NYSBA

SPRING 2017 | VOL. 26 | NO. 1

Bright Ideas

A publication of the Intellectual Property Law Section of the New York State Bar Association

25 YEARS
INTELLECTUAL PROPERTY LAW SECTION

Inside

Table of Contents

Message from the Chair

With any hope, you are reading this message with the sun shining through your window or while sitting outside, enjoying the fresh air that spring so happily brings back to our state. Winter is finally in our rearview mirror, and (as I write this) we are not yet accosted by summer heat. Joyfully shedding my coat this week, I found myself pondering how beautifully our Section's activities align with the seasons. This is an exciting time of year—a perfect opportunity to get out of the office and embrace all that our Section has to offer.

Gazing backward, our Annual Meeting this winter was another resounding success. Program Chair Bill Samuels organized a day full of interesting, well-presented topics ranging from patent damages to social media to data privacy to product design. The meeting was well attended, integrating Section members who have been involved for years with new faces that we are excited will be part of the Section's future. A heartfelt thank you to everyone whose participation helped make the event both educationally valuable and socially enjoyable.

Our Section's plans for summer are definitely something to look forward to! Starting things off on Wednesday, June 7, from 5:00-8:30 pm, the Section will be holding our 15th Annual Women in IP program. This hallmark event has become a Section highlight, bringing together a diverse cross-section of women in the IP field to learn from each other, network, and further our supportive community. A distinctive panel of inspiring practitioners will discuss their careers and experiences, offer strategies for success, and provide insights on topics including how the IP field has changed, developing a client base, and achieving that ever-ephemeral balance between home and work. With the exceptional Joyce Creidy at the helm and Baker & McKenzie as our host, this is certain to be a fantastic evening. Whether you are just starting out or have been practicing for decades, Women in IP is a great opportunity to connect with old friends, make new ones, and glean some wisdom along the way. We look forward to seeing you there.

Speaking of wisdom, that provides the perfect segue to another program that the Section will offer this summer. Tentatively entitled Tips of the Trade, the program will provide a unique, skills-based, collaborative discussion aimed at identifying and sharing practical tips for increasing efficiency, facilitating legal practice management, and otherwise making the busy lives that we all lead a bit easier. Topics will range from big picture to granular, tackling issues such as effectively using technology, incorporating proven time management techniques, and streamlining reimbursement of travel expenses. The program will be spearheaded by Diversity Committee Co-Chair Deborah Robinson and me and will encourage active audience participation and sharing of suggestions and ideas. Start thinking about your best suggestions, and keep your eyes open for more details about when and where to share them!

Finally, before we "spring ahead" too far through the year, I'm excited to share that the return of flowers and sun will also bring the return of more regular Committee meetings. The Executive Committee has been discussing how the Section can best serve the interests of our members, encourage member participation, and continue to build strong communities both within the Committees and within the Section as a whole. With this in mind, we will be reinvigorating CLE-accredited Committee meetings to provide Committee/Section members an opportunity to gather more regularly, plan and present topics, and generally increase opportunities for education and networking. Committee membership is offered at no extra charge to Section members, and our Committees cover a wide array of practice areas—patent, trademark, trade secrets, litigation, cybersecurity/data privacy, and many others.

Please visit the Section's website at http://www.nysba.org/IPCommittees/ to learn more about our Committees. Also feel free to contact our NYSBA liaison, Adriana Favreau (afavreau@nysba.org), or me (eklein@kramerlevin.com), should you have any questions about Committees or want to get involved. We will be distributing more information about Committee meetings over the next few months. Stay tuned!

Erica D. Klein

Save the Date!

15th Annual Women in IP Program
Wednesday, June 7, 2017
5 to 8 p.m.
Baker & McKenzie LLP
452 Fifth Avenue, New York, NY

Panel topics include *Strategies for Success, How the IP Field Has Changed, Developing a Client Base, Mentoring Relationships* and *Achieving a Balance Between Home and Work.*

Visit www.nysba.org/IPL for details.

