Law à la Mode –

ISSUE 35, FEBRUARY 2023

DLA PIPER

Contents

Editorial

Welcome to the 35th edition of *Law à la Mode*.

Like in previous editions of *Law à la Mode*, DLA Piper colleagues from across jurisdictions have worked together to bring you articles that address topical challenges and opportunities that the fashion and retail sectors are facing.

This edition of *Law à la Mode* focuses on the metaverse. We have several articles addressing the various legal considerations and implications that organisations must consider when using the metaverse.

From setting up shop and advertising in the metaverse, to a discussion around the first case of trademark infringement through NFTs in Italy, this edition showcases the quickly evolving world of the metaverse and how companies can begin to navigate it.

We hope you enjoy this edition of *Law à la Mode*. If you have any comments or feedback, please get in touch with DLA Piper's Consumer Goods, Food and Retail sector group at olivia.sharman@dlapiper.com.

Ruth Hoy
Partner and Global Co-Chair,
Retail and Fashion Sector
London

The end of returns for fashion brands? Legal considerations for digital twins in the metaverse

Authors: Gareth Stokes (Partner, Birmingham) and **Kurt Davies** (Associate, Birmingham)

Returns are the bane of brands' ecommerce offerings.

An exciting prospect the metaverse offers is the possibility of customers having a "digital twin," an avatar that's the same size and shape as the customer and able to stroll through the metaverse. While the avatar might be a three-headed dragon in some contexts, for some metaverse services – particularly anything related to purchasing wearable items for delivery in real life – the digital twin will prove very useful. The twin, along with perfect digital replicas of the items offered by online retailers in the metaverse, will allow customers to buy with greater confidence that they're going to get an item that fits.

This creates a much more immediate experience for the customer and delivers greater brand engagement for the retailer. It also drives financial and environmental savings by reducing returns.

But if you want to set up shop on a plot of virtual reality, what's the first thing to consider?

Top-down or decentralised?

There are two metaverse concepts: "top-down" – with the platform operator acting as the arbiter and town planner; or decentralised and "web3" enabled – where users own and build their environment.

A top-down approach might make it easier to secure and create a safe space. A top-down has features that can easily facilitate legal compliance, and perhaps connect to other top-down metaverses giving access to a large pool of customers, all in exchange for giving up a large slice of control and data.

Let's assume your brand opts for the top-down option – what are the legal implications?

Data protection

Your virtual store will receive a vast array of rich datasets from customers and other sources that dwarf those collected via your ecommerce site. Depending on the capabilities of the VR headsets customers use to peruse your wares, you could be collecting data such as vital signs and eye tracking from which certain behaviours can be inferred.

Though this is an exciting opportunity for any brand, the applicable privacy laws will need to be determined. This will depend on the location of the platform operator's servers, your location, and the location of customers.

If UK/EU laws apply, as a data controller you bear a host of data protection duties. For instance, you should carry out an impact assessment to determine the lawful basis for using the data, the impact on your customers and how this can be mitigated, and how you will inform them of all of this. Some of this is troublesome enough on the old-fashioned internet – cookie banners anyone?

Intellectual property

Your brand may want to engage designers to build your store and design digital assets. The contracts with these designers should ensure that copyrighted work is owned by the brand. If your store is to have accurate digital copies of physical goods, the contracts commissioning those items must allow for the creation of the matching digital copies for your metaverse shop window.

You will also need to police use of your brand's intellectual property. Make sure the platform provider polices infringement, offers a clear reporting/disputes process, and has the tools to combat infringement.

Consumer protection

Your customers will be protected by their local consumer protection regime when interacting with your metaverse store, with sales in the metaverse constituting distance sales. Your brand's ecommerce terms of sale will need amending to reflect your brand's new sales channel, or perhaps a new, separate set of metaverse-centric terms are preferrable. The customer (or avatar) journey will also be different. You will need to consider how your brand can ensure that compliance obligations are met, such as providing pre-contractual information to consumers and ensuring it's clear when a purchase becomes binding, all while ensuring the customer experience is slick.

