Katten

KATTISON AVENUE

Advertising Law Insights From Madison Avenue and Beyond

Fall 2022 | Issue 9

Letter From the Editor

Welcome to the season of crisp air, pumpkin flavored everything and the fall edition of *Kattison Avenue*. What started as a seemingly routine privacy policy update for TikTok may be a bellwether for companies who run afoul of personal data protections. Associate Cynthia Martens spoke with legal experts in Italy to examine the influence of Italy's data privacy protection authority, the Garante per la Protezione dei Dati Personali, and how it and other privacy agencies are coordinating to crack down on and increase penalties for privacy violations. Fresh from the National Advertising Division (NAD) annual conference, Partner Mike Justus explains why lawyers and brands will need to get creative when placing required disclosures in the metaverse. Partner David Halberstadter focuses in on the latest developments in the *1-800 Contacts v. Warby Parker* infringement dispute. While the case hasn't yet set precedent, it's one to watch, especially for online retailers protecting and competing against well-known brands. Finally, in preparation for the sunsetting of certain exemptions for business-to-business and human resources data under the California Consumer Privacy Act on January 1, Katten's privacy practice flags key issues for businesses that will need to review and likely update their data privacy compliance processes by the end of the year. We hope you enjoy the issue and invite you to connect with any of us to discuss developments in advertising law.

Jessica G. Kraver

#tiktokcringe: Targeted Ads Are No 'Legitimate Basis' for Data Processing, Says Italy's Data Privacy Protection Authority

European data authorities are increasingly united in policing data and privacy violations

By Cynthia Martens

It began, innocently enough, with an update to TikTok's privacy policy. Via upbeat messaging, users learned that they would soon receive "personalized" advertising based on their activities on the trendy video platform, now the world's most downloaded app for those aged 18 to 24, who even use it as a search engine.

But on July 7, Italy's data privacy protection authority, the Garante per la Protezione dei Dati Personali (Garante), issued a sharply-worded ruling against Tik Tok, warning that using personal data automatically archived on users' devices to send them targeted ads is illegal without the users' explicit consent.

In This Issue

Targeted Ads Are No 'Legitimate Basis' for Data Processing, Says Italy's Data Privacy Protection Authority

Is the Metaverse a Giant 'Native Advertisement'?

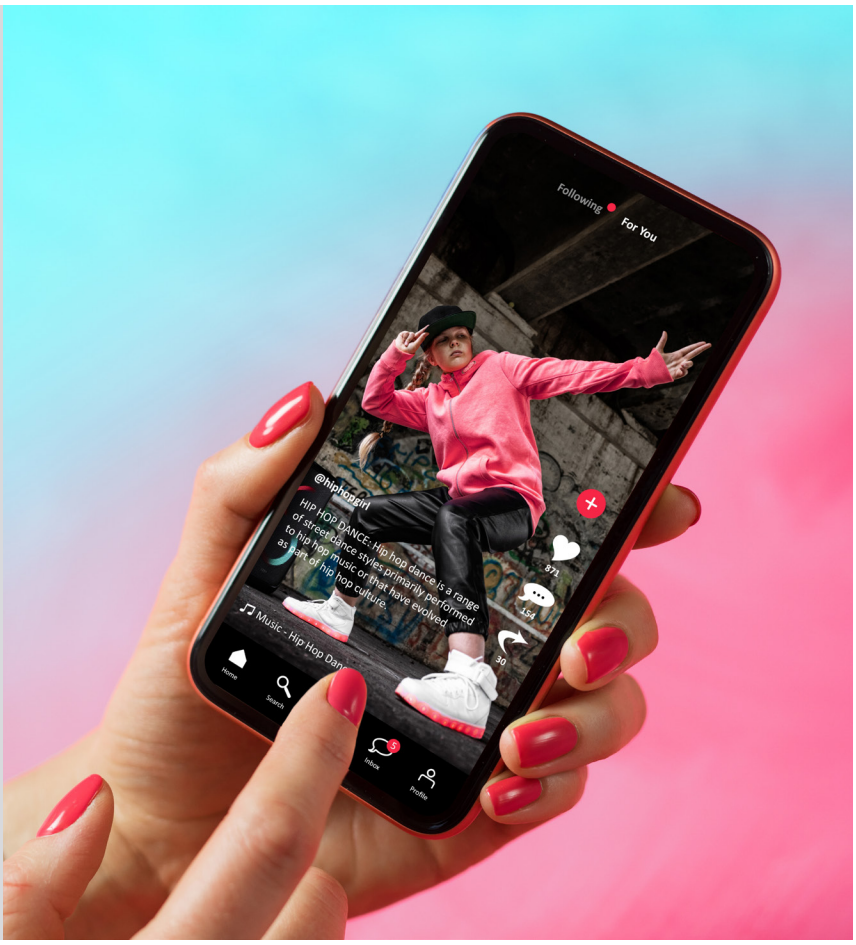
Warby Parker Beats Back 1-800's Infringement Claims