Privacy in M&A Transactions: Navigating the Traps

By Daniel Ilan, Emmanuel Ronco, Natascha Gerlach, and Jane Rosen

I. Introduction

One aspect of mergers and acquisitions that is receiving growing attention is the relevance of privacy issues[1] under U.S. and EU laws as well as under the laws of a growing number of other jurisdictions.[2] This article discusses the principal M&A-related privacy risks and highlights certain "traps" that are often overlooked. In Part I we discuss risks associated with a target's pre-closing privacy-related liabilities and consider ways to mitigate these risks through adequate diligence and representations in M&A agreements. In Part II, we discuss the risks associated with transferring or disclosing personally identifiable information ("personal data") of an M&A target (or a seller) to a purchaser (or prospective purchaser). In Part III, we discuss risks associated with the purchaser's post-acquisition use of such personal data.

II. Risks Associated with the Target's Pre-Closing Privacy-Related Liabilities

In M&A transactions, purchasers often assume the liabilities of the target, including for past noncompliance with privacy laws, which may result in fines, damages arising from private actions, significant harm to a company's goodwill and, in some cases, criminal liability.[3] Yet privacy-related diligence and related representations often just skim the surface.

A. Privacy Due Diligence: Key Areas of Inquiry

As part of the due diligence process, it is important to consider all applicable laws, the target's privacy policies and contractual commitments, the existing privacy standards in the target's industry and, most importantly, the target's actual practices (and its compliance with all of the foregoing).

1. Identifying the Applicable Laws

The first step in privacy diligence is ascertaining which federal, state, and non-U.S. laws might apply to the target's business. This requires an in-depth understanding of the business of the target and knowledge of the relevant laws. While many countries have enacted privacy laws, U.S. state and federal laws and EU laws, including the EU's restrictions on cross-border transfer of personal data, are most often implicated in cross-border M&A deals.

The U.S. legislative privacy framework is fragmented—no comprehensive federal legislation exists. Section 5 of the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices, has been enforced against companies that failed to safeguard personal data or comply with posted privacy policies; various other federal laws apply to select industries or to particular categories of information (and empower various federal agencies to promulgate regulations). In addition, states have passed their own privacy laws applicable to entities that operate in those states or collect personal data about individuals residing in the state. Thus, in the United States the task of simply ascertaining all laws applicable to a particular target may be a complicated endeavor. There are also industry standards and guidelines issued by industry groups, which are not legally enforceable but are considered "best practices."

EU law may apply, even to targets outside of the EU, if their data processing activities make use of equipment situated within the EU. In addition, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which will come into force on May 25, 2018, also will apply to non-EU targets that process personal data of EU-based individuals ("data subjects"), without regard to where the related equipment is situated.[4]

- ***Trap***: *An M&A target often will be subject to privacy laws in jurisdictions beyond those in which the target and its subsidiaries are incorporated. A purchaser should ascertain the jurisdictions in which the target has branches or sales offices and the jurisdictions in which it collects or stores (in local servers) personal data. Within each jurisdiction, more than one set of privacy-related laws may apply, depending on the target's business.*

2. Published Privacy Policies

An important component of privacy due diligence under U.S. law involves determining whether the target has put in place adequate privacy policies and/or terms of use and investigating whether it is in full compliance with such published policies (whether posted online or otherwise provided to customers). The FTC is the key U.S. agency regulating privacy and data security practices, and its rulings, interpretations, and opinions must be examined to understand the requirements and restrictions. The FTC has made clear that companies must make their policies describing their practices with respect to personal data publicly available and that it views failure to comply with such policies to be a violation of Section 5 of the FTC Act.[5]

EU law stipulates certain minimum information that must be provided to data subjects in order for the

Daniel Ilan is a partner in Cleary Gottlieb Steen & Hamilton's New York Office. **Emmanuel Ronco** is counsel in the firm's Paris office, **Natascha Gerlach** is senior attorney in the Brussels office, and **Jane Rosen** is an associate in the firm's New York Office. A version of this article was first published at www.clearymawatch.com/2016/10/privacy-ma-transactions-navigating-traps.