Cystal-ball gazing

What we think of the metaverse and how it will operate years into the future involves some educated guesswork, particularly as our laws adapt to it and web3 more generally. However, it would be reasonable to bet on most, if not all, of the above being key legal considerations for innovative brands in the years to come. And as the metaverse takes off, keeping brick and mortar stores relevant will take more creative thinking.

Metaverse advertising – fashion week and advertising rules

Authors: John Wilks (Partner, London) and **Hannah Potter** (Trainee Solicitor, London)

Paris, New York, Milan... and Decentraland?

2022 saw the launch of the first metaverse Fashion Week, providing an excellent example of the new advertising opportunities available to brands like Dolce & Gabbana who participated. But how does metaverse advertising differ from other types of media, and what legal issues do brands need to consider when venturing into this exciting new space?

What might a metaverse ad campaign look like?

Metaverse campaigns have taken a variety of forms and are sure to keep evolving. Some have opted for hybrid events, like Gucci Garden, an interactive virtual exhibit that mimicked a physical experience in major cities. In Tommy Hilfiger's metaverse pop-up, users could purchase a clothing NFT and redeem it for a physical counterpart. Others use the metaverse as a brand promotion tool: in Nikeland, users play games and clothe avatars. Balenciaga have created wearable NFTs for avatars, who can model pieces and be featured on billboards in Fortnite.

Whose ad rules apply?

The first step to understanding advertising rules in the metaverse is working out which countries' regimes apply. The decentralised nature of the metaverse might make it harder to work this out. But existing rules on online advertising are relevant, such as UK regulator the ASA's (Advertising Standards Authority) 2021 Online Remit Guidance. This sets out various principles which can cross over to a metaverse environment, such as:

- Paid-for ads that target UK consumers are in the ASA's scope. Aspects such as currency and language are used to establish targeting, although in a metaverse scenario (where products may be priced in crypto) it may harder to determine targeting.

- Non-paid for ads fall within the ASA's scope where the advertiser is UK-based.

Regulators are likely to increasingly need to collaborate with their counterparts in other jurisdictions (e.g. through the European Advertising Standards Alliance) in tackling metaverse ads, given their cross-border nature.

What are the key obligations for metaverse advertising?

Existing rules apply to advertising in the metaverse, but the new context may change how these apply and their significance. Key risk areas that brands should have front of mind include:

- **Ensure advertising is recognisable as advertising.** The immersive nature of the metaverse can increase the risk of consumers not spotting what is advertising and what is not. Content displayed in ad spaces which replicate the real world, such as billboards, are less likely to be mistaken for other content. But when NFTs, clothing, advergames and avatars are presented in the metaverse, it may be unclear what is advertising and what is not, and text-based labels may be hard to incorporate.

- **Influencer advertising** has been a focus for regulators for some time (see the DLA Piper Influencer Marketing Guide), and avatar influencers can expect no exception. How do you #ad an avatar? Metaverse advertising – applying old rules to a brave new world.

- **Adverts that purport to mirror how a real-life article of clothing would fit or look** (e.g. displayed on avatars) **could give rise to claims of being misleading**. Again, there's the issue of where and how disclaimers could effectively be incorporated.
- **Ads for age-restricted products must be handled particularly carefully to ensure targeting restrictions are not breached.** For example, in the UK, products such as gambling, alcohol, High Fat Salt and Sugar (HFSS) foods, and cosmetic interventions, should not be targeted at children. In a metaverse context, the proliferation of young audiences, use of avatars, and the interconnected and decentralised nature of the platform raise new challenges with age verification and targeting.
- **Brands deploying gamified advertising should consider the rules on in-game purchasing** (particularly the needs for clarity on terms and to avoid unduly pressuring users).
- **Brands who are releasing NFTs should be aware that they may be treated as cryptoassets**, so additional obligations apply (in the UK see the ASA's guidance which includes the requirements to make investment risks clear and not to take advantage of consumers' inexperience).

Overall, while the issues thrown up by advertising in the metaverse are not new, the medium certainly creates heightened risks in some areas (particularly given its immersive nature, appeal to young people, and connections with NFTs and gaming), and so is likely to draw regulator attention for the foreseeable future.

How accessible and inclusive is your retail online presence?

