CALIFORNIA DOUBLES DOWN ON DETERRING DECEPTIVE DARK PATTERNS

Billy Minshall

Written coverage abounds concerning the proposed regulations from the newly formed California Privacy Protection Agency ("CPPA") created under the California Privacy Rights Act of 2020 ("CPRA"). While much of the coverage touches broadly on the proposed changes, it is important to note that one of the key changes relates to dark patterns. Dark patterns are generally defined as deceptive methods to get a consumer to do, or not do, something. Dark patterns, or deceptive design patterns, have been around for a long time but have grown in usage with websites and phone applications. California began targeting dark patterns in 2018 when it passed the California Consumer Privacy Act ("CCPA"). However, the CPRA, which amends and adds to the CCPA, further targets the use of dark patterns.

How Does the CPRA Govern Dark Patterns?

In the CCPA, dark patterns were not explicitly included in the text of the law. The authority cited by the California Attorney General when they promulgated their rules gave vague instructions to "promote consumer awareness,"[1] "ensure that the notices and information…are provided in a manner that may be easily understood by the average consumer,"[2] and "minimiz[e] the administrative burden on consumers.[3]" Those regulations include this unnamed definition for a dark pattern: "a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out."[4] The regulations provided some examples, including, "a request to opt-out shall not require more steps than…to opt-in,"[5] "[a] business shall not use confusing language,"[6] and "the business shall not require the consumer to search or scroll through the text of a privacy policy,"[7] among others.[8]

The CPRA, on the other hand, explicitly mentions dark patterns three times. First, the term is defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation."[9] Second, the law states that "agreement obtained through use of dark patterns does not constitute consent."[10] Finally, the law gives the CPPA authority to

[1] CCP §1798.185(1)(4)(3); note, all citations to the CCPA may no longer be valid due to the CPRA superseding them.
[2] CCP §1798.185(1)(6).
[3] CCP §1798.185(1)(7).
[4] 11 CCR §7026(h).
[5] 11 CCR §7026(h)(1).
[6] 11 CCR §7026(h)(2).
[7] 11 CCR §7026(h)(5).
[8] The other examples listed in 11 CCR §7026(h), are other inconveniences to deter consumers from enforcing their rights, which are also dark patterns.
[9] CCP §1798.140(l); all citations to CPRA are current California law.
[10] CCP §1798.140(h).

promulgate rules regarding opting-out of the sale or share of personal information with the instruction that any link "[d]oes not make use of any dark patterns."[11]

The proposed CPRA regulations contain a much broader exploration into dark patterns. For example, the proposed regulation lists numerous principles that businesses must comply with to process requests or obtain consumers' consent. The listed principles are that the choices be "[e]asy to understand,"[12] have [s]ymmetry in choice,"[13] "[a]void language…confusing to the consumer,"[14] "[a]void manipulative language,"[15] and be "[e]asy to execute."[16] Each of the principles include a non-exhaustive list of illustrative examples as well. Subsection (b) states that any "method that does not comply with" the listed principles "may be considered a dark pattern."[17] Also, any consent obtained "through the use of dark patterns" is considered void.[18] Finally, there is a catch-all provision deeming any method that "has the effect of substantially subverting or impairing user autonomy, decision making, or choice, *regardless of a business's intent*" as a dark pattern.[19] To obtain consent from a consumer – which is required under §7002 – a business must comply with these principles.[20]

Another change in the proposed regulations is the CPRA's expansion of consumer rights beyond notice of the ability to opt-out of the selling of their personal information. The CPRA provides consumers with the right to opt -out of selling and sharing,[21] a right to limit the use of sensitive information,[22] and a right to delete, correct, and know.[23, 24] The proposed regulations will also allow consumers the right to employ global opt-out preference signals and an alternative opt-out link that must be respected by businesses.[25] Importantly, all of these new, or revised, consumer rights incorporate the dark pattern rules outlined above.[26]

Another important change in the CPRA is that there will no longer be a 30-day window for businesses to cure a potential violation.[27] This shift makes getting things right before the law is in effect even more important. It is yet to be known whether or not the CPPA will employ a grace period for violations, absent the statutory requirement. It is probably wise to assume they will not.

[11] CCP §1798.185(20)(C)(iii).
[12] §7004(a)(1); note, all proposed regulations are not yet in effect.
[13] §7004(a)(2).
[14] §7004(a)(3).
[15] §7004(a)(4).
[16] §7004(a)(5).
[17] §7004(b).
[18] *Id.*
[19] §7004(c), italics added for emphasis.
[20] See §7002(a).
[21] §§7013 and 7026.
[22] §§7014 and 7027.
[23] §7020.
[24] "Right to know" means the consumer's right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.
[25] §§7015 and 7025.
[26] See §7013(e)(5); §7015(c)(2); §7020(d); §7025(c)(3); §7026(b); §7027(c); §7028(b) and (c).
[27] See §1798.155(b) for both acts.

What Are the Consequences for Continuing to Use Dark Patterns?

