Challenging Electronic Assent to Arbitration, Robocalls, and More

Karla Gilbride and Timothy Sostrin

January 27, 2021

CONTENTS

A January decision from Massachusetts' highest court, ***Kauders v. Uber Technologies, Inc.***, 159 N.E.3d 1033 (Mass. 2021), highlights how consumers and employees can effectively challenge their electronic assent to terms found on a company's website. While a consumer may visit a website to make a purchase or sign up for an offer, buried in the terms of use or elsewhere may be attempts to treat the consumer's site visit as assent to arbitration, robocalls, limitations on liability, class action waivers, forum selection, use of the individual's information, or more.

This article examines how a consumer or employee can effectively challenge the individual's alleged electronic assent to these terms, primarily in the context of arbitration and the consent provisions of the Telephone Consumer Protection Act (TCPA). But issues of electronic assent can appear in almost any type of consumer or employee litigation.

The article explains when the design of a company's website or mobile interface provides insufficient notice or too ambiguous an acceptance mechanism to establish a binding contract such as where a "browse-wrap" or "sign-in-wrap" process is not adequate to show assent. The company also bears the burden of describing the website consent process in place at the time of consummation, proving the consumer was the one engaged in that process, and presenting such evidence with an adequate foundation. Where assent involves a required written disclosure to the consumer, the electronic consent must be preceded by a separate process for the consumer to consent to electronic information. The terms being consented to on a website must also apply to the party seeking to enforce them—not always the case where a website owner is distinct from the party seeking to enforce website terms.

Browse-Wrap, Click-Wrap, and Sign-in-Wrap

The principles of contract consummation are the same whether the consumer's assent is by use of a handwritten signature or via an electronic action. As the *Kauders* court stated: "The touchscreens of Internet contract law must reflect the touchstones of regular contract law." The agreement must be properly formed under state law and the burden of proof is on the party seeking to enforce the contract.

State law (based on the Uniform Electronic Transactions Act (UETA)) permits electronic signatures to replace "wet" signatures when the electronic signature meets certain criteria, including the specific intention for the electronic action to be a signature. To be effective under UETA, the action constituting electronic assent must be logically associated with the agreement and executed with intent to agree.

As the *Kauders* court explained, online settings differ in material respects from other contexts in which consumers sign legally binding documents. Clicking a button on a screen does not convey the same "solemnity" as signing a physical document, an act which most consumers understand to carry legal significance.

Most courts find that "browse-wrap" agreements are unenforceable—that is where a website notice states that the terms of agreement are found by clicking on one or more hyperlinks, but the consumer is allowed to complete the transaction without clicking on those hyperlinks. This is the equivalent to purporting to form a contract by notifying consumers that, by walking through the store aisles, the consumer has agreed to the store's terms and conditions. Such passive contract formation will only be upheld in exceptional circumstances. *See* **NCLC's *Consumer Arbitration Agreements* § 4.3.4.4**. The click would not meet UETA's requirement for an electronic signature because the action was not sufficiently "attached to or logically associated with" the terms of the agreement.

Click-wrap agreements are presented on the digital screen, in a scrolling window, or via hyperlink, and the consumer cannot proceed further in making a purchase, downloading software, or otherwise completing the transaction without first clicking a button stating "I agree" or similar language. While often enforceable, click-wrap agreements are not always so, especially when the language surrounding the button or other elements on the webpage create confusion about what the user is agreeing to by clicking the button. *See* **NCLC's *Consumer Arbitration Agreements* § 4.3.4.2**; ***Sgouros v. TransUnion Corp.***, 817 F.3d 1029 (7th Cir. 2016).

Many online interfaces, such as Uber's interface for new rider registration described in *Kauders*, fall somewhere between browse-wrap and click-wrap and are sometimes called "sign-in-wrap." Sign-in-wrap requires the consumer to click a button to agree to a transaction, and text somewhere on the page informs consumers that by pressing the button the user assents to the linked terms and conditions. But sign-in-wrap agreements differ from click-wrap in that there is not a separate button to accept the terms; rather, the button ascribed to have contractual significance is the same button to be pressed to obtain the desired service or product, such as signing into an account or checking out after making a purchase. *See* **NCLC's *Consumer Arbitration Agreements* § 4.3.4.3**.

In finding a sign-in-wrap unenforceable, the *Kauders* court focused on the screen's design elements—the relative fonts in which different terms appeared, and the use of color contrast to direct the eyes to particular blocks of text and not to others. In *Kauders*, the payment information was highly

conspicuous and the terms of use much less so, obscuring the significance of signing up for Uber's service. *See also* ***Nicosia v. Amazon.com, Inc.***, 834 F.3d 220, 236–237 (2d Cir. 2016) (Wash. law); ***Specht v. Netscape Communications Corp.***, 306 F.3d 17, 30–32 (2d Cir. 2002) (Cal. law). The *Kauders* court also found clicking a button labeled "done" did not clearly manifest assent to the terms of use because the "connection between the terms and the act is neither direct nor unambiguous." While the court did not mention UETA this connection is also a necessary element for an electronic signature under UETA.