Authors: Chloe Forster (Partner, London)
Lisa Hodgson (Legal Director, Birmingham),
Linzi Penman (Senior Associate, Edinburgh),
Laura Maclennan (Associate, Edinburgh)
Isla Neil (Associate, Edinburgh)

Retailers know their physical premises need to be accessible to all customers; but technology like the metaverse has revolutionised the consumer experience. Following the COVID-19 pandemic, the way we shop has changed. The Office of National Statistics notes that the percentage of online sales in the UK jumped from 18% to 37% during the pandemic. A recent survey found that in the UK, businesses lost more than GBP17 billion in sales in 2019 from disabled shoppers abandoning websites due to accessibility barriers. With the increased popularity of online shopping and new possibilities unlocked by using the metaverse to connect with consumers, you have to check if your online presence is as accessible as your physical premises, to maximise sales and customer satisfaction, and to ensure legal compliance.

Consumers are protected from disability discrimination under the Goods and Services section of the Equality Act 2010, which you may be familiar with in the context of ensuring that your shops make reasonable adjustments. But you might not have considered how this applies to your online presence. For example, as a retailer, you may be wondering:

What should be done to ensure your online user journeys are accessible, legally compliant and aligned to your company values?

"Good" accessibility is difficult to define, as this differs from person to person and disability to disability. Also, the legal obligations on the private sector differ slightly from the public sector. Those in the public sector have recently been subject to online compliance regulations, following legislation introduced in 2018 which required all public sector websites and mobile apps (with some exceptions) to meet specified accessibility standards by June 2021. Namely, to ensure websites and apps are "perceivable, operable, understandable, and robust" to meet the European accessibility standard EN 301 549 and the Web Content Accessibility Guidelines (WCAG) 2.1 to level AA. Though no deadline has been imposed on the private sector, the same principles apply and are a useful indicator for all businesses that have to comply with the Equality Act 2010.

At a high level, it's important for retailers to comply with the duty to make reasonable adjustments. This duty arises where a provision, criterion or practice or the lack of an auxiliary aid or service, puts a disabled person at a substantial disadvantage compared with a non-disabled person. The EHRC Statutory Code of Practice (Code) on discrimination in services, which provides guidance on the detail of the Equality Act, includes various important points which companies should take into account when assessing how to comply with their reasonable

adjustment duty. In particular, the Code specifies that the duty requires service providers to take positive steps to ensure that disabled people can access services. This goes beyond simply avoiding discrimination.

How does this interact with other regulatory requirements, like data protection and consumer protection?

Use of technology like the metaverse could mean a more accessible and inclusive shopping experience for many people with disabilities. But for a retailer's online presence to be truly accessible the technology is only a starting point, and there are more active steps retailers can take across their websites, apps and metaverse presence. As a start:

- Colours are important for brand awareness, but accessibility should be considered. For example, there are certain colour combinations that are particularly difficult for colour-blind customers to read. And people with hypersensitive variation of autism often need reduced stimulation by using "cooler" colours. Retailers should also be aware that there has been a wave of recent complaints made to data protection authorities against companies using marketing techniques that use human psychology to achieve a preferred outcome, such as colouring "no" buttons green, and "yes" buttons red.
- Make sure your key legal policies are accessible by avoiding complex navigation to reach important documents like your privacy policy and terms and conditions. Ensure it can be accessed by both keyboard and mouse users in one click and that if you signpost it (e.g. "access here") then the signpost should be understood by those that may otherwise face challenges to access it. Consider including a braille display or a screen magnifier. Or, have an immersive reader that reads out phrases like "sign me up." And explain what is being signed up to – maybe with use of infographics or captioned videos.
- If a retailer's policy is that all customer complaints must be made in writing, this may place someone with, for example, dyslexia at a substantial disadvantage in making a complaint. Here, amending the policy to permit those who struggle to use a written complaints procedure to make their complaint by telephone is likely to be a reasonable adjustment to make.
- Many organisations use tracking pixels. These are trackers embedded in websites, sponsored ads and emails which capture user data, including time spent on a website. Under the current UK data protection and privacy regime, pixels require consent where they are stored on a device or access information stored on a device. As these trackers are generally more difficult for users to spot (compared to their cookie counterparts which are better-known by users and easier to audit), it's particularly important that their presence is highlighted to users in an easily accessible way, so people understand how their data is being used. These trackers are often used to measure the success of marketing campaigns such as email click rates. So it's important to ensure consent is in place where necessary, so you can harness the data for analytics and to inform future marketing.