California Consumer Privacy Act's Employee and B2B Exemptions to Expire on January 1

News to Know

ICO: TikTok Data Processing Violates UK Law

The United Kingdom's Information Commissioner's Office (ICO) released a statement on September 26 describing provisional findings that TikTok had breached UK data protection law between May 2018 and July 2020, exposing the company to a £27 million fine. According to ICO investigations, TikTok may have "processed the data of children under the age of 13 without appropriate parental consent, failed to provide proper information to its users in a concise, transparent and easily understood way, and processed special category data" — comprising ethnic and racial origin, political opinions, religious beliefs, sexual orientation, union membership, genetic and biometric data or health data — "without legal grounds to do so." – Cynthia Martens



American companies, take note: alongside its counterparts in other European Union member states, the Italian Garante is a powerful legal entity, a collegiate body with departmental branches dedicated to fields such as health, human resources, marketing, freedom of expression and cyberbullying, among many.

"Its investigative powers are quasi absolute. It is even above state secrets. But, at the same time, its inspection and enforcement activities are limited to the realm of personal data violations. That always has to be the spark that lights the fuse," said Pierluigi Perri, an Italian lawyer and professor at the University of Milan with expertise in data protection and web surveillance.

Outside the TikTok ruling, the Garante has drafted guidelines on the use of cookies and other tracking tools; penned a general application order concerning biometrics; issued a general injunction regarding "silent calls," or unsolicited telephone calls in which individuals answer their phones but are not put through to any speaker; and commented on the legality of vehicle geolocation in the context of employer-employee relations.

Headquartered in Rome, the Garante has an advisory function, working with the Italian Parliament to ensure new laws comply with data protection legislation and making recommendations to various executive branches of government. It also has the authority to impose administrative sanctions and accessory sanctions, which could include an order to stop processing data — a move that would send shivers down the spines of social media executives. On the other hand, the Garante cannot issue criminal sanctions; it can only refer crimes to the prosecutor's office. And it cannot order the payment of damages. Individuals seeking redress for data privacy violations may go to court or to the Garante, but they cannot do both.

The ability of advertisers to purchase web data and target individual consumers has been of special concern to lawmakers, and Europe has been ahead of the curve on privacy legislation, much to the chagrin of Silicon Valley. Since the European Union adopted the General Data Protection Regulation (GDPR) in 2016, the European Data Protection Board (EDPB) has worked to ensure its consistent application throughout the European Union.

TikTok had cited "legitimate interest" under the GDPR as the legal basis for its data processing and advertising practices. The facts, however, suggested to the Garante "that TikTok's choice is merely instrumental to achieving its own goals, whereas the legitimate basis for data collection appears to be of secondary importance, adaptable to the circumstances," as stated in the ruling.

Pasquale Stanzione, president of the Garante, law professor and one of Italy's leading authorities on privacy and consumer protection, authored the TikTok opinion. In an interview for Kattison Avenue, he acknowledged that "using 'legitimate interest' as a lawful premise for data processing requires an undoubtedly complex, fact-specific analysis." In addition to reiterating that consent was the only appropriate basis for TikTok's proposed processing of personal data for targeted advertising, he expressed concerns over the platform's attractiveness to minors, noting that the limits of current age verification tools mean that targeted advertising "could reach the youngest users, including with inappropriate content."

Exactly what a "legitimate basis" *is* in this context continues to ruffle feathers in Europe. Article 6 of the GDPR allows for the processing of personal data only if and to the extent that at least one of six conditions applies, including the catch-all that processing is necessary "for the purposes of the *legitimate interests* pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

"Legitimate interest is what I tell my students is the unicorn of privacy because it's hard to understand exactly what it is," Prof. Perri said during an interview for *Kattison Avenue*. "It's a legal doctrine that allows one party to process the other's data on the basis of mutual interest. So, we're both benefiting without saying anything — there is no contract, no need for anything formal and the data processing can go ahead without explicit consent." He cited prevention of fraud or a pre-existing commercial relationship between the parties as textbook examples.

From a commercial advertising perspective, of course, consent is less valuable than legitimate interest because internet users can withdraw their consent at any time. As one *Harvard Business Review* writer noted, "One of the biggest pain points in the era of consent is the potential loss of data."

According to Eurostat, the statistical office of the European Union, in the decade between 2011 and 2021, the share of European households with internet access rose from 72 percent to 92 percent, with highest access levels reported in urban areas. One of the most common online activities in Europe in 2021 was social networking. Eurostat also reported that 53 percent of all European internet users had refused to allow the use of their personal information for advertising, while 39 percent claimed to read privacy policy statements before providing personal information. Awareness of online tracking via cookies was especially high — 86 percent — among European internet users aged 16 to 24.

