Katten

KATTISON AVENUE

Advertising Law Insights From Madison Avenue and Beyond

Fall 2019 | Issue 1

Letter From the Editor

Welcome to the inaugural edition of *Kattison Avenue*, a newsletter examining the hot topics in advertising from Katten's office on Madison Avenue in New York City and beyond. As we prepared to launch our first issue, we wanted to highlight the dynamic nature of advertising law today, which not only encompasses traditional advertising issues, but also intellectual property, technology and privacy considerations. Advertising law has become an interdisciplinary practice that draws on the expertise of various specialties, which is evident in the breadth of our featured articles. Be sure to click on the blue hyperlinks throughout this newsletter for relevant and related content. We hope you enjoy our first edition and please look for us at the upcoming Association of National Advertisers/Brand Activation Association (ANA/BAA) Marketing Law Conference in San Diego on November 4–6.

Jessica Kraver

In This Issue

The Profit Motive: Supreme Court To Decide When an Infringer's Profits May Be Awarded to a Trademark Owner

by David Halberstadter

It is hardly uncommon for the manufacturers of one product to refer to another company's product in its advertisements and marketing materials. This frequently occurs under the label "comparative advertising;" examples include Pepsi referencing Coke during the companies' famous "Cola Wars" and Burger King's commercials, in which it compared its flame-broiled "have it your way" burgers to the "have it their way" burgers offered by McDonalds.

These uses of another's trademark are legally permissible; so, too, are so-called "nominative fair uses," in which one company uses another's trademark to describe the other company's goods or services rather than as a source-identifier for its own products. Examples include "We service Samsung appliances" and "Proudly serving Boar's Head deli meats." Another permissible use, often referred to as a "compatibility assurance," includes marketing statements such as "Our Printers Are IBM-Compatible."

But, sometimes, a company (or its public relations team) can go too far or get too clever, turning what might have been a legally defensible use of another's mark into potential trademark infringement and leading inevitably to litigation. In the 1990s, Weight Watchers International sued Stouffer Corporation, the maker of Lean Cuisine diet foods, for marketing its products with the statement "Stouffer's presents Weight Watchers exchanges for all 28 Stouffer's Lean Cuisine entrees." Stouffer was found to have infringed on Weight Watcher's trademark because this statement falsely implied Weight Watcher's endorsement of Lean Cuisine products.

In 2000, Pizza Hut sued Papa John's for advertisements in which Papa John's claimed that it had "won big time" in taste tests over

The Profit Motive: Supreme Court To Decide When an Infringer's Profits May Be Awarded to a Trademark Owner

Pizza Hut, and that its sauce and dough were better than Pizza Hut's because they were made with fresh tomatoes and filtered water and did not include ingredients like xanthan gum and hydrolyzed soy protein. Initially, a jury sided with Pizza Hut, finding Papa John's claims were false and misleading. A federal appellate court subsequently reversed the decision.

Finally, in 2018, film studio STX Entertainment launched an advertising blitz for its very adult-themed summer release, The Happytime Murders, starring Melissa McCarthy and a group of puppets designed by Brian Henson (Jim Henson's son). The advertisement made prominent use of the tagline "No Sesame. All Street." Sesame Workshop, the producer of the children's television series Sesame Street, did not take kindly to this marketing tactic and asked a federal judge to issue a temporary restraining order (TRO) requiring STX to discontinue the use of that tagline. The federal judge concluded that the tagline was legally permissible and denied the TRO request. Sesame Workshop dismissed its lawsuit several days later.

The Lanham Act provides several potential remedies for trademark infringement, including injunctive relief, recovery of the plaintiff's actual damages and, potentially, recovery of the infringer's profits. But the circumstances under which a trademark plaintiff is eligible for an award of the infringer's profits has been the subject of many conflicting district and appellate court decisions.

15 U.S.C. § 1117(a) provides, in relevant part:

When a violation of any right of the registrant of a mark registered in the Patent and Trademark Office, a violation under section 1125(a) or (d) of this title, or a willful violation under section 1125(c) of this title, shall have been established in any civil action arising under this chapter, the plaintiff shall be entitled, subject to the provisions of sections 1111 and 1114 of this title, and subject to the principles of equity, to recover (1) defendant's profits, (2) any damages sustained by the plaintiff, and (3) the costs of the action.