There's always a tricky balance between providing enough comprehensive information to satisfy legal requirements and having a "sleek" user journey with as few words as possible. The Information Commissioner's Office (ICO), responsible for upholding information rights and data privacy in the UK, has issued guidance to help companies navigate these competing requirements. The ICO suggest a layered approach, providing users with a short initial message containing all key information, and linking the user to a second layer containing a more detailed description.

A similar approach is recommended from a consumer protection perspective – dense, legalistic language buried within terms and conditions is unlikely to be readily understood. Instead, key messaging and important terms should be clearly presented, with the option for users to access further detail. Information requirements can also be satisfied through having a user-friendly FAQ page, where users can easily jump to a specific topic, for example, "How do I make a return," hyperlinked to aid accessibility.

What should you think about when considering use of the metaverse to connect with consumers who have a disability?

Your metaverse presence should be designed, reviewed, and audited to ensure compliance with legal requirements. Novel points could arise from a consumer's use of avatars in the metaverse: as a retailer you'll have a greater opportunity to monitor your customers on the metaverse, including analysis of their avatars to expand their profiles. Avatars can be used by disabled people to communicate aspects of their disability, and the increased use of biometrics on the metaverse (e.g. how someone communicates or the way someone walks) means that retailers could suddenly be processing a substantial amount of special category data on their customers. This type of personal data merits extra protection in law given its sensitive nature and requires a secondary "lawful basis" when processing. In the context of your online consumer profiling, this is typically the data subject's consent. Internally, retailers who may be collecting this data should work on their data protection impact assessments, to identify the risks posed by processing such sensitive data in this way and to ensure that risks are managed appropriately.

On a final note, it's worth noting that a recent survey in the UK found that 22% of the total UK population have a disability. This means addressing accessibility gaps in consumers' experiences is not only an opportunity to better align with your brand values; there's also a very strong financial business case for doing so. Retailers should be aware this is not only a commercial or ethical point, but a legal one – for example, the Royal National Institute of Blind People have launched a toolkit on how to hold website owners to account and are active in bringing cases against non-compliant websites. The UK's Equality and Human Rights Commission can also use their legal powers against offending organisations. This means that there's not only a risk of legal action against your business, but also potential adverse publicity and reputational damage.

So – if you haven't already – now's the time to start considering accessibility when curating your metaverse presence, or user journeys for websites and apps.

Metaverse art and fashion – How does this Miro look on my metawall?

Authors: David Alexandre (Counsel, Luxembourg) and **Alejandro González Vega** (Associate, Luxembourg)

Fashion and art have always been deeply entangled. Many famous fashion houses have looked for inspiration for their collections in the works of grand masters, like van Gogh, Monet or Picasso. And many artists, like Sorolla or Zuloaga, have reflected a real passion for fashion in their work.

Creating NFTs from physical artwork

Using works of art for décor is not unusual in the world of fashion. And it's not unusual for fashion brands to invest in and own works of art. But, if a company owns pieces of art, does this mean that it's free to use them as it sees fit? Could a company create NFTs out of the works and display them in the metaverse?

This is exactly what Spanish fashion group Mango recently did with some paintings from famous artists Joan Miró, Antoni Tapiès and Miquel Barceló. To celebrate the opening of its flagship store in New York, Mango, with various artists, created five NFTs based on reinterpretations of works of art created by these painters. The NFTs were then displayed in the Museum District of the platform Decentraland.

Little did Mango know that its probably well-intentioned initiative was to meet resistance from the Spanish collecting society VEGAP, which represents visual artists. VEGAP filed a request for a preliminary injunction before the Courts of Barcelona, which was granted. Pending trial, the court ordered that the NFTs were deposited in a safe digital wallet to prevent them from being damaged or lost.

Although we still don't know the court's final decision, the question arises about the rights that the owner of a work of art enjoys with respect to copyright, particularly when it comes to using them in the digital world.

So who owns the rights?