Prof. Perri said European consumers, broadly speaking, are more concerned about the use of their personal data by corporations

than by the government, whereas worries run in the opposite direction in the United States.

In addition, the philosophical framing of data privacy rights has led to different legislative approaches in Europe and the United States. Whereas US laws frequently anchor privacy to personal choice, he said European law centers on "protecting personal dignity" and a "strong notion of privacy as a fundamental right" found in Articles 8 and 9 of the *Charter of Fundamental Rights of the European Union*. Because fundamental rights are non-negotiable, European lawmakers tend to view with suspicion the use of personal data for advertising and marketing or even as payment for services.

"The European Union showed extraordinary foresight in its understanding, back in 1996, of the importance of legislation protecting individuals with respect to the increasingly pervasive processing of their personal data," Prof. Stanzione said, noting that the lack of regulation of the internet early on led to a dramatic power imbalance between large corporations and consumers. He described the GDPR as a "broad, futureproof legal framework" that sought to withstand the inevitable evolution of technology, adding that a robust protection for internet users can only stem from their freely given, specific, unambiguous and informed consent to data processing. "One of the greatest successes of [European] privacy law has been increasing public awareness of the importance of protecting our freedom by protecting our data," he said.

Despite its sweeping authority, from the outset, the Garante has suffered from a lack of resources. "Already my predecessors publicly complained about the lack of funding allocated to the Garante considering its duties, especially when compared to other European authorities and even other Italian authorities," Prof. Stanzione said. While a 2021 legislative degree offered some relief, Stanzione said the entity is in urgent need of greater staffing as privacy and data protection issues proliferate. "Just consider that only a few staffers are assigned to work on telemarketing matters," he noted.

Through a protocol agreement in 2002 that was most recently renewed in 2021, Italy's tax police, the Guardia di Finanza (known as the GdF), has assisted the Garante in carrying out inspections. Prof. Stanzione said the GdF's support has been crucial, given the Garante's limited resources and the fundamental rights it is charged with protecting.

Disparities in member-state resources notwithstanding, advertisers and other data processors should recognize the increasingly powerful cohesiveness of European data authorities. Prof. Stanzione referred to such cooperation as "the defining feature" of European privacy law, despite the fact that it is time-consuming, a challenge given "the short time frames that characterize the relationship dynamics between users and platforms in our digital society."

He expressed confidence in Europe's Digital Services Act package, composed of the Digital Services Act and Digital Markets Act, which is in the final stages of approval after its formal adoption by the European Parliament this summer. With the European Council's stamp of approval, the package will enter into force 20 days after the underlying acts are published in the Official Journal this fall.

"Both of these measures move in the direction of a much-needed adaptation of consumer protection to the unique demands of a constantly evolving digital reality, by providing users with a range of tools to proactively exert broader control over their data," he said. "At the same time, they reinforce the obligations — of disclosure, loyalty, honesty, but, more generally, responsibility — of platforms, aiming to align freedom of expression, freedom of economic initiative and the protection of fair competition, while also shielding users from improper uses of their personal data."

Prof. Perri noted that the EDPB is now discussing parameters for administrative sanctions by member-state data protection authorities to promote greater uniformity. He also said that there has been effective coordination among the entities in issuing sanctions related to use of "cookie walls," which prevent users from accessing services unless they consent to share their data. The EDPB took a stand against cookie walls in 2020.

TikTok, meanwhile, has hit pause on that privacy policy update.

Is the Metaverse a Giant 'Native Advertisement'?

A bigger question may be: how do companies prominently disclose ad content in a limitless space?

By Michael Justus

The metaverse virtual world is a shiny new sandbox for brands to play in. Just as sponsored content dominates social media, so too will advertising blanket the metaverse. Platform terms and features for branded content on social media is quite developed, but that is not yet the case for the metaverse. As affirmed at the 2022 National Advertising Division (NAD) Annual Conference, the traditional laws and regulations apply in the metaverse.

For example, advertising must be identified as such, and must not be disguised as some other type of content. Per the FTC's "native advertising" guidance, it is deceptive to present advertising as something else, "[b]ecause knowing that something is an ad likely will affect whether consumers choose to interact with it and the weight or credibility consumers give the information it conveys." Native advertising issues generally come down to disclosures. For example, an "ADVERTISEMENT" disclosure at the top of a sponsored magazine article, or "#sponsored" in an influencer's social media post. While the traditional disclosure requirements apply in the metaverse, the FTC announced its plans to update its ".com Disclosures" guidance with respect to games and virtual reality.

Native advertising is a central issue in the metaverse. Because of the vast interactive nature of a virtual world, it can be difficult for users to distinguish ad content from other content. Users of virtual reality hardware, such as the Oculus headset, can move and look wherever they want, which affects strategic placement for legal disclosures. This leads to a paradox: the traditional issue with disclosures is squeezing them into limited space, while in the metaverse the issue is making disclosures unavoidable in limitless space. Further, the metaverse audience can skew younger, and it may be more difficult for younger users to distinguish ads or influencer endorsements from other content.

