Cybersecurity Law Report cslawreport.com

Jan. 18, 2023

Consumer Privacy

Scrutiny Over Dark Patterns Presents Further Challenges in Online Contracting

By Sherry-Maria Safchuk, Edward Somers and Melina Montellanos, *Buckley LLP*

The Electronic Signatures in Global and National Commerce (ESIGN) Act and its state analogue, the Uniform Electronic Transactions Act (UETA), have played a transformative role advancing e-commerce in the United States for more than two decades. Provisions of the ESIGN Act contain safeguards designed to assure that consumers understand that they are agreeing to receive required disclosures electronically and that they have the ability to access such disclosures.

These assurances continue to be a concern for consumer advocates and regulators, particularly with regard to "dark patterns," a loosely defined term that generally describes engineering online or mobile presentations to imperceptibly shape the visitors' experience and guide them to make often unconscious decisions. Sensitivity to how dark patterns can harm consumers is increasing and the FTC, the Consumer Financial Protection Bureau (CFPB), and other regulators have already intensified their focus on this issue.

That intense focus, coupled with the use of existing case law, could mean trouble for any commercial entity that offers an online method to communicate and conduct business with consumers. Practical measures along with sound practices and procedures can help mitigate risk.

See "Shedding Light on Dark Patterns: What Financial Institutions Need to Know" (Jul. 21, 2021).

Regulators Are Paying More Attention

Regulators and courts have a long history of scrutinizing online contracts and consumer disclosures. Recently, the CFPB and the FTC have taken an acute interest in digital contracting, concerning themselves with the means and manner used to sign up consumers for products and services. This interest should encourage market participants to place renewed energy in their web and mobile platforms because these federal agencies have signaled an interest in using their authority to police unfair, deceptive, or abusive acts or practices (UDAAP), and to crack down on dark patterns.

A consumer agreement that is formed through the use of dark patterns might be rendered unenforceable against a consumer and may also expose the entity to civil monetary penalties and con-

sumer remediation.

Approaches to mitigating risk can be found by listening to the regulators themselves; some of whom have been quite vocal. Additional help can be gleaned through examining case law regarding digital contracting because various courts have grappled with substantially the same issues for decades, even though the term dark patterns has been less prominent (but not entirely absent) in supervisory and enforcement circles until recently. It is, therefore, helpful when examining dark pattern issues to consider the same general concepts of fairness, notice, mutual assent to terms, and meeting of minds found in contract law.

See "California AG Opinion Hands Companies New Tasks for AI, Data Maps, Marketing" (Apr. 13, 2022).

I'll Know It When I See It

The term dark pattern is not easily reduced to a concise (or even uniform) definition. Web designer and usability expert Dr. Harry Brignull claims to have coined the term in 2010. To further explain its meaning, he identified 11 types of dark patterns with varying degrees of specificity. His typologies include specific deceptions, such as "friend spam," which is when a website tricks a consumer into allowing it to access the consumer's contacts to spam messages from the consumer. But Brignull also includes some typologies that are rather vague, such as "bait and switch," where a consumer sets out to do one thing, but a different, undesirable thing happens instead. The FTC appears to value his opinion – it included him as an expert in a dark patterns workshop hosted by the agency in 2021.

When current CFPB Director Rohit Chopra was an FTC commissioner, he added an element of both profit and consumer harm to the definition, describing dark patterns as "design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent." The inclusion of profit, harm, and deception in the definition of the term is considered informative of Director Chopra's priorities, but also likely driven by the limits of the FTC's and CFPB's supervisory and enforcement authority to police UDAAPs.

Most recently, the FTC has identified four types of dark patterns that it finds most troubling:

1) Misleading Consumers and Disguising Ads

This includes: (1) "advertisements that look like independent, editorial content;" (2) "comparison shopping sites that claim to be neutral but really rank companies based on compensation;" and (3) countdown timers designed to make consumers mistakenly believe they only have a limited time to purchase a product or service.

2) Making It Difficult to Cancel Subscriptions or Charges

This includes "tricking someone into paying for goods or services without consent."

3) Burying Key Terms and Junk Fees

Hiding or obscuring material information from consumers – such as burying key limitations of the product or service or required fees in "dense terms of service documents that consumers don't see before purchase."

4) Tricking Consumers Into Sharing Data

This is when consumers purportedly have choices about privacy settings or sharing data but the manner in which the choices are shown is designed to intentionally steer consumers toward the option that gives away the most personal information.

See "FTC and $391-Million State AG Case Put Location Data Enforcement on the Map" (Jan. 4, 2023).