In most civil law countries, the copyright system rests on two basic pillars: its subject matter is the work itself, and not the means whereby such work is incorporated; and copyright belongs originally to the author. So from a copyright perspective, enjoying property rights on the medium where the work exists does not grant any copyright to the owner (e.g. owning a copy of a book does not bestow any rights to the novel).

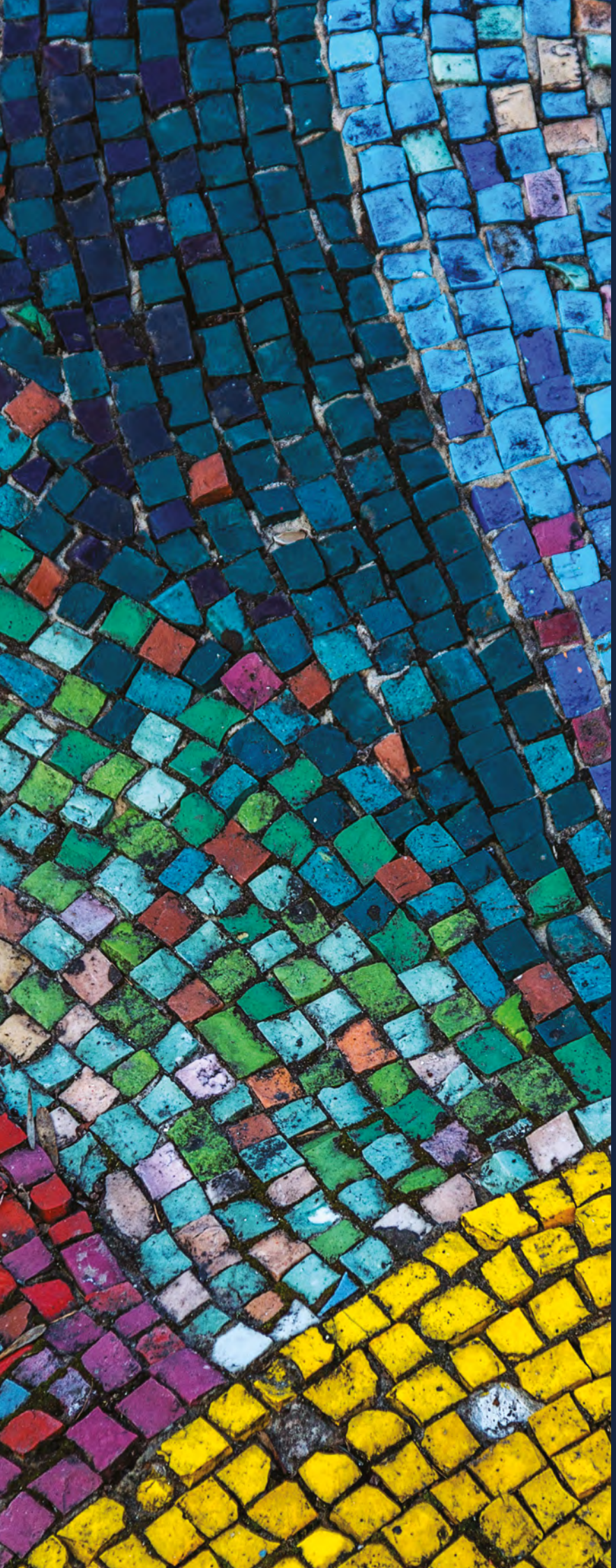
In the case of works of visual art, where the medium and the work are intrinsically intertwined, some legislations grant a limited set of rights to the owner. That is the case of the Spanish Copyright Act, which allows the owner of such works the right of public exhibition, unless the author has expressly opposed it.

Does regulation extend to the metaverse?

In the matter examined, under the Spanish legislation, Mango would be free to exhibit the paintings it owns – for example, in a store or a gallery.

But can this right be interpreted to allow displaying NFTs based on those works in the metaverse?

This issue is open to debate. On the one hand, access to a digitalised work by the public at the place and time of their choice would usually fall under the making available right and not under the right of public exhibition. However, the particular conditions of the metaverse, where the works are located at certain specific coordinates, do not really differ much from the work being in a museum, meaning it could be considered public exhibition.