Influencers in the metaverse may look just like other avatars. Branded content could be one small item in a vast virtual world, like a single virtual product. An entire virtual world may be a brand activation, such as Axe body spray's "Mistaverse" campaign on Fortnite. The metaverse activation featured a capture-the-flag game on the Fortnite gaming platform, promoted by a popular gaming influencer. Players could obtain "Med Mist" healing spray dispensed from a spray can. The "Mistaverse" included a virtual billboard-style disclaimer stating, "The greatest advertisement you will ever play. Our legal team told us to write this."

AXE Presents: Enter the Mistaverse

Ultimately, the legal question is how to disclose advertising content in an interactive virtual space so that users recognize it as advertising. The intertwined marketing issue is how to do so without ruining the effectiveness and authenticity of the content. Legal and marketing teams will need to get creative.

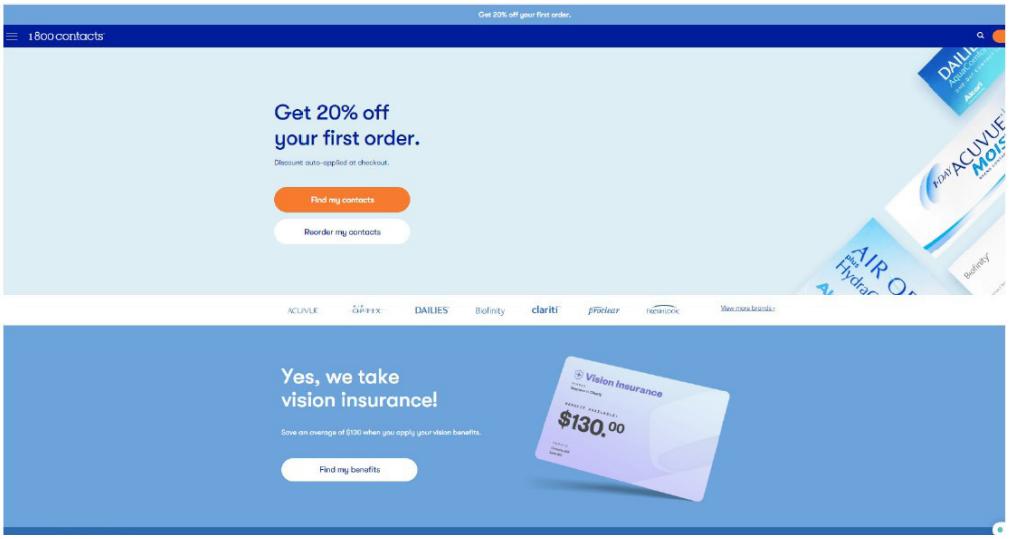
Warby Parker Beats Back 1-800's Infringement Claims

Court applies Polaroid *factors to determine likelihood of confusion*

By David Halberstadter

In our Fall 2021 issue, we reported on the Second Circuit's decision in *1-800-Contacts, Inc. v. Federal Trade Commission*, 1 F.4th 102 (2d Cir. 2021). In that case, the Second Circuit reviewed the online contact lens retailer's practice of filing trademark infringement lawsuits against competitors who purchased 1-800-Contacts related "keywords" so that their own paid advertisements would appear in the search results of consumers searching online for 1-800's website. 1-800 typically then entered into settlement agreements in which the competitors agreed not to bid on 1-800's name or variations of its trademarks in future keyword auctions conducted by search engines. The Federal Trade Commission considered these settlement terms a method of unfair competition under the FTC Act, but the Second Circuit disagreed.

Our article questioned whether 1-800's trademark claims against competitors were meritorious and noted that 1-800 had just filed another federal lawsuit, in which it asserted that eyeglasses retailer, Warby Parker, infringed on 1-800's trademarks by purchasing search engine keywords such as "1-800 Contacts" and other variations, in order to advertise its recently-launched contact lens business. *1-800 Contacts Inc. v. JAND Inc., d/b/a Warby Parker*, Case No. 21-cv-06966 (S.D.N.Y., filed August 18, 2021). As promised, we are keeping tabs on this lawsuit. Here's the latest.