Pin Down the Business in Time and Space

The effectiveness of a consumer's website assent will be determined by the website's design and the consent process at the time the site was visited by the consumer. And of course, the terms being assented to are not the terms presently on the website, but those on the site at the time of the consumer's visit. Unless the business can competently testify that the interface and language has undergone no changes in the interim, screenshots as to how the website and the consent process work now are not dispositive as to the website's appearance and content at the time of alleged consummation, including such details as the font size, the exact text that appears near the relevant button, and the terms being consented to.

The contract proponent must prove the version of the page the consumer would have seen when the contract was allegedly formed, a difficult task especially for interfaces that are dynamic and adjust their appearance based on input received from the consumer. Always put contract proponents to the test of being able to show the entire flow the consumer would have seen, as it appeared at the time they are alleged to have seen it, introduced with a competent foundation.

Similarly, the same webpage may appear very different on a 14-inch computer screen than on a small tablet or mobile phone. If the consumer remembers the device used to access the site in question and that fact is placed in the record, then any screenshots the contract proponent offers to demonstrate the process should show how each step would have appeared on the type of device and screen size the consumer used.

Require Proof That It Was the Consumer Who Did the Clicking

Once a consumer denies an electronic signature, the proponent of an online agreement has to prove that the particular consumer took the action that constitutes acceptance of that agreement (in other words—electronically signed it), rather than just proving that the consumer's information was entered into a form at a website. Just as in the physical world, if a person denies signing a document, the party attempting to prove the validity of the contract must prove that the signature is valid. This distinction is particularly important in the context of online lead generation and telemarketing, where there is a market for the contact information of individuals who have not necessarily expressed any prior interest in the product or service being sold. This often arises as an issue for consumer consent to robocalls as a defense to a TCPA action. For a browse-wrap contract, the business must prove that the consumer visited the website and had an opportunity to review the terms at issue. For a click-wrap or sign-in-

wrap contract, the business must prove that the consumer, and not some other person or entity, was the one who electronically signed by clicking the button or checking the box.

It is not enough to present a "recording" (e.g., through a product called a Jornaya) showing the steps someone allegedly took to click on the website. Consumers should establish that this is not a video of the actual web experience, but a reenactment. Moreover, these reenactments do not establish who visited the website; there must be proof that the individual in the "recording" doing the clicking was the consumer.

The business may offer an IP address, the consumer's contact information, and the time and date of the web visit. Even this may be bogus.

Depending on the type of website involved, there is a real chance the consumer did not in fact visit the website. Where a business (often called an "affiliate marketer") is paid by its business partner to drive customers to a website (via a blog or Facebook, etc.) and is paid for each lead, the affiliate marketer has a financial incentive to use bots and "human click farms" to create fictitious visits. Another way that a business can have the consumer's contact information and even IP address without the consumer having visited a particular site occurs where an intermediary (e.g., a lead aggregator) purchases consumer leads (contact information and IP address) from one website and sells them, manipulating the data to appear as if they originated from a different website.

These frauds, while indirectly injuring consumers, are primarily aimed at businesses buying the contact information from the fraudster. Such frauds occur so frequently that there is a whole industry hired by website owners to detect such fraud. *See* **FraudLogix**, **Anura**, and **this article**. An attorney explaining to a court the pervasiveness of this fraud may help the court credit a consumer's claim not to have visited the site. *See also* ***Fraudulent Web Traffic Continues to Plague Advertisers, Other Businesses***, Wall Street Journal, Mar. 8, 2018; ***Bot Form Fills are Destroying Lead Generation Industry. What Can Be Done?***, Performance Marketing Insider, Mar. 19, 2019; Digiday, **Confessions of a Lead-Gen Specialist**.

When investigating a claim that the consumers visited a particular website, begin by asking if they recall going to the website in question or if they had reason to do so—for instance, if the website promotes student loans, was the consumer even looking for such a loan in the first place? Further, check to see if the consumer's static IP addresses for the consumer's devices match the IP address provided by the company. While neither a match nor a non-match are conclusive, they will help to narrow down your investigation.

When investigating a purported consent data-set produced in a class action, indicia of lead fraud in the data set may be apparent. Special characters in the name/address fields (such as "*", "[", or "{") indicate that the data may have originated through bots or automated processes, rather than from an individual consumer visiting a website. Likewise, hundreds or thousands of records associated with the same IP address may indicate that the data associated with that IP address was originated by bots or automated processes as well. An expert can help identify fraudulent information.