However, even admitting that "hanging" a digitalised version of a work of art in the metaverse amounts to public exhibition, the act of converting the physical work of art into an NFT is, irremediably, an act of reproduction. This conclusion is supported by the case law of the CJEU in *Allposters*, where the court considered that the alteration of the medium of a work (from paper to canvas) was an act of reproduction that prevented the exhaustion of the distribution right.

So, unless the author has consented, via copyright license or assignment, to the creation of digital representations of their work, any such action would constitute an unlawful act of reproduction of the work. Of course, adapting or reinterpreting the work to create an NFT would also require the authorisation of the copyright holder if it results in a derivative work.

Apart from the author's economic rights, moral rights, in particular those of attribution and integrity, also have to be respected.

In conclusion, when using copyrighted works in the metaverse, special attention should be paid to avoid infringing the rights of the creator, even where there is a valid title to the original.

Italian court rules on the first case of trademark infringement through NFTs

Authors Valentina Mazza (Lawyer, Milan) and **Carolina Battistella** (Trainee Lawyer, Milan)

The Court of Rome has issued the first Italian decision on intellectual property rights infringement through the unauthorised sale of NFTs and took a position on some of the recurring issues in the various NFT lawsuits pending in the different jurisdictions.

The case was brought by a famous Italian football club against a company that marketed NFT digital playing cards depicting a well-known football player wearing the team's strip, using the distinctive signs (both word and figurative trademarks) of the team. The NFTs were sold on a well-known marketplace and in the secondary market through resale by first buyers, from whom the respondent company nevertheless continued to receive remuneration.

First, in rejecting the respondent's defences, the court found that the use of the football club's trademarks by the creators of the cards in question had a purely commercial purpose, as it could not be justified by the public interest in the publication of the player's image in light of his fame nor by educational or scientific purposes. The court held that though the player had played for the plaintiff team and had given consent for the use of his image on the cards, the respondent company was obliged to get permission to use the distinctive signs of the team itself. The fame of the team also contributed to the value of the digital image offered for sale with the NFTs.

The Court of Rome also ruled on the scope of protection of the trademarks registered by the football team, which according to the respondent, had not been extended to the classes relevant to the sale of NFTs. After pointing out that the signs in question undoubtedly enjoyed a reputation, the court noted that the trademark registrations expressly stated (particularly for class 9, which is relevant here) that goods not included in the Nice Classification and downloadable electronic publications were covered. Crucial for the finding of likelihood of confusion was that the team was already present in the field of crypto or blockchain games, based on similar technologies, through agreements with third parties. So the court concluded that the sale of NFTs by the respondent infringed the plaintiff's trademarks, as it was likely to create the false impression that there was a commercial connection between the two companies.

The decision also held that the respondent's conduct amounted to an act of unfair competition, including by misappropriation of values.

The court largely upheld the football team's claims. It granted an injunction extended to the production, marketing, and promotion of the NFTs and contents at issue in the lawsuit. And the injunction also covered any other NFTs, digital content and products in general bearing the photograph included in the contested cards (even modified) or the distinctive signs of the team. It was deemed irrelevant that the respondent had ceased the production and marketing of the NFTs since the contract for the use of the player's image was in place until 2024, and users would still be able to resell the NFTs in the secondary market.

The decision issued by the Court of Rome clarified the interpretation of the notion of "commercial use" and the scope of protection of registered trademarks. And it also confirmed the suitability of "dynamic injunctions" in relation to NFTs and metaverse-related infringements of intellectual property rights.

In the case, the football club acted directly against the company selling the infringing NFTs. But this option is not always available as in most instances the seller details are unknown. Most marketplaces have not adopted a system to authenticate their users and verify their identity and their title to mint and/or sell the digital assets. This makes it impossible to trace the seller who offered the infringing NFT on the marketplace. For this reason, right holders often consider taking action directly against the platforms (e.g. OpenSea, Rarible), which are subject to the general regime of liability applicable to Internet service providers, in their quality of hosting providers.

This situation should soon change given the entry into force of the Digital Service Act (Regulation (EU) 2022/2065), which under Article 30 introduced an obligation for online platforms to obtain the trader's information. According to Article 10, information on users must be disclosed by ISPs only upon a court's order. So, to get the full information, right holders might still have no other option than bringing a lawsuit against the platform to seek an order to disclose the users' data and eventually act against them.