Section 1125(a) prohibits the use of "any word, term, name, symbol or device or false designation of origin that is likely to cause confusion or mistake or to deceive as to the affiliation, connection or association of a person with another person, or as to the origin, sponsorship, or approval of his goods." This is the section of the federal Lanham Act that covers most claims of trademark infringement and false advertising. Section 1125(c) prohibits the dilution of a famous mark by "blurring" (the whittling away of distinctiveness caused by the unauthorized use of a mark on dissimilar products) or "tarnishment" (an unauthorized use of a mark which links it to products that are of poor quality or which are portrayed in an unwholesome or distasteful context that is likely to reflect adversely upon the trademark owner's product). Section 1125(d) prohibits cyber-piracy.

The point of disagreement among the federal appellate courts is whether or not a plaintiff asserting a claim of trademark infringement under Section 1125(a) must make a preliminary showing that the defendant's actions were "willful" in order to be entitled to a disgorgement of the defendant's profits. The literal language of this section would appear to require willfulness only with respect to trademark dilution claims, not trademark infringement or cyber-piracy. But the circuit courts that have found willfulness to be a prerequisite, even for trademark infringement under Section 1125(a), have relied on other portions of the statute, its legislative history and various amendments to interpret this section and apply this remedy only upon finding that the defendant acted willfully.

In fact, there is a relatively even split among the federal circuits on this issue. The Third, Fourth, Fifth, Sixth, Seventh, and Eleventh Circuits do not require plaintiffs to show that the infringement was willful before considering whether to award them profits as a remedy to trademark infringement. These appellate courts consider proof of willful infringement to be an important factor, which must be considered in balancing the equities when determining whether an accounting of profits is appropriate, but not an essential predicate to such an award.

By contrast, the Second, Eighth, Ninth, Tenth and DC Circuits interpret the Lanham Act as requiring plaintiffs to make a threshold showing of the defendant's willful infringement before the plaintiffs are permitted to litigate their entitlement to recover profits. The First Circuit also requires a showing of willfulness but only in cases where the plaintiff and defendant are not direct competitors.

Whether the Lanham Act is properly interpreted as making willfulness a prerequisite to an award of profits or merely one of the important factors to be considered in the analysis, the current disagreement among the federal circuits has led to unpredictability and differences in outcomes depending upon the circuit in which a trademark infringement action is filed. So, companies with substantial trademark portfolios, that both seek to enforce their intellectual property rights and are called upon to defend trademark claims filed by others, cannot reliably evaluate the risks associated with potential trademark litigation, whether they are the plaintiff or the defendant in any given situation.

Fortunately, the United States Supreme Court has agreed to resolve this split among the federal circuits. On June 28, the court granted the plaintiff's petition for a writ of certiorari (i.e. it agreed to review the appellate court's decision) in *Romag Fasteners Inc. v. Fossil Inc.*, Docket No. 18-1233 (Docketed March 22, 2019).

In its petition for certiorari, Romag argued that it is often challenging for a trademark infringement plaintiff to prove that it has sustained actual, monetary damages as a result of the alleged infringement. Accordingly, claimants often seek in the alternative the disgorgement of any profits of the defendant that are attributable to the alleged infringing use of the claimant's trademark. It contended that the "deep and even split" among federal circuit courts on the necessity of finding willfulness by the defendant as a prerequisite to an award of profits has thwarted the uniform application of federal trademark law. Moreover, the frequency with which courts apparently grapple with this question amplifies its importance.

Fossil opposed Romag's petition for *certiorari*. It acknowledged that the various federal circuit courts applied different standards to determine whether an accounting of a trademark infringement defendant's profits is justified, with some courts holding that "principles of equity" make willful infringement a prerequisite and others considering willfulness only an important factor. Nevertheless, Fossil argued, in practice both standards result in willful infringers disgorging their profits and non-willful infringers not having to account for their profits. Fossil asserted that it was unnecessary for the Supreme Court to consider this issue because "the overwhelming majority of cases result in an accounting when the infringement was willful and [are] denied when it was not."

As is typical, the Supreme Court offered no explanation why it granted Romag's petition. But it is now clear that, one way or the other, there will be a uniform, standard test applied to this important trademark issue.

Cookie Sales Aren't Limited to Girl Scouts: When Advertising Cookies[1] are "Sales"

Personal Information Under the CCPA

By Dagatha Delgado

Advertising cookies[2] have become an important way for businesses to deploy online advertising campaigns, target audiences and increase advertisement revenue. The technology can track an individual's behavior on a website and/or across the internet (e.g., websites and webpages visited, scrolls, clicks, etc.) in order to understand the individual's habits and preferences to customize advertisements based on the individual's interests. Use of such technology may constitute a "sale" of personal information under the California Consumer Privacy Act of 2018 (CCPA).