processing of their personal data to be deemed fair and lawful. Such information is often supplied by companies through a privacy policy. The data protection authorities (DPAs) of each EU member state are tasked with monitoring compliance with EU law, including the principles of fair and lawful processing. For example, the UK's DPA, the Information Commissioner's Office, has issued detailed guidance as to how a privacy policy should be drafted.[6] A target's privacy policy should be assessed by reference to such local standards or published guidance in each Member State.[7]

However, assessing whether a target's privacy policies are adequate and whether the target is in compliance with these policies requires identification of those policies that apply to the personal data in question, and that may not be a simple task:

- *Different policies applicable to different data sources.* The target may publish several different privacy policies that govern the use of personal data collected through various mechanisms (for example, through its online platform, its mobile application, or in materials sent via mail).
- *Different policies applicable to different subsidiaries, business lines, or divisions.* The target may consist of several subsidiaries or business lines, and their privacy policies may vary (including as a result of the fact that some subsidiaries or business lines were acquired from third parties, and their pre-acquisition privacy policies were maintained).
- *Updates or changes to the privacy policy.* A privacy policy may have changed over time. However, statements made in old policies (or in prior versions of the current policy) with which the target currently does not comply still may give rise to liability because the applicable privacy policy governing a particular set of personal data is the one that was made available to the persons from whom the personal data was collected when the data was collected. It thus is important to identify the policy that was in effect when the personal data concerned was collected. For example, in 2004 the FTC alleged in a complaint against Gateway Learning Corp. that it was an unfair practice for Gateway to apply the terms of a new privacy policy to information it had collected from consumers under an earlier policy ("Respondent's retroactive application of its revised privacy policy caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.").[8] Similarly, in 2011, Borders sold its customer personal data (including personal data of approximately 45 million customers) to Barnes & Noble in a bankruptcy auction. The FTC sent a letter to the court-appointed consumer privacy ombudsman stating its view that any transfer of personal data in connection with the bankruptcy should be subject to significant restrictions. The FTC specifically noted that Borders' privacy policy had changed over time, initially stating "we do not rent or sell your information to third parties" and that "we will only disclose your email address or other personal data to third parties if you expressly consent to such disclosure" and later being amended to state that customer information may be transferred if Borders engages in an M&A transaction.[9]

Once the relevant policies are identified, they should be carefully reviewed. Such diligence should focus on two main areas. First, the policies should be reviewed to determine whether they contain all the information required to be published under applicable law. Examples of the types of information that privacy laws in various jurisdictions may require include the precise categories of personal data collected; the purposes for which customers' personal data is intended to be used; the categories of third parties with whom the personal data is shared; and information about, and a mechanism to obtain consent to the use of, cookies. Second, the policies should be reviewed to determine whether they contain statements or promises with which the target does not comply. This inquiry obviously requires diligence of the target's actual practices.

Finally, if the target does not have an online privacy policy, it is important to determine whether it is required to have one. Absence of a published policy may violate a contractual obligation or give rise to violation of law. (For example, California's privacy laws require all operators of commercial websites or online services that collect personal data about individual consumers residing in California to post privacy policies.)

- ***Trap 1:*** *A purchaser should not stop inquiring even after receiving a copy of a company's privacy policy. A company can have multiple privacy policies in effect at any given time (for different platforms and/or business lines), and each of those policies could lead to privacy-related liabilities. Policies from prior years (or past versions of the current policy) also may be relevant to the extent they are different from the current ones.*
- ***Trap 2:*** *A purchaser should not be lulled into a false sense of security by a target's privacy policy that provides detailed promises regarding data security (e.g., use of firewall, encryption, and/or Secure Socket Layer technology) or personal data handling (e.g., claiming that servers reside only in a certain jurisdiction). This may indicate that the target is privacy-savvy and equipped to deal with associated risks, but it also increases the risk of non-compliance with such promises, so it should encourage further diligence.*

3. Contractual Obligations

A final area of inquiry is the target's contracts with third parties (other than its published online or offline policies). When the target is a service provider that has entered into agreements containing privacy-related requirements, assessment of compliance with such contractual obligations may be important. A particular area of concern in this context is the target's indemnification obligations and the extent to which its liabilities under each contract may be capped or otherwise limited. The nature of privacy-related exposure is such that a significant portion of the potential liability is associated with third-party claims, where users and customers bring actions (including class actions) for privacy breaches.