The stores have eyes: CCTV, biometric information and consumer privacy

Authors: Sarah Birkett (Senior Associate, Melbourne), **Alex Moore** (Senior Associate, Sydney), **Linzi Penman** (Senior Associate, Edinburgh)

For shoppers entering bricks-and-mortar retail spaces, the presence of security cameras has long been the norm. But some CCTV systems do more than just "watch." Technological advances allow in-store systems to collect and analyse biometric information from individual customers – and it's this retailer activity which is now attracting headlines. Biometric information such as electronic copies of faces, fingerprints, voices collected via CCTV can be used by retailers for many purposes, including to build profiles of the individuals entering their stores, identify returning shoppers and to identify specific individuals that have previously been removed from their premises. But the technology also raises privacy and other ethical concerns.

Here we look at the use of in-store CCTV and biometric information and compare sentiment from Australian and UK consumers in relation to consumer privacy implications.

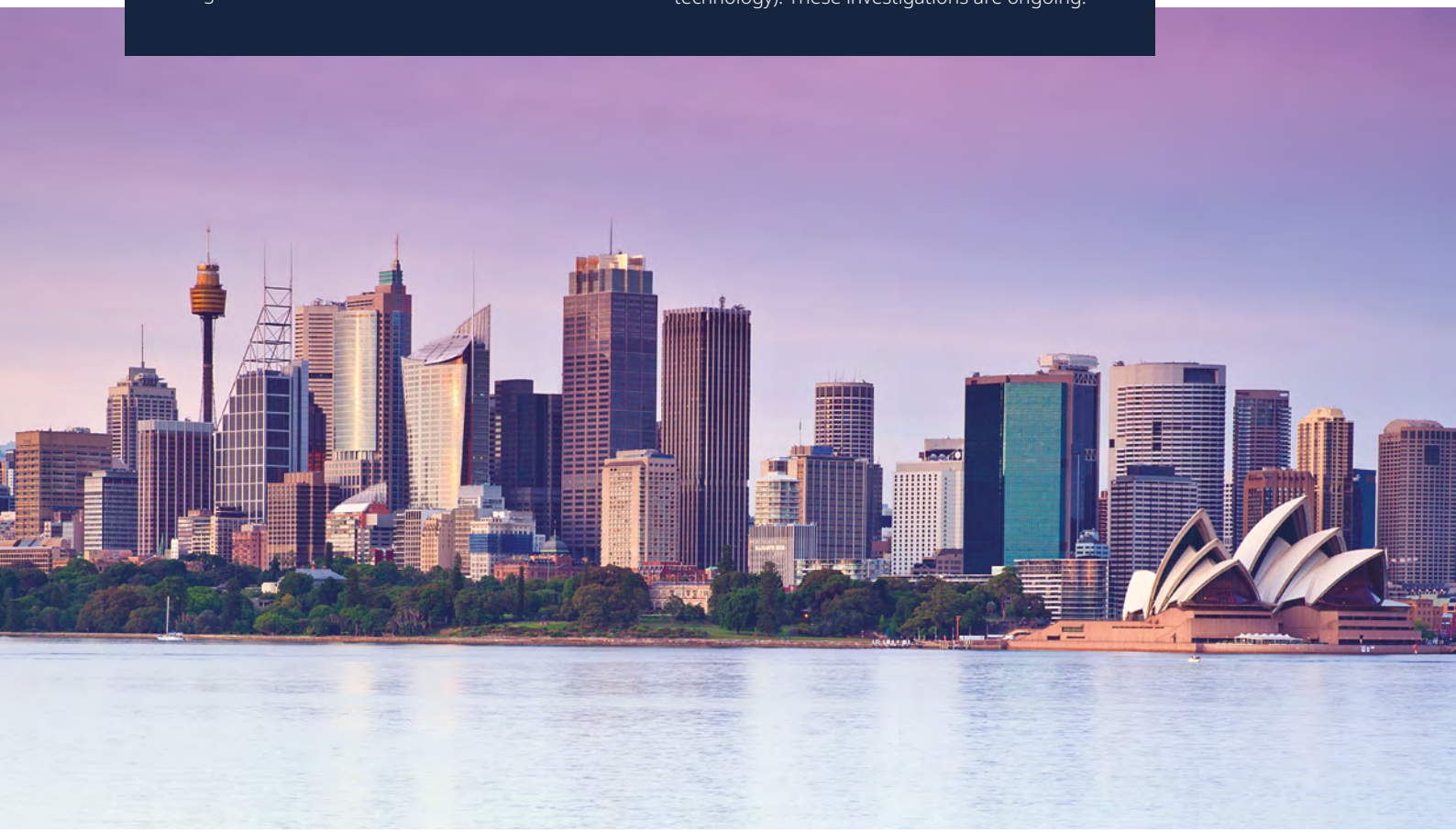
Australia

Biometric information used for automated biometric verification or biometric identification or to create biometric templates is classed as "sensitive information" under the Privacy Act 1988 (Cth). This can include the use of CCTV systems to identify specific individuals, whether or not an individual is named. The collection, use and disclosure of sensitive information must only occur where it's reasonably necessary for the collecting entity's functions or activities *and* (for the initial collection) with the consent of the individual to which the information relates.

Sentiment among Australian consumers about collection of biometric data in retail settings is generally negative. For example, the federal privacy regulator, the Office of the Australian Information Commissioner (OAIC), found in its *Australian Community Attitudes to Privacy Survey 2020*, that 66% of Australians were reluctant to provide biometric information to businesses – higher than their unwillingness to provide medical or health information (60%) or even location data (56%).

In line with these sentiments, the OAIC has conducted high-profile investigations of retailers using CCTV to collect biometric information:

- In 2021 the OAIC made a determination against a multinational convenience store operator regarding its large-scale collection of sensitive biometric information. The organisation captured images of consumer faces via tablets provided for customers to complete surveys regarding their in-store experience. The OAIC determined that this collection was not reasonably necessary for the purpose of improving and understanding customers' in-store experience, and that organisation had collected the information without consent. This amounted to two breaches of the Privacy Act.