Regulators Have the Tools to Effect Change in the Market

Loose definitions aside, the serious approach federal regulators are taking towards dark patterns is quite palpable:

- When Chopra was with the FTC, he denounced dark patterns and argued in favor of the FTC's methodical use of all of its tools against "popular, profitable, and problematic" dark pattern business practices.
- In April 2021, the FTC hosted a virtual workshop that examined dark patterns and expressed its concern.
- The FTC issued a subsequent enforcement policy statement in October 2021, warning companies of its intent to act against illegal dark patterns. The FTC's policy statement clarifies that it will use its enforcement power to stop dark patterns and warns that any sign-up process that fails to (1) provide clear, up-front information of the product or service, including the costs and deadlines by which the consumer must act to stop further charges, (2) obtain consumers' informed consent before charging them for a product or service, and (3) provide easy and simple cancellation, is illegal.

Both the FTC and CFPB have wielded their familiar authority to police issues of consumer fairness, abuse, and deception, resulting in an enforcement action against a credit reporting agency (CRA) and an action against an online personal finance company – in each instance, alleging th[illegible] dark patterns to deceive consumers.

The CFPB alleged that the CRA used dark patterns to collect consumer credit card information that appeared to be part of an identity verification process, but through a series of deceptive buttons in the online interface, "signed consumers up for recurring monthly charges using the credit card information they had provided." The FTC, in its action, accused the personal finance company of using false claims of "pre-approved" credit offers to lure in consumers. According to the FTC, the user interface was knowingly designed "to trick consumers into taking particular actions in the company's interest."

The FTC also published a report examining how dark patterns can affect consumer choice and decision making, which could violate the FTC Act and other laws. That guidance includes several recommendations for avoiding that infraction, such as remediating design choices when a business has actual knowledge that a structure manipulates consumer behavior by inducing false beliefs. The FTC also recommends clearly including any unavoidable fees in the upfront, advertised prices because failure to do so may deceive consumers.

These broad concepts presented by the FTC and CFPB are starting points for determining what regulators may be reviewing to identify a compliant digital platform. Additional help comes through case law. In contract litigation, courts have addressed some of the very same issues now being raised by regulators in their reviews of dark patterns. Because those cases appear to be asking the same principal question – whether the online contract should be enforced – they may foreshadow whether regulators would find certain digital platform structures to be prohibited dark patterns.

See "What to Expect From the FCC and FTC Under the Biden Administration" (Sep. 8, 2021).

Judicial Experience and Practical Responses

The ESIGN Act and the UETA provide for the general validity of electronic substitutes, and some general consumer protections, but they are largely technology- and process-neutral, having very little to say about *how* an electronic document is presented or *how* a signature is obtained.

By imposing only limited requirements on parties, the ESIGN Act and UETA leave much of that *how* to the market. Without statutory guidance, most courts have looked to general principles of contract law when called upon to decide the effectiveness of an agreement or disclosure. Electronic agreements, like their paper and ink counterparts, must satisfy basic requirements – *i.e.*, there must be an offer, an acceptance, consideration, and mutual assent to the terms (a meeting of the minds).

Mutual Assent to Terms Requirement

In one example – *Sgouros v. TransUnion* – the U.S. Court of Appeals for the Seventh Circuit ruled that a CRA could not enforce an arbitration clause in a service agreement because that clause failed to meet the "mutual assent to the terms" requirement. The CRA argued that the consume[illegible] in fact agreed to the arbitration clause when he clicked the "I accept & Continue …" butto[illegible] he scroll window in the service agreement. However, the court disagreed, relying on gener[illegible] act

formation principles to conclude that the consumer had not received reasonable notice that his purchase of his credit score included agreeing to arbitration, and without that notice, the consumer could not have consented to the arbitration clause.

Notably, the court reached this holding even though the service agreement appeared facially to comply with ESIGN Act requirements for electronic records and signatures. For example, the "I accept & continue …" button placed at the bottom of the agreement is reasonably an electronic symbol that was likely attached to or logically associated with the electronic agreement, which at least facially – through "I accept" – suggested that the person clicking intended to sign the agreement. The relevant document, presented in an electronic format on a website, was certainly an electronic record within that definition.

Notwithstanding the apparent compliance with the ESIGN Act, the court looked to contract law factors to decide whether there was a meeting of the minds. It noted that (1) the arbitration clause appeared at the bottom of the scroll box, (2) the consumer was not required to scroll down to the bottom of the scroll box, (3) the consumer's attention was not otherwise called to the arbitration clause, and (4) the statement next to the "I accept & continue …" button did not mention arbitration, but, rather, simply stated that the plaintiff was authorizing the CRA to access his personal credit information. This analysis, grounded in contract principles, is quite similar to the exercise that regulators find themselves engaged in with their own dark patterns analysis.