1-800 Contacts' Home Page

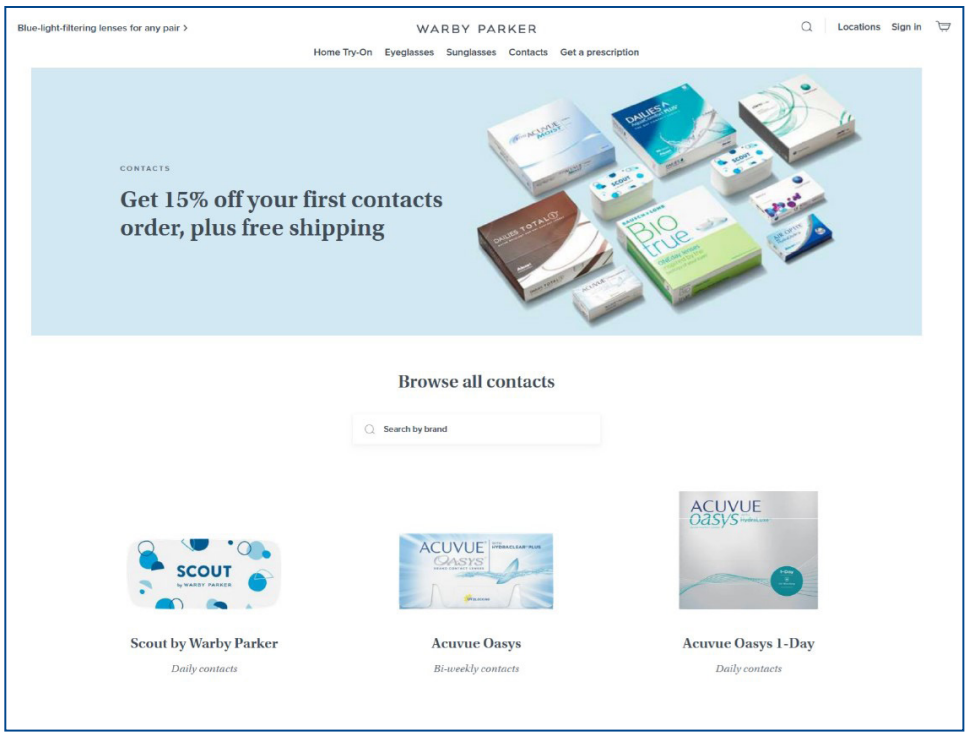
On June 27, United States District Judge P. Kevin Castel of the Southern District of New York granted Warby Parker's motion for judgment on the pleadings and entered judgment for Warby Parker. To be sure, this is only one district court's decision; it has no precedential value and it is based upon the specific allegations of 1-800's complaint. Nevertheless, the court's summary dismissal of 1-800's claims could put a serious dent in the company's litigation strategy for deterring competitors from engaging in keyword advertising. This decision could embolden other competitors to ramp up their bidding on keywords related to 1-800's marks and to refuse to settle should 1-800 sue them. And other retailers with a substantial online presence and strong trademarks may think twice about engaging in similar litigation-and-settlement tactics.

1-800's Key Allegations

1-800 alleged that Warby Parker, as part of its recent foray into the online contact lens market, sought to confuse and mislead consumers searching for 1-800's online store. 1-800 asserted that, among other things, Warby Parker bid for keywords relating to 1-800's trademarks in search engine auctions, so that when a consumer conducts an online search for "1800 contacts" or using similar search terms, the search results page will display a paid search result for Warby Parker's website at or near the top of the results page, often above the "organic" search results for the actual 1-800 website.

According to the complaint, if a consumer clicked on the Warby Parker advertisement that appeared in the search results for "1800 contacts," he or she was directed to a "landing page" for contact lenses on Warby Parker's website that allegedly

mimicked the look and feel of 1-800's website. By contrast, 1-800 claimed, if a consumer instead searched for "Warby Parker contacts" and clicked on those search results, they were directed to a different landing page that replicated the overall look and feel of the Warby Parker website. In other words, 1-800 claimed that consumers searching for 1-800's website were directed to a Warby Parker web page that looked similar to 1-800's, while consumers searching specifically for Warby Parker contact lenses landed on a different page that looked more like Warby Parker's other web pages.



Warby Parker's Landing Page for "1-800 Contacts" Search Results

The Court Applies the *Polaroid* Factors

The principal question before the court was whether 1-800's complaint plausibly pleaded that Warby Parker's use of 1-800's marks through search-term advertising and the linking of a particular landing page on Warby Parker's website would likely cause confusion as to the origin or sponsorship of Warby Parker's goods. The court therefore evaluated 1-800's allegations against the Second Circuit's test for determining the likelihood of consumer confusion, commonly referred to as the *Polaroid* Factors, so-named for the Second Circuit's decision in *Polaroid Corp. v. Polaroid Elecs. Corp.*, 287 F.2d 492 (2d Cir.1961).

(For readers outside the Second Circuit, each federal circuit has its own, comparable test for likelihood of confusion. For example, the Ninth Circuit applies the *Sleekcraft* Test, established in *AMF Inc. v. Sleekcraft Boats*, 599 F.2d 341 (9th Cir. 1979). The Third Circuit uses the *Lapp* Test, based on *Interpace Corp. v. Lapp, Inc.*, 721 F.2d 460 (3d Cir. 1983). The Fourth Circuit uses factors developed in two appellate decisions, *Pizzeria Uno Corp. v. Temple*, 747 F.2d 1522 (4th Cir. 1984) and *Sara Lee Corp v. Kayser-Roth Corp.*, 81 F.3d 455 (4th Cir. 1996).)