Sale of personal information

The CCPA's definition of "sale" includes "making available" personal information[3] to a third party for "monetary or other valuable consideration."[4] On its face, this definition would appear to include third-party advertising cookies, which generally involve a business inserting code onto its website to enable the placement of third-party tracking cookies on the website. By inserting such code, a business makes personal information available to the third party via the third-party cookie. In exchange for "making available" this information to the third party, the business, among other things, improves advertising campaigns (and presumably increases revenue) – valuable consideration.

"Sale" exceptions

The CCPA provides certain exceptions to transfers being "sales," if certain conditions are met. Personal information shared with "service providers" does not constitute a "sale," if the information is necessary for a business purpose, the business notifies the individual, and a written agreement is in place prohibiting the provider from (1) selling the information, and (2) retaining, using or disclosing the information (i) for any purpose (including commercial purposes), except to perform the contract and (ii) outside the direct business relationship.[5] Given the different types of cookies and parties involved in online advertising,[6] meeting those conditions in the current environment is difficult, at best. For instance, behavioral advertising networks may retain cookie information in their networks to benefit other members in the network.[7]

The CCPA also exempts from "sales" transfers when an individual "uses or directs the business to intentionally disclose personal information or uses the business to intentionally

interact with a third party," provided the third party does not then sell the information.[8] An individual who consents or opts-in to advertising cookies might be considered to have used or directed a business to disclose personal information or interact with a third party. An "intentional interaction" occurs when an individual intends to interact with a third party via a deliberate action — hovering, muting, pausing or closing content (e.g., cookie pop-up notices) do not qualify as intent to interact with a third party.[9] Note, however, that a business could be liable for a third party that "sells" information (inconsistent with the CCPA), if the business had actual knowledge or reason to believe the third party intended to "sell" the information, as the business did not have an appropriate contract in place.[10] Unfortunately, as a general matter, cookie providers' terms and conditions do not generally specify how or what information may be disclosed, so it is challenging for a business to determine what the service providers may be doing with cookies.

Obligations for "sellers"

Assuming the use of advertising cookies is a "sale," a business deploying third-party cookies will have to comply with the obligations imposed on "sellers" of personal information. The CCPA requires that a business disclose in its website privacy notice the personal information it has sold in the last 12 months and the types of third parties to whom it was sold.[11] The California Attorney General's (AG) proposed California Consumer Privacy Act Regulations also require a "Notice of Right to Opt-Out" that must include:

1. A description of an individuals' right to opt-out;
2. A web form for submitting opt-out requests online via a clear and conspicuous "Do Not Sell My Personal Information" link, or an offline method for submitting opt-out requests;
3. Instructions for any other method for submitting opt-out requests;
4. Any proof required when an individual uses an authorized agent to exercise opt-out rights, or in the case of offline notices, a URL where individuals can find information about authorized agents;
5. A link to the business' privacy notice; and
6. Information on how a consumer with a disability may access the notice in an alternative format.[12]