One area that is often overlooked in privacy diligence is the existence of contractual obligations to comply with the published policies of third-party platforms through which the target's goods or services are provided. In particular, more and more products and services are offered via third-party online platforms (including Facebook, Android and iOS apps, and Amazon Web Services), and usage of these platforms may require compliance with their privacy standards. Similarly, many third-party services used in connection with apps, such as Google Analytics and Google AdSense, require such compliance as part of their terms of service.

Finally, under EU law, when a data "controller" (an entity that determines the purposes and means of the processing of personal data) enters into a contractual arrangement with a data "processor" (a third party that processes personal data on behalf of the controller, such as a service provider), the contract must (i) be enshrined in a written agreement; (ii) require that the data processor act only on the instructions of the controller; and (iii) require the processor to comply with security obligations equivalent to those imposed on the controller under applicable national legislation. Under U.S. federal law, the Gramm-Leach-Bliley Act, as implemented by various federal agencies, generally requires companies that offer financial products or services to individuals to (i) take reasonable steps to select and retain third-party service providers capable of maintaining appropriate safeguards for the protection of non-public records and information and (ii) contractually require such service providers to implement and maintain such safeguards. Similar requirements exist in some cases under U.S. state law (e.g., Massachusetts and Maryland, where companies must require by contract that service providers implement and maintain appropriate data security measures). New York's proposed cybersecurity regulations, which would apply to certain entities operating under a license, registration, charter, certificate, permit, accreditation, or similar authorization under New York banking, insurance, or financial services laws, require such entities to have a policy of including preferred data security provisions in their agreements with third-party service providers.[10] It is therefore important to confirm that the target's agreements with third-party service providers contain provisions that comply with such laws.

- ***Trap:*** *When the target's business provides products/services through third-party platforms or relies on third-party service providers, the target may be required to comply not only with its own privacy policies but also with privacy policies and online terms of service published by these third parties.*

4. Internal Practices, Policies, and Security Measures

Review of the target's published privacy policies and contractual commitments, and the applicable privacy laws to which it is subject, is certainly necessary in order to identify the privacy-related requirements with which the target must comply. However, only an examination of the target's practices and internal policies (including those provided to employees) regarding collection, processing, storage, protection, use, disclosure, transmission, transfer, retention, and disposal of personal data can provide meaningful insight into the target's privacy-related exposure. In addition, a technical overview (even if high level) of the security measures actually employed by the target (such as encryption and breach detection), as well as any procedures and preparedness for breach notification, may be advisable in certain personal data-focused industries.

- ***Trap:*** *A purchaser should be sure to confirm that the target's actions match its words. A target that has sophisticated internal privacy policies and breach procedures still may have significant privacy exposure if it does not make sure that such policies and procedures are notified to all relevant employees and enforced across all of the target's businesses, subsidiaries, or locations.*

B. Privacy-Related Representations in M&A Agreements

Practitioners often rely on a general "compliance with laws" representation to address privacy-related risks, but such a representation does not always provide sufficient protection for a purchaser against privacy and data security risks. The "compliance with laws" representation is often heavily qualified and covers a limited period of time (e.g., the target's operation during the year prior to the transaction), which may not be appropriate for privacy matters. The representation also fails to cover certain issues of concern in the privacy context.

Privacy-specific representations can cover not only compliance with privacy laws but also compliance with contractual obligations (and terms of use) relating to personal data and implementation of data security measures that are not necessarily required by law or contract, such as industry-standard security measures (e.g., payment card industry standards), disaster recovery plans and procedures, and backup equipment and facilities. Such representations may also cover threatened enforcement actions and privacy-related complaints, as well as loss of or unauthorized access to personal data in the past (whether or not constituting a violation of law at the time), given the reputational damage to which such issues can give rise. Finally, while a "compliance with laws" representation does not include any disclosure requirements, a privacy representation can serve to force the target to disclose information about its policies and practices that is crucial to understanding the magnitude of the privacy risks.