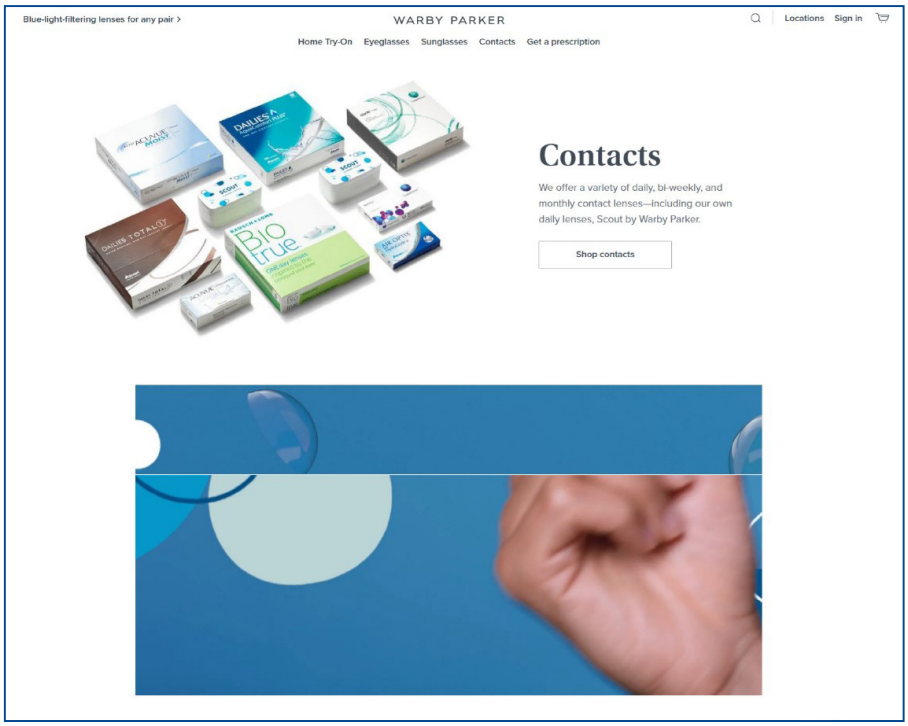
To begin, the court noted that the *Polaroid* test for determining the likelihood of consumer confusion "is a fact-intensive inquiry that depends greatly on the particulars of each case," and that no single factor is determinative. In this case, the court chose to focus on the *Polaroid* factors that it considered most relevant to the circumstances alleged: the strength of 1-800's marks; the degree of similarity of the marks at issue; the proximity, competitiveness and relative quality of the products sold by the parties; alleged evidence of bad faith by Warby Parker; and the sophistication of consumers in the relevant market.

Taking the allegations of 1-800's complaint as true, the court concluded that 1-800's marks are strong. However, the court also concluded that the marks at issue were substantially different. In many trademark infringement cases, the defendant is using a mark that looks or sounds similar to the plaintiff's mark; for example, when a drug store chain offers a "house brand" for a product that is packaged and labeled in a way that copies a brand name's packaging. In this instance, the court rejected 1-800's argument that "the marks used by the parties are identical" because Warby Parker was using 1-800's marks as keywords to trigger search result advertisements. Rather, the appropriate comparison was between 1-800's marks and Warby Parker's marks:

> While Warby Parker "uses" the 1-800 Contacts Marks by bidding on search results for the marks, the crux of 1-800 Contacts's claims here is that after the search results for the 1-800 Contacts Marks are displayed to the consumer, there is an appreciable number of consumers who cannot discern, either before or after clicking on the paid links to Warby Parker's website, that the contacts being sold by Warby Parker on their website are actually unrelated to 1-800 Contacts or the 1800contacts.com website.

The court observed that when a consumer's search results are displayed, Warby Parker's paid search result is prominently labeled as an "Ad" and displays Warby Parker's own website address.

With regard to the proximity of the products at issue, their competitiveness with one another and their relative quality, the parties did not dispute, and the court concluded, that the parties' products are virtually identical and are in direct competition with one another.



Warby Parker's Landing Page for "Warby Parker Contacts" Search Results

Turning to 1-800's allegations that Warby Parker acted in bad faith, the court concluded that there was some evidence of bad faith by virtue of Warby Parker providing links to different contact lens landing pages, depending on whether a consumer searched using variations of 1-800's name and marks or using variations of Warby Parker's name and marks. The latter landing page matched the overall aesthetics of the rest of Warby Parker's website while, according to the complaint, the former landing page was specifically designed to mimic the aesthetics of the 1-800 website, such as a light blue box near the top of the page, or a discount offer for the consumer's first order, both of which were missing from the regular Warby Parker website page for contacts. That said, the court also pointed out significant differences between 1-800's website and the Warby Parker landing page at issue, including the fact that Warby Parker's name is clearly displayed on that page.