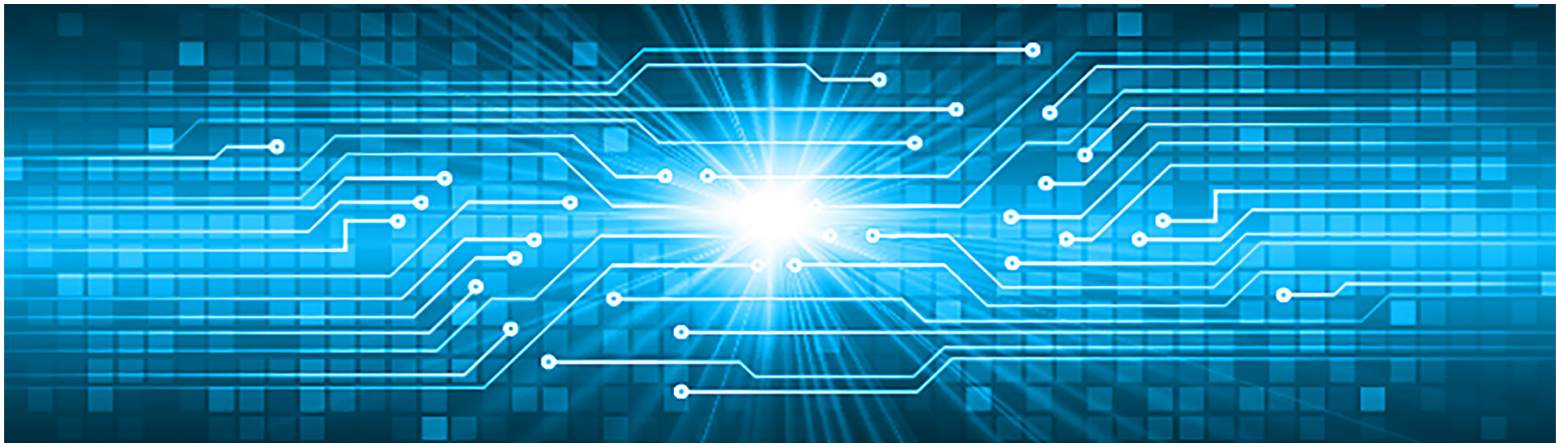
Additionally, the CCPA requires that a "Do Not Sell My Personal Information" link be placed in a business' privacy notice and on its website "homepage" (meaning the homepage and any page personal information is collected)[13] that enables individuals to opt-out of "sales."[14]

Over the last few years, some companies have implemented cookie management tools on their websites to allow individuals to set their cookie preferences (and opt-out of advertising cookies). However, such tools may fall short of CCPA compliance with respect to "sales." Under the CCPA, a business that receives an opt-out request must refrain from "selling" the individual's information without subsequent "express authorization" and must wait 12 months before asking the individual to reauthorize the sale or accept cookies.[15] Cookie preferences are typically saved on the browser on which preferences were set. An individual that clears the browser's cache, or uses a different browser or device to access the website, may be asked again to accept cookies (violating the 12-month waiting period).[16] Where a business has enabled advertising cookies, it risks violating the restriction on "selling" the information after having received an opt-out request.

IAB (draft) framework

The Interactive Advertising Bureau (IAB) has proposed an approach to help businesses that participate in Real-Time Bidding (RTB) transactions meet their obligations under the CCPA through its draft CCPA Compliance Framework for Publishers & Technology Companies.[17] The Framework would require certain disclosures be made, and contemplates creating a limited service provider relationship with downstream technology companies when an individual opts-out of the "sale" of personal information. Companies can participate in the Framework by signing the IAB Limited Service Provider Agreement.[18]

To help meet the CCPA and Regulations "sale" notice obligations, the Framework would require publishers that participate in the Framework to implement the required "Do Not Sell My Personal Information" link, and to provide explicit notice relating to programmatic advertising transactions; otherwise, the publishers will have to preset all individuals as having opted-out, thereby indicating that it does not "sell" personal information.[19] In addition to the information required by the CCPA and Regulations, the explicit notice must include an explanation that the opt-out is at a device level and describe how individuals can opt-out across different devices.[20] The explicit notice requirement may help alleviate the issue of inadvertently "selling" the personal information of an individual that previously opted-out on one device and later accessed a website on a different device.



The Framework would also help businesses meet the conditions necessary to satisfy the CCPA's service provider exception in the event an individual opts-out of the "sale" of their personal information. When an individual opts-out, a signal is sent to all "Downstream Participants" (i.e., SSPs, DSPs or ad servers that participate in the Framework) engaged in the RTB transaction; in return, most Downstream Participants would become limited service providers under the IAB Limited Service Provider Agreement.[21] Under the Agreement, the Downstream Participants cannot use or disclose personal information received from Digital Properties, except to perform certain business purposes (to the extent permitted by the CCPA)[22] applicable to their role in the RTB process and on behalf of the Digital Properties.[23]

Conclusion

Many questions remain on how CCPA impacts online advertising. To avoid potential liability, businesses should assess their online advertising activities and use of cookies. Terms and conditions of any third-party cookies should be carefully reviewed, and businesses should seek to confirm whether the third party intends to use or share the information for its own purposes. Businesses should ensure that it complies with the requirements for "sales" of personal information, and consider whether an exemption applies (service provider or consent).