- In 2022, an independent investigation by consumer advocate group Choice led to major national retailers Kmart, Bunnings and the Good Guys being referred to the OAIC over their alleged use of facial recognition technology in their in-store CCTV systems. Choice considered the use of such technology to be "disproportionate" to the legitimate business functions of those retailers. The OAIC has since opened investigations into Bunnings' and Kmart's use of facial recognition technology (with the Good Guys having paused their use of the technology). These investigations are ongoing.



United Kingdom

In 2020, it was reported that the number of CCTV cameras in the UK reached 5.2 million (one camera for every 13 people). The UK's data protection regulator, the Information Commissioner's Office (ICO), has published guidance on video surveillance, available on its website, which covers CCTV and other systems which make use of AI. It also provides checklists for businesses to ensure their use of video surveillance complies with UK data protection law.

One use case some retailers have for facial recognition technology is to identify "problem" customers. A regional consumer co-operative used this technology to add customers to a blacklist with alerts to staff when those customer(s) entered stores without being transparent on this processing. Biometric data was not passed to police but instead kept for up to two years. Whether this is a proportionate response in high-risk stores for shoplifting is now under investigation by the ICO.

Like the Australian statistics in terms of public sentiment, a 2019 study in the UK found that, while 82% of respondents supported the use of facial recognition technology by law enforcement agencies, less support was found its use by retailers – only 30% believing this was acceptable. In terms of the thoughts of the regulator, the ICO's video surveillance guidelines note that, given the potential intrusion on individual rights and freedoms, "it is therefore important that the use of surveillance is not seen as the cure to the problems that organisations may face. But instead, a helpful supporting tool where lawful, necessary and proportionate in the circumstances." So it's important to ensure any use of the tool is justifiable, and that retailers have carried out data protection impact assessments and have visible CCTV signage explaining processing.

Conclusion

Businesses operating in the retail sector should take stock of activities in this space. This includes reviewing in-store monitoring practices to identify if biometric data is being collected, how that data is being used and otherwise processed, and to what extent processing aligns with local data protection laws. Retailers should also stay alert for further developments in this area from local regulators, including outcomes of investigations into use of facial recognition technology and updated guidance.