The court observed that 1-800's complaint focused on would-be consumers of 1-800's contact lenses. Because 1-800 is exclusively an online retailer, the court determined that "the relevant consumer base, conducting internet searches in the year 2022, would likely be familiar with both the concept of paid search results and the significance of website address links." It concluded that "the relevant consumer base here would be sophisticated enough to (1) review the results of their online search — including linked website addresses that will navigate them to a different website when clicked — before clicking on such links, and (2) review the contents of any website that they have navigated to before taking further action, such as making an online purchase and providing sensitive payment information."

After considering the relevant *Polaroid* factors, the court reached the conclusion that 1-800 had failed to plausibly allege a likelihood of confusion as a matter of law and entered judgment against 1-800. So where does that leave the online retailer? First, the judgment has no precedential value; it is only a district court decision. It also is unlikely to prevent 1-800 from making similar allegations against another competitor based on that competitor's unique uses of 1-800's marks; and the court's decision likely would not be a basis for a different defendant to assert collateral estoppel or *res judicata* as a defense, because the decision was based exclusively on 1-800's allegations in this case, a comparison of the relevant search results and a selection of the parties' web pages.

On July 27, 1-800 filed a formal notice of appeal from the district court's decision. We will update readers on the status of that appeal in a subsequent publication.

Meanwhile, the district court's decision could well have a chilling effect on 1-800's strategy of using litigation and resulting settlements to prevent competitors from using 1-800's marks as keywords for paid advertising, and might encourage competitors sued by 1-800 from quickly capitulating to 1-800's trademark infringement lawsuits, or from settling such litigation on terms that include refraining from bidding on 1-800 marks in the future. More broadly, all online retailers — those with highly-recognizable and very strong marks and those seeking to compete with such companies — should take note of this dispute and its summary dismissal before heading down a similar path.

Advisory: California Consumer Privacy Act's Employee and B2B Exemptions to Expire on January 1, 2023




By Trisha Sircar, Jose Basabe, Catherine O'Brien and Rachel Schaub

The California Consumer Privacy Act (CCPA) is California's groundbreaking legislation that seeks to give California consumers certain rights over how a business handles "personal information" collected about its consumers. On October 11, 2019, California Governor Gavin Newsom signed AB 25 into law, which provided businesses with temporary relief by exempting personal information that is collected in certain employment contexts and in a business-to-business (B2B) context from the scope of the CCPA until January 1, 2021. As previously reported, Governor Newsom signed AB 1281 into law on September 29, 2020, providing a one-year extension to the partial employee and B2B exemptions to January 1, 2022, applicable only in the event that the California Privacy Rights Act (CPRA) ballot initiative failed. When the CPRA was approved during the 2020 election by California voters, the exemptions were extended one final time to January 1, 2023. On August 31, 2022, the California legislature adjourned without extending the exemptions, which automatically expire on January 1, 2023 in conjunction with the CPRA effective date.

Types of Employee and B2B Data Now Subject to CPRA

The CCPA contains a partial employee exemption for personal information collected by a business about a person who was either a job applicant or past/current employee or in an otherwise related position, including owners, directors, officers, contractors and beneficiaries/dependents. The exemption is limited to when the business used the information provided "solely" for employment-related actions. The B2B exemption applies to personal information of employees or business contacts that a business collected to aid in providing or receiving a product or service to and from another business.

What Should I Do Now With Employee Data and Personal Information Collected in a Business Context?

This development marks California as the first and only state with a general privacy law that applies to this type of personal information. Personal information collected in certain employee

contexts and in a B2B context will now be subject to the onerous compliance requirements under the CPRA. Businesses will have to immediately pivot their data privacy compliance efforts and:

- Assess the personal information collected, used and disclosed from California employees and job applicants. This will require employers to map employee data and work with their human resource and information technology departments.
- Update employee, job applicant and other privacy notices and disclosures to incorporate personal information collected in an employment and B2B context.
- Businesses will be required to disclose a full text privacy notice to employees, as opposed to the previously abbreviated version permitted under the exemptions. These notices will have to include a variety of information, including: (i) the categories of sensitive personal information and personal information collected and processed; (ii) the purposes for the processing; (iii) the retention period by category of personal information; (iv) the description of the rights available; and (v) the manner in which individuals may exercise such rights.
- Assess the personal information collected by service providers and third parties.
- Review and update any contracts with service providers and contracts that process employee personal information or personal information collected in a B2B context.
- Review and update policies and procedures to include the expanded rights under the CPRA.

In short, the CPRA ramps up notice requirements and imposes compliance obligations and other duties on more businesses than previously covered in the CCPA.

What Are Some Other New Issues That Need to Be Assessed?