---

1 For purposes of this article, we refer to cookies, the same holds for similar tracking technologies.

2 See All About Cookies, https://www.allaboutcookies.org/. Website cookies are a small data file that are stored onto an individual's browser or device when an individual accesses a website. Session cookies are stored until a browser is closed, and are typically used to "remember" an individual's activities on the website (e.g., online shopping cart). Cookies that are stored for longer periods are persistent cookies, and these generally remain on a browser after the browser has been closed. Persistent cookies "remember" the actual individual (i.e., the individual's browser/device). Cookies can be placed, read, and/or written to by the business that operates the website (first-party cookies) or by other third parties (third-party cookies).

3 Advertising cookies could fall under a number of categories of personal information, including the following: unique identifiers (a persistent identifier used to recognize an individual or device, over time and across different services, including "cookies, beacons, pixel tags, mobile ad identifiers, or similar technology"); internet activity (browsing history, search history, and information about interactions with a website, application, or advertisement); or even "inferences" to create a profile about the individual's preferences, characteristics, behavior, etc. See Cal. Civ. Code. § 1798.140(o)(1)(A), (F), (K), (x).

4 Cal. Civ. Code § 1798.140(t)(1) (emphasis added).

5 Cal. Civ. Code § 1798.140(t)(2)(C), (v), (w)(2)(A).

6 For example, advertisers, publishers, ad networks, ad exchanges, data management platforms (DMPs), demand side platforms (DSPs), and supply side platforms (SSPs).

7 David Zetoony et al., *California Consumer Privacy Act (CCPA): Answers to the Most Frequently Asked Questions Concerning Cookies and AdTech 13* (2019) (available at https://www.bclplaw.com/en-US/thought-leadership/answers-to-the-most-frequently-asked-questions-concerning.html).

8 Cal. Civ. Code § 1798.140(t)(2)(A).

9 Cal. Civ. Code § 1798.140(t)(2)(A).

10 Cal. Civ. Code § 1798.140(w)(2).

11 Cal. Civ. Code § 1798.120(b).

12 Cal. Code Regs. tit. 11, § 999.306(a)(2)(d), (c) (proposed Oct. 11, 2019) (to be codified at Cal. Code Regs. tit. 11, § 999.300). Note: As of writing this article, the California Attorney General proposed California Consumer Privacy Act Regulations are open for public comment until December 6, 2019.

13 Cal. Civ. Code § 1798.140(l).

14 Cal. Civ. Code § 1798.135(a)(1)-(2).

15 Cal. Civ. Code §§ 1798.120(d), 135(a)(5).

16 Zetoony et al., *supra* note 7, at 22.

17 *Interactive Advertising Bureau, LLC., CCPA Compliance Framework for Publishers & Technology Companies* (Draft for Public Comment) (Oct. 2019) (hereinafter, "IAB Framework"). Note: As of writing this article, the IAB Framework is open for public comment until November 5, 2019.

18 IAB Framework, at 4.

19 IAB Framework, at 7-8.

20 IAB Framework, at 7-8.

21 IAB Framework, at 9.

22 Permitted business purposes under the CCPA include, but are not limited to, the following: (i) counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards; (ii) protecting against malicious, deceptive, fraudulent, or illegal activity; (iii) short-term, transient use, provided the personal information is not disclosed to another third party and is not used to build a profile about an individual or otherwise alter an individual's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction; and (iv) providing advertising or marketing, analytic, or similar services on behalf of the business or service provider. See Cal. Civ. Code § 1798.140(d)(1), (2), (4), (5).

23 IAB Framework, at 9, 13.

Takeaways From the 2019 National Advertising Division Annual Conference

By Michael Justus

Katten sponsored the 2019 National Advertising Division (NAD) Annual Conference in New York City on September 23rd and 24th. In addition, Katten Intellectual Property partner Michael Justus served on the Planning Committee for the conference and moderated the panel, "How to Walk with the Tech Giants." Michael provides his key takeaways from the conference below.

Having reflected on another enlightening NAD Conference, I'm pleased to share some of my key takeaways and favorite moments below.

Deep thoughts on mobile content

In a dynamic keynote presentation, global head of Twitter ArtHouse Stacy Minero used engaging examples of viral ad campaigns to prove that the role of mobile advertising has definitively shifted from merely a "second screen" to the primary launch pad for new campaigns. Ms. Minero also demonstrated why savvy brands engaged in influencer marketing have shifted their focus from influencers with the biggest followings to influencers who can most authentically connect with the target audience. Similarly, brands are focusing less on mobile content that grabs fleeting moments of users' attention and more on content that triggers lasting emotional connections and fosters long-term relationships between the consumer and the brand.