Both the CCPA and the CPRA clearly state that each violation will be subject to a $2,500 fine, or $7,500 if it is intentional. What does "each violation" mean? In a recent action brought by the California Attorney General, Sephora was alleged to have violated the CCPA by selling personal information without the option for consumers to opt-out.[28] Sephora was not alleged to have engaged in dark patterns, but this prosecution is a useful example as to the monetary penalties companies might face from enforcements. Sephora settled the action for a $1.2 million fine.[29] It is unclear from the settlement whether each violation was considered from each consumer, each sale of data, or each day they didn't cure their violation. It is also not clear from the settlement if the violations were treated as intentional or not. Nonetheless, the size of the fine is indicative of more large fines in the future.

What Does California Define as a Dark Pattern?

The proposed regulations provide a number of illustrative examples of what would be considered dark patterns.[30] The examples are mostly obvious, such as when a website uses a larger "yes" button for accepting cookies than the "no" button,[31] switching the order of where the "yes" and "no" buttons are on a list of choices,[32] or broken links or nonfunctional email addresses.[33] The catch-all provision in subsection (c) creates ambiguity and confusion because anything can be a dark pattern if it confuses consumers, regardless of the business's intent. The Attorney General has posted potential enforcement case examples on its website,[34] which are helpful, but not indicative of how *new* cases will be prosecuted if and when the new regulations go into effect. Still, we can use the previous cases as examples of what not to do, since the new regulations will be more restrictive.

We do not have many clear examples of what will get prosecuted in California, but it is almost certain that California will be more aggressive in its prosecutions than any other jurisdiction. Nonetheless, if we look to other jurisdictions for guidance, we can get a better idea of what will *surely* be considered a dark pattern in California.

[28] See the complaint; https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20%288-23-22%20FINAL%29.pdf.

[29] See settlement; https://oag.ca.gov/system/files/attachments/press-docs/Filed%20Judgment.pdf.pdf.

[30] See §7004(a)(2)-(5) for examples.

[31] §7004(a)(2)(D).

[32] §7004(a)(3)(C).

[33] §7004(a)(5)(B).

[34] https://oag.ca.gov/privacy/ccpa/enforcement#top.

How Do Other Agencies Handle Dark Patterns?

California is not alone in combatting the use of dark patterns. The Federal Trade Commission (FTC) recently brought actions against businesses for using dark patterns to the detriment of consumers. In September 2020, the FTC agreed to settle charges against Age of Learning, Inc. (ABCmouse) for $10 million for making it nearly impossible for consumers to cancel their subscriptions.[35] Then-Commissioner Chopra provided a separate statement regarding dark patterns after the settlement which identifies other dark patterns and lays out how the FTC would handle future enforcement actions.[36] Besides the "roach motel" dark pattern employed by ABCmouse, he identifies "using buttons with the same style but different language, a checkbox with double negative language, disguised ads, or time pressure designed to dupe users into clicking, subscribing, consenting, or buying" as other dark patterns the FTC will be targeting. Other prominent enforcement actions relate to subscriptions as well and are not quite comparable to the provisions in the CCPA or CPRA.[37] What can be drawn from the FTC is that burying request forms in privacy policy pages, not answering emails with requests to opt-out/cancel or providing circular links in order for the consumer to opt-out are all clearly dark patterns. Besides the FTC, the Consumer Financial Protection Bureau (CFPB) has also been active in prosecuting dark patterns.[38]

The Colorado Privacy Act and the Connecticut Data Privacy Act, which go into effect on July 1, 2023, also ban the use of dark patterns. Colorado and Connecticut are still in the rulemaking process and will likely have the same issues of defining what will be prosecuted as a dark pattern. It will be important for companies, whether subject to these laws or not, to stay apprised of how other states prosecute alleged dark pattern violations.

How to Navigate the Road Ahead?

Everyone is still in the dark about what is considered a dark pattern in California. The CPRA going into effect next year, along with its new regulations, will shine some light on what the CPPA will be looking to prosecute. Until there are more enforcement actions, there is little more we can do but guess as to what will be considered a dark pattern. Regardless, there are steps that can be taken to minimize exposure to future enforcement actions:

- **Listen to your customers** – If you receive any complaints, leverage them to improve your processes, especially if there are issues with multiple complaints.

[35] https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing.

[36] https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

[37] https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions.

[38] Sometimes the FTC partners with the CFPB in enforcement actions, but with very similar targets; see a recent lawsuit - https://www.consumerfinance.gov/about-us/newsroom/cfpb-charges-transunion-and-senior-executive-john-danaher-with-violating-law-enforcement-order/.

- **Follow the Research** – There are groups, such as the Center for Internet and Society at Stanford, that have been conducting research and providing feedback on dark patterns.[39] This type of information will likely be consumed by regulators.

- **Common Sense** – Have someone at your company test your processes to see if they are confusing. Your employees are consumers as well.

For assistance with or additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.

__Redgrave LLP__ is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.

[39] See this letter sent to the California Attorney General as an example, https://cyberlaw.stanford.edu/sites/default/files/blogs/CCPA%20comments%20October%2028%202020_corrected.pdf.