent is usually gathered through privacy or cookie pop-ups or banners that appear when a consumer visits a website. Sometimes these consent pop-ups do not offer consumers the opportunity to make choices, and simply serve as an alert to site visitors that data-collecting cookies are present, and take a consumer's continued usage of the site as evidence of consent.[6] In many of these cases, for a consumer to find out what exactly cookies or other tracking technologies - such as web beacons or pixels - are collecting, they must find and parse a privacy or cookie policy that is long, contains unclear or inadequate information, and very rarely provides a comprehensive list of the website's "partners" that may embed these tracking technologies into a consumer's browser, or receive data collected by the website itself. Many of these policies go on to refer consumers to the privacy policies of each and every one of a site's partners in order to get a complete picture of how their data is used.[7] In the case of apps, sometimes entities take a consumer's decision to download the app as an indication of consent. Others require the consumer to create a login to use the app, and by doing so, assume the consumer is agreeing to the company's privacy policy. Below is just one example: the app Fetch Rewards, currently #4 in the "top free apps" list in Apple's app store, which informs users of this policy in small text at the very bottom of the screen, only once users have gotten as far as having downloaded it.

(See below)

[6] R.J. Cross of COPIRG, "Cookie pop-ups: why you should think twice before hitting 'accept'", *COPIRG blog*, 19 July 2022. Available at: https://copirg.org/blogs/blog/usp/cookie-pop-ups-why-you-should-think-twice-hitting-accept.

[7] *Out of Control: How consumers are exploited by the online advertising industry*, Norwegian Consumer Council, 14 January 2020. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf



Even when privacy or cookie consent pop-ups display options consumers can use to make choices about their data, there may be dark patterns, like confusing coloring or misleadingly sized buttons, that inhibit a consumer's ability to make clear and affirmative choices. These pop-ups may also use pre-checked boxes consenting to the collection and use of a consumer's data, making opting-in the default.

The CPA rightfully seeks to change the status quo outlined above and give consumers more control over their data. Requiring companies to respect global opt-out signals is one crucial tool the CPA offers consumers.[8] Finalizing its rollout promptly is important to extend meaningful protections to consumers as quickly as possible. For consumers who do not use these mechanisms, however, the Department's strict reading of the CPA's consent language remains key for guaranteeing meaningful consent practices, as does the enforcement of the CPA's data minimization provisions.

Conclusion

COPIRG thanks the Department for its engagement with consumer groups in its CPA rulemaking process. We look forward to continuing to work with the Department as the process continues to ensure that consumers are afforded the best protections possible under the CPA.

Sincerely,

Danny Katz, COPIRG Foundation Executive Director

[8] Work done by the groups Consumer Reports and the Electronic Frontier Foundation on global opt-out mechanisms provides examples of how the technical aspects of these provisions may be crafted.