A celebrity, a dog and a computer-generated image walk into a bar

The "How to Walk with the Tech Giants" panel — which I moderated — covered the latest NAD and Federal Trade Commission (FTC) developments relating to influencers and customer reviews. An overarching theme throughout the panel was the well-established principle that endorsements from influencers, consumer reviews and otherwise must adequately disclose the relationship between the endorser and the brand. Perhaps my favorite moment was the panelists' discussion of non-human influencers like Menswear Dog (a handsome pup that wears men's clothing in partnership with clothing brands) and computer generated imagery (CGI) influencers like Lil Miquela (a very real-looking computer image of a woman that partners with fashion brands and others). One interesting point of discussion was whether a CGI influencer, who is not real, can lawfully endorse a product when he/she/it has not actually tried the product.

The panelists also discussed a number of recent cases that help draw some lines around what level of responsibility advertisers bear for customer reviews and other third-party endorsements and claims. For example, in *Advanced Purification Engineering Corporation (Water Filter Systems)*, Report #6238, NAD/CARU Case Reports (January 2019), NAD determined that the advertiser did not exercise sufficient control over the content of Amazon customer reviews to be responsible for unsupported "Made in USA" statements in the reviews. On the other hand, in *T-Mobile USA, Inc. (T-Mobile Wireless Services)*, Report #6234, NAD/CARU Case Reports (December 2018), NAD held that T-Mobile must have substantiation for customer tweets reposted by T-Mobile that compared objectively provable attributes of T-Mobile and AT&T services and conveyed a typicality message. Although this area of the law is developing and some questions remain, it is clear from these cases that advertisers should ask themselves whether they have taken any steps to repost, promote or exercise control over third-party posts.

Self-regulate and carry a big stick

As usual, speakers from NAD and FTC reiterated their ongoing cooperation and FTC's support for the NAD self-regulatory process. NAD is, of course, a self-regulatory forum that cannot issue legally binding injunctions. But NAD does carry a big stick by way of FTC's willingness to step in and investigate parties to NAD proceedings that choose not to follow NAD's recommendations. This year, NAD pointed to the recent *Implus Footcare, LLC* Matter, in which FTC's investigation after a referral from NAD led to the advertiser agreeing to also cease additional claims that were not even at issue in the underlying NAD proceeding. The clear message from NAD is to think twice before shrugging off its recommendations as "non-binding."

Overall, the 2019 NAD Annual Conference was engaging and informative, and I'm already looking forward to the 2020 conference.

When Website Social Media Plugins Need to Comply Under EU Data Protection Law

By Dagatha Delgado

EU Data Protection Laws Unplug Social Plugins

Website social media plugins have become increasingly popular over the last few years. Social plugins offer businesses a way to promote their products or services and increase traffic to their websites. However, a recent European court decision found that website operators implementing these technologies could be liable for compliance with EU data protection law.

The Fashion ID case

On July 29, the Court of Justice of the European Union (CJEU) found a German online clothing retailer, Fashion ID, to be liable under the EU Data Protection Directive[1] as a "joint controller"[2] for embedding a social media plugin, the Facebook "Like" button, on its website.[3] The functionality of the button caused the personal data (IP address and browser user agent string) of Fashion ID's website visitors to be automatically shared with Facebook as soon as visitors accessed the website. Notably, the plugin collected and transmitted this information even if a visitor was not a Facebook member or has not clicked on the "Like" button.

Under the Directive, a "controller" is defined as the "natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data."[4] The CJEU found that Fashion ID determined, jointly with Facebook, the purposes and means of the processing (i.e., the collection and disclosure) of personal data. In this case, Fashion ID consented (at least implicitly) to the collection and disclosure of personal data for the purpose of "benefit[ting] from the commercial advantage consisting in increased publicity for its goods," as the "Like" button allows Fashion ID to "optimise the publicity of its goods by making them more visible" on Facebook.[5] Fashion ID jointly determined the means of processing as it "exert[ed] a decisive influence over the collection and transmission of the personal data" by embedding the social plugin on its website.[6]

Consequently, Fashion ID's status as a joint controller required that it comply with the obligations imposed on data controllers under EU data protection law. Specifically, the court held that a website operator, such as Fashion ID, that implements social plugins that collect and disclose personal data to the plugin provider, is responsible for complying with (1) the duty to inform individuals of its data processing activities, and (2) the obligation to establish a lawful basis[7] for processing personal data, as required under EU data protection law. Where a website operator relies on a visitor's consent to process personal data using a social plugin, the operator (not the plugin provider) is responsible for obtaining the visitor's consent prior to such processing. However, the court