Application to Arbitration Challenges

For a number of courts, consumers stating in affidavits that they did not visit the website or click the button in question may be enough to defeat a company's attempt to compel arbitration. This denial switches the burden to the party seeking to prove the validity of the contract, which requires proof that the consumer actually took the action (such as clicking the box) that is considered the electronic signature. Other courts will usually allow a trial under Federal Arbitration Act § 4 focused specifically on the question as to whether an arbitration agreement was formed. Either party can request a jury trial. The business would then need to produce a witness able to offer competent evidence about the unique IP address that accessed the website or accepted the terms and how the witness knows that action was taken by the plaintiff.

Difficulty of Producing Admissible Evidence As to the Consumer's Electronic Assent

As with any evidence, the business will have to meet its burden to produce evidence with a proper foundation that the consumer assented to the challenged terms and of the surrounding circumstances. Particularly in the case of website consent to telemarketing robocalls, it is unlikely that the telemarketing seller will own the website, but instead the seller or its agent will have purchased the consumer's contact information from an intermediary who purchased the information from another intermediary or the site owner. The seller seeking to enforce the website-assented term will have no first-hand knowledge of the site and cannot produce first-hand evidence as to the content of the site at the relevant time or the consumer's alleged assent.

In a TCPA class action, because the issue of consent must be resolved for all class members, the class may seek to prove no consent rather than have to argue that the seller cannot meet its burden for each class member. One approach may be to track down the site owner. This may be found on the website itself or subpoenaing the entity in whose name the domain or URL is registered. Seek from the site owner whether the consumers have consented to robocalls from the seller—the site owner may respond by disavowing any knowledge of the seller or the consumer.

Also demand information on the chain of transfer of the consumer's contact information and consent from the website owner all the way to the seller—there may be a number of intermediaries (e.g., lead generators, lead aggregators, or lead marketers) and the seller often cannot produce this evidence. The seller will have to show the integrity of the data—where it came from, how it was stored, and how it was maintained. Parties along this chain may disavow having any records related to the consumer.

Federal E-Sign Requirements Involving TCPA, Other Electronic Disclosures

Companies lure consumers to websites, seeking to obtain on the site the consumer's consent to telemarketing robocalls, not just from the website's owner, but from an array of companies that purchase the information from the website owner. There are a number of ways to overcome this

consent defense to a TCPA action in addition to those discussed above concerning the nature of the assent and proof of the identity of the party assenting.

The TCPA requires that the consent to telemarketing robocalls be in writing and contain a clear and conspicuous written disclosure of the implications of the written consent. *See* 47 C.F.R. § 64.1200(f)(8)(i)(A); **NCLC's *Federal Deception Law* § 6.3.4.1.2**. The federal E-Sign statute allows for electronic disclosures to replace such written disclosures to consumers only if the company first follows E-Sign's consumer consent provisions, requiring consumer disclosures and the consumer demonstrating the ability to access the information in electronic form. *See* 15 U.S.C. § 7001(c); **NCLC's *Consumer Banking and Payments Law* § 11.4**. For more on the TCPA and E-Sign, see **NCLC's *Consumer Banking and Payments Law* § 11.4.6**.

In other words, for the consumer's consent to telemarketing robocalls to be effective, *before* the consumer consents to robocalls, the website should first provide the consumer with E-Sign disclosures and the consumer should also first respond to those disclosures to show the consumer can access electronic disclosures. The same is the case with any other assent to terms where federal or state law require certain *written* disclosures prior to the consumer's assent.

Where TCPA Assent Must Be Linked to a Particular Seller

The TCPA requires that a consumer provide prior express written consent to receive telemarketing robocalls from the *seller*, i.e., the entity whose products or services are being sold. *See* 47 C.F.R. § 64.1200(f)(8). Consent found on a website not owned by the seller should be ineffective unless the consent clearly and conspicuously refers to the seller and not just to the website owner. It should not be enough for the consent provision to name the seller's agent (e.g., a "dialing vendor") or partner company that assists with the telemarketing—it should list the name of the seller. The "clear and conspicuous" disclosure required for prior express written consent may not be satisfied where the disclosure merely provides a hyperlink from the disclosure to a page that contains a list of hundreds of sellers. This is particularly the case where the seller listed bears no relationship to the website or the content advertised on the website.

If the TCPA consent disclosure language is not properly in electronic form, or does not adequately identify the seller, then the consent is not only ineffective for one consumer, but for all consumers who allegedly consented via that website. This is a powerful result for a TCPA class action.