Trends in Data Privacy Regulation: Dark Patterns

Article By
John J. Rolecki
Varnum LLP
Varnum, etc.

Related Practices & Jurisdictions
- Communications, Media & Internet
- Consumer Protection
- Administrative & Regulatory
- All Federal

Friday, May 27, 2022

Have you tried to unsubscribe from a recurring service and given up? Have you opted to “accept all” cookies on a website to access the content without an annoying banner covering half of the page? Nearly all web users have encountered some form of what is commonly known in the data privacy community as a “dark pattern”: an interface designed to nudge user behavior toward choices he or she might not normally make if the options were presented differently. Although businesses and their web or app designers may feel tempted to explore employing these methods, the increased regulatory focus on dark patterns makes it more important than ever to consider the avoidance of dark patterns as a legal obligation, not just a best practice. This advisory will address the following:

- What is a dark pattern?
- What are regulators doing about them?
- Guidelines for avoiding enforcement issues.

What is a dark pattern?
Dark patterns exploit human psychology to manipulate our decision-making on the internet. Often the choices we are “nudged” to make benefit the companies providing the website or application we are using but are contrary to our own interests. A September 2019 study identified and categorized 15 types of dark patterns encountered about 11% of the time across 11,000 popular shopping websites.[1] The researchers grouped these mechanisms into seven categories: sneaking, urgency, misdirection, social proof, scarcity, obstruction and forced action.[2] The same study noted that third-party developers were frequently the source of dark patterns embedded on e-commerce sites.[3]

What are regulators doing about them?
Undeniably, there is a clear trend of increased attention, regulation and enforcement regarding dark patterns. In general, U.S. law prohibits “unfair or deceptive acts or practices in or affecting commerce.”[4] Although this law – Section 5 of the FTC Act – does not expressly reference dark patterns,[5] the regulators in charge of enforcing it have repeatedly signaled an increased focus on dark patterns and have acted accordingly with related enforcement actions.[6] Just last month (April 2022), the Consumer Financial Protection Bureau sued Transunion for allegedly using “an array of dark patterns to trick people into recurring payments and to make it difficult to cancel them.”[7] Some of the emerging comprehensive data privacy state laws also address dark patterns, either expressly prohibiting them in certain circumstances or deeming behavior resulting from dark patterns insufficient to constitute consent.[8] Notably, in April 2022 the Network Advertising Initiative (NAI) – a self-regulatory organization for adtech – directly addressed dark patterns in newly-released guidance.[9]
While the issue of whether using dark patterns undermines a data subject’s actual consent to process his or her data under Europe’s General Data Protection Regulation (GDPR) is far from new, on April 23, 2022, the European Commission took a more concrete step toward regulating them in its preliminary agreement to the structure of the new Digital Services Act (DSA).[10] In describing the framework of this probable forthcoming law that will regulate content made available on online platforms,[11] the European Parliament voiced the same concerns described above: “[o]nline platforms and marketplaces should not nudge people into using their services, for example by giving more prominence to a particular choice or urging the recipient to change their choice via interfering pop-ups. Moreover, cancelling a subscription for a service should become as easy as subscribing to it.”[12] Echoing these concerns, the preliminary DSA terms state: “[p]roviders of online platforms shall not design, organize or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions.”[13] While U.S. data privacy regulations are nowhere close to being in lockstep with those of the European Union, this development is notable because in a global digital economy, European data privacy regulations influence business – and sometimes legislation – in the U.S. as well.

Guidelines for avoiding enforcement issues.

Although the issues presented by dark patterns are not new, the frequency with which new laws and those who enforce them expressly address dark patterns is a new and notable global trend. Although dark patterns have generally been subject to challenge in the U.S. as deceptive business practice under Section 5 of the FTC Act,[14] the rapid emergence of more targeted data privacy regulations has brought a new spotlight to these practices. This growing regulatory framework guarantees that overlapping layers of domestic and international regulators will be attuned to the issue over the coming years. Regulators are also likely to increasingly have improved mechanisms and resources to enforce these laws. Further, since data privacy laws are generally extraterritorial, international developments on the matter cannot be ignored by businesses that offer e-commerce abroad.

Avoiding dark patterns in web design, particularly relating to e-commerce, should be considered more than a best practice: regulators have clearly signaled it is a legal obligation. Beyond e-commerce, as data privacy laws increasingly mandate businesses to consider and comply with consumers’ data processing preferences, businesses with a digital presence must be conscious of – for starters – the manner in which they obtain consent to cookie placement or other data collection mechanisms, data sharing, direct marketing or any number of forms of processing which may be subject to a number of current and future laws.


[2] Id. at 12.

[3] Id. at 22 et seq.


[6] Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security Commission, File No. P065401 (October 1, 2021). (“The use of dark patterns and other conduct that seeks to manipulate users only underscores the limits of treating present market outcomes as reflecting what users desire or value.”); see also Stipulated Order for Permanent Injunction and Monetary Judgement, Federal Trade Commission v. Age of Learning, Inc., No. 2:20-cv-7996 (C.D. Cal Sept. 8, 2020), (fining the respondent $10 million due to the online children’s education company’s alleged concealment of the fact that users that signed up for “special offer” memberships would be automatically charged a renewal fee at the end of the 6 or 12 month period and obfuscation of the cancellation process). An FTC commissioner’s extremely strong statement regarding dark patterns, issued in connection with the Age of Learning matter, is available here.

[7] The CFPB’s April 12, 2022 press release can be found here, and the formal complaint is found here.

[8] California’s current comprehensive data privacy law, the California Consumer Privacy Act (CCPA), does not expressly address dark patterns. The California Privacy Rights Act (CPRA), which will supersede the CCPA on January 1, 2023, defines dark patterns, establishes that an “agreement obtained through use of dark patterns does not constitute consent,” and prohibits businesses from employing dark patterns to obtain a user’s consent to resume data processing once a user chooses to opt-out. The forthcoming Colorado Privacy Act (CPA) (effective July 1, 2023) takes a similar approach. The forthcoming Virginia Consumer Data Protection Act (VCDPA) (effective Jan. 1, 2023) and Utah Consumer Privacy Act (UCPA) (effective Dec. 31, 2023) do not expressly reference dark patterns.


The European Commission has described “online platforms” to include “online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.”


Available at https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf.


© 2022 Varnum LLP

National Law Review, Volume XII, Number 147