November 4-6, 2019 ANA/BAA Marketing Law Conference

Katten is proud to be a sponsor of the annual ANA/BAA Marketing Law Conference to be held at the Marriott Marquis San Diego Marina on November 4-6, 2019. This event will provide hands-on legal and practical guidance in marketing, advertising and privacy law. Over 160 of the top legal minds will discuss new forms of content, new platforms, new markets and the challenges these changes present, as well as how to overcome them. Doron Goldstein and Kristin Achterhof, co-chairs of the Advertising, Marketing and Promotions practice, will be in attendance. Doron will also be a speaker on a panel entitled, "Global Privacy: Managing Tracking & Other Consumer Preferences," on November 4.

Doron S. Goldstein
Partner
doron.goldstein@katten.com

Kristin J. Achterhof
Partner
kristin.achterhof@katten.com

clarified that Fashion ID's role as a joint controller is limited to processing personal data for which it is actually capable of determining the purposes and means of processing; that is, a website operator is not responsible for what the plugin provider, such as Facebook, does with the data after it has been transmitted.[8]

Applying CJEU's findings to GDPR

While the CJEU analyzed the Fashion ID case under the requirements of the Directive, the court's findings and interpretation of the scope of joint controller responsibilities are applicable to the General Data Protection Regulation (GDPR or Regulation), which has since repealed and replaced the Directive. The GDPR imposes similar obligations on controllers, including, inter alia, the duty to inform individuals, the obligation to establish a lawful basis and, when applicable, the obligation to obtain valid consent prior to processing personal data.

However, the GDPR introduces additional responsibilities, specifically for joint controllers. Article 26 of the Regulation requires that joint controllers determine, in a transparent manner, their respective responsibilities for compliance with their obligations, unless their respective responsibilities are determined by EU law or EU member state law. The Regulation also states that joint controllers must also develop an "arrangement" that reflects each controller's roles and responsibilities and requires that the "essence of the arrangement" be made available to data subjects (i.e., website visitors). Finally, the GDPR permits data subjects to exercise their rights in respect of, and against, each controller.

Key takeaways

Despite the marketing and promotional benefits social plugins may provide, businesses should be mindful of the implications of these third party features. Notably, social plugins that automatically transmit personal data to the plugin provider may impose obligations on website operators as controllers under EU data protection law. Accordingly, website operators that have embedded social plugins or other third party technologies should verify what data, if any, is collected and transmitted from the plugins or other technologies, be sure to understand how the technologies operate, and be aware of what obligations may arise by virtue of implementing those technologies. Website operators should revise their privacy notices, as necessary, to accurately reflect their data processing activities and to disclose their joint-controller relationships, if applicable. Importantly, website operators should ensure an appropriate legal basis exists for processing personal data.

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, "Directive").

2 The Directive defines a "controller" as the "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."

3 Judgment of 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, C-40/17, EU:C:2019:629 (available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=D3397DD88DEA1C9E0F300C16ED907248?text=&docid=216555&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=13652906) (hereinafter, "Fashion ID").

4 Directive, Article 2(d).

5 Fashion ID., para. 80. Facebook's purpose for processing the personal data was for its own economic interests, "as it can use those data for its own commercial purposes." Fashion ID., para. 80.

6 Fashion ID., para. 77. Facebook jointly determined the means by making the plugin available to website operators while "fully aware of the fact that it serves as a tool for the collection and disclosure of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook." Fashion ID, para. 77.

7 As mentioned, the CJEU analyzed the Fashion ID case under the Directive, which has since been repealed and replaced by the General Data Protection Regulation ("GDPR"). Article 7 of the Directive provides that personal data may only be processed if at least one of six criteria are met (i.e., consent, contractual obligation, legal obligation, legitimate interest, vital interest, public interest), all of which align to the legal bases enumerated in Article 6 of the GDPR, which requires that controllers establish a legal bases in order for processing to be lawful. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6 (hereinafter, "GDPR").

8 Fashion ID., para. 76, 85.

Katten

For more information, contact: Jessica Kraver
Associate | Intellectual Property Department | Katten Muchin Rosenman LLP
+1.212.940.6523 | jessica.kraver@katten.com | 575 Madison Avenue | New York, New York 10022