There are multiple new requirements under the CPRA that will apply to personal information collected from consumers, as well as in the employment or recruitment context and when transacting with actual or prospective business contacts. Some of the key new requirements include:

- The CPRA's expanded rights will now grant the right to know and access, the right to deletion and the right to correction of personal information.
- The CPRA expands the scope of behavior covered by the CCPA by amending all mentions of "selling" to include "sharing." This term is defined as any disclosure of personal information to third parties for cross- context behavioral advertising, regardless of whether consideration is exchanged. Where a business engages in sharing, it must post a link titled "Do Not Share My Personal Information" and provide consumers an opportunity to opt out of sharing.
- The CPRA introduces the new concept of "sensitive personal information," which will require businesses to develop additional disclosures about the use of sensitive personal information in their privacy notices and responses to individuals' requests exerting their expanded CPRA rights.
- The CPRA introduces new data minimization and data retention requirements. Businesses must not collect more personal information than is necessary and must not retain personal information for longer than is reasonably necessary for disclosed purposes. Accordingly, businesses will have to develop, review and update internal data retention policies and procedures.

We Can Help You

With January 1, 2023 rapidly approaching, if you have any questions about how to prepare your business to comply with the onerous requirements of the CPRA, please contact a member of Katten's Privacy, Data and Cybersecurity team.

News to Know

Advertisers Will 'Pay a Price' for Making False Claims, FTC's Consumer Protection Chief Warns

Speaking at the National Advertising Division's annual conference, Samuel Levine, director of the Federal Trade Commission's Bureau of Consumer Protection (BCP), emphasized his agency's work to "root out deceptive advertising and ensure a fair marketplace for consumers

and honest businesses."

In a clear departure from his predecessor, Levine said he won't be moving away from monetary relief against national advertisers. He noted this is his view, despite the Supreme Court's decision last year in *AMG Capital Management, LLC v. FTC*, which stripped the agency of its authority to recover damages through Section 13(b) of the FTC Act.

"I believe that the remedies we seek should be based on the violations we allege, not the size of the company that committed them," he said. "That is why, in spite of the AMG decision, the Commission is consistently seeking monetary relief in our cases against national advertisers. Allowing advertisers to reap the rewards of deceptive claims not only leaves consumers in the lurch but also undercuts honest businesses who play by the rules."

He provided an overview of BCP actions and strategies, including using settlements as a way to stop wrongdoing and protect consumers.

"Alternative paths to monetary relief can be slower and more challenging …. But when we pursue a case, we do not settle for inadequate relief, even if it means needing to invest greater resources – and taking a longer path – than we did when we could seek monetary relief under 13(b)," he said. Read Samuel Levine's full remarks.

Federal Trade Commission Releases Guidance to Merchants That Offer Buy Now/ Pay Later (BNPL) Options to Customers

On September 26, the Federal Trade Commission (FTC) published a blog post warning all entities that have a role in the "BNPL ecosystem" that "basic consumer protections" in the Federal Trade Commission Act apply to such payment offerings. The FTC advised merchants and others to undertake a three-part BNPL compliance check. Read the Katten advisory.

5 Top NFT Questions Attys Want IP Agencies to Explore

In an article highlighting several questions regarding the intellectual property implications of non-fungible tokens (NFTs), *Law360* spoke with Intellectual Property Partner **Michael Justus** about the need for administrative guidance on NFT-related trademark applications. Mike was among several interviewed attorneys who identified issues that they are hoping will be addressed in a joint study launched by the US Patent and Trademark Office (USPTO) and the US Copyright Office. Read the article.

Kattison Avenue Contributor David Halberstadter Lauded as 2022 'West Trailblazer'

The *American Lawyer* has named Litigation Partner **David Halberstadter** in its 2022 edition of "West Trailblazers," which honors professionals in the region "who have moved the needle in the legal industry." The Trailblazer series, which was launched in 2021, spotlights individuals who are agents of change in their respective practice areas. Read more.

Katten's Advertising, Marketing & Promotions Practice

Katten represents advertisers, advertising and promotions agencies, technology developers, content producers, and media and entertainment companies, in reimagining the connection to consumers. From clearance, privacy and regulatory obligations to smooth product launches and brand integration, we address concerns in a variety areas, including: ad, marketing and promotional programs; agency-client relationships; branded entertainment; contests and sweepstakes; internet distribution; licensing and vendor agreements; litigation (comparative and false advertising, First Amendment issues, Lanham Act, unfair competition laws, etc.); privacy and data security; talent and production agreements; user-generated content; and sponsorships.

Kristin J. Achterhof
Partner
Chair, Advertising, Marketing & Promotions
kristin.achterhof@katten.com

Katten

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

CENTURY CITY | CHARLOTTE | CHICAGO | DALLAS | LONDON | LOS ANGELES | NEW YORK | ORANGE COUNTY | SHANGHAI | WASHINGTON, DC