Small Variations Have Big Consequences

In other cases, the courts had shown how seemingly small variations in the design of hyperlinks to the terms and conditions may have big consequences to a contract's enforceability. In *Meyer v. Uber*, the U.S. Court of Appeals for the Second Circuit ruled that a consumer had received sufficient notice of arbitration clause when the registration process for the application included a blue and underlined hyperlink that when clicked, took the consumer to another screen with the terms of the contract, which included the arbitration clause. However, in a factually similar case, *Cullinane v. Uber Techs*, the opposite decision was reached by the U.S. Court of Appeals for the First Circuit. In that case, the user could view the arbitration clause by clicking a gray rectangular box in white bolded, non-underlined text. The First Circuit took issue with the fact that the hyperlink did not have "the common appearance of a hyperlink," which is "commonly blue and underlined," and that other terms on the same screen were a similar or larger size, typeface and with more noticeable attributes.

Key Judicial Considerations

The above cases and others like them are likely illustrative of future outcomes in similar regulatory actions and court disputes. To that end, courts examining digital platforms for general concepts of fairness, notice, mutual assent to terms, and meeting of minds have at various times and [illegible]ious jurisdictions considered:

- **Terms and conditions with insufficient notice of a contractual relationship or terms.** Websites that fail to conspicuously disclose to the consumer that by taking specific actions they are agreeing to enter into a contract, or that a given contract includes certain terms – such as arbitration provisions – are likely to be closely scrutinized by courts or chastised by regulators. This can stem from a failure to clearly label an assent mechanism as such or failure to provide adequate qualification or explanation around the assent mechanism or hyperlinked terms. In one case, a court declined to find that the consumer assented to an agreement where the terms were provided with the statement "I understand and agree to the Terms & Conditions" above a large button labeled "Continue" "because nothing expressly linked the 'I understand and agree…' language to the 'Continue' button."
- **Links to terms and conditions that are small, are buried in the fine print, or otherwise blend in.** Courts also have considered whether a hyperlink to terms and conditions was sufficiently conspicuous, meaning that it was clear to the user that they could review the terms and conditions to which they were agreeing by following the link. This examination may include determining whether the hyperlink stood out (was capitalized, in large text, or was in the middle of the page) among the text on the screen. In one New York case, the court found that contract terms, including a mandatory arbitration and choice of venue, were not enforceable because the terms of use were not obviously available to the consumer. According to the court, those terms were overshadowed by a "Sign In" button that was, in contrast, "very user-friendly and obvious, appearing in all caps, in a clearly delineated box in both the upper right-hand and the lower left-hand corners of the homepage." Additionally, courts have found that links hiding in corners of websites or buried in the fine print fail to provide adequate actual notice.
- **Links that do not look like hyperlinks.** If a hyperlink does not have the appearance of a hyperlink (commonly blue and underlined), it is more likely to be questioned by courts and regulators. In one case, a court faulted a ride-share company's mobile platform for presenting terms and conditions with "no familiar indicia to inform consumers that there was in fact a hyperlink that should be clicked and that a contract should be reviewed."
- **Links that are nested or are not provided at the time of agreement.** Hyperlinks within other hyperlinks are more likely to be found to fail to provide adequate notice to consumers of the terms of a contract. In a California case, the court found that the plaintiff's consent to a hyperlinked agreement applied only to the terms and conditions document immediately behind a first hyperlink, but did not apply to a second agreement accessible through a nested hyperlink in the first agreement.
- **Assent mechanisms that do not have spatial proximity to terms.** The further away the checkbox or button is from the language stating what the consumer is agreeing to [illegible]s likely that the related contract will be found enforceable.

Businesses should take some simple, practical measures to reduce their regulatory risk. Continuing to stay current with regulatory guidance and reviewing case law can help manage an institution's risk. So, too, can maintaining policies and procedures related to document delivery, contracting platforms and marketing. Having thoughtfully written policies on issues – and following them – can also produce a halo effect during encounters with regulators.

Sherry-Maria Safchuk is a partner in the Los Angeles office of Buckley LLP, and assists clients on privacy and data security issues, including matters related to federal and state privacy and data security laws such as the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Safeguards Rule, Right to Financial Privacy Act, California Financial Information Privacy Act and California Consumer Privacy Act.

Edward Somers is a partner and leads the Chicago office of Buckley LLP, where he focuses on advising financial institutions and the fintech industry in regulatory, supervisory, and enforcement matters related to payment systems, consumer lending, and electronic contracting. He routinely assists clients with compliance issues relating to the Electronic Fund Transfer Act, the Electronic Signatures in Global and National Commerce Act, and the Uniform Electronic Transactions Act.

Melina Montellanos is an associate in the Washington, D.C., office of Buckley LLP, where her practice focuses on state and federal regulatory compliance matters for a variety of financial services industry clients. She advises on compliance with federal law and regulations in both deposits and payments, and consumer lending.

The authors wish to express their appreciation for the assistance of partner Jeremiah Buckley in the preparation of this article.

© 2023 Mergermarket Limited. All rights reserved.