Privacy-specific representations, tailored to include the foregoing matters as appropriate, should be considered whenever the risks discussed in this article are present.

- ***Trap:*** *A purchaser should not assume the "compliance with laws" representation will necessarily cover privacy matters adequately. A privacy representation that is tailored to the risks associated with the target's handling of personal data can be used, when appropriate, to cover important areas beyond mere compliance with applicable law.*

A word of caution: privacy-related representations in M&A agreements can offer a certain level of comfort to a purchaser, and they should therefore be negotiated carefully, but they are often qualified by knowledge and/or materiality, and any indemnity for breach of the representations is subject to significant limitations. And even if damages are awarded as a result of an indemnity claim relating to breach of privacy-related representations, they may not be sufficient to compensate for the type of public relations and customer relationship damage often associated with privacy failures.

"A word of caution: privacy-related representations in M&A agreements can offer a certain level of comfort to a purchaser, and they should therefore be negotiated carefully, but they are often qualified by knowledge and/or materiality, and any indemnity for breach of the representations is subject to significant limitations."

III. Risks Associated with Transferring or Disclosing Target's (or Seller's) Personal Data to Purchaser

M&A transactions often involve the disclosure or transfer of personal data from a seller to a purchaser. This normally includes personal data associated with the acquired target (or acquired assets), such as data relating to employees, customers, users, contractors, suppliers, and business partners. While most personal data is transferred at closing, some disclosures also may occur between signing and closing.

A. Risks Associated with Disclosure Between Signing and Closing

M&A lawyers are not always aware of the risks associated with disclosure of personal data between signing and closing (when signing and closing are not simultaneous). In particular, M&A agreements often contain a clause providing for access to books and records between signing and closing, enabling the purchaser to request certain types of data it reasonably needs, including for purposes of integration planning. But it is a mistake to assume that because a deal is signed, personal data relating to the target business may be shared freely between the purchaser and the seller. While some M&A agreements state that the seller need not provide access to information prior to closing if providing such access would be in violation of applicable law, such a carve-out is not necessarily applied in practice and, in any case, understanding whether a particular disclosure is in violation of privacy laws may be difficult.

1. U.S. Law

Under U.S. law, the pre-closing disclosure of personal data must comply with all relevant state laws, contractual restrictions, and any promises made about the treatment of personal data in the target's published privacy policy. As discussed in Part I, the FTC has made clear that it views failure to comply with published privacy policies as a violation of Section 5 of the FTC Act, which bars unfair or deceptive acts or practices. Relevant state laws include the California Online Privacy Protection Act of 2003, which requires all operators of commercial websites and online services that collect California residents' personal data through a website to identify categories of third-party persons or entities with which the operator may share the personal data.

Ideally, the target's privacy policy will contain a clear statement that a transfer or disclosure of personal data may occur in connection with an M&A transaction, including prior to consummation of the transaction (it may not suffice to state that personal data may be shared "upon" or "following" a merger or sale of the company or its businesses, given that prior to closing the transaction is not consummated). In addition, it will be important to ensure that the purchaser safeguards the information to the extent required by applicable law;[11] does not further disclose the personal data; and does not use it in any way that violates the applicable privacy policy (including any use that is not necessary for integration planning or consummation of the M&A transaction). It therefore may be advisable for the seller to enter into a "data protection agreement" with the purchaser with respect to such obligations. A data protection agreement also can include requirements to abide by any restrictions contained in the seller's/target's contracts with third parties to the extent related to the personal data shared prior to closing.

2. EU Law

Under EU law, the disclosure of data relating to data subjects must comply with the laws implementing EU Directive 95/46/EC of October 24, 1995 (the "Directive") in each Member State.[12] Generally, for the "processing" (a broad concept that includes transfer or disclosure) of personal data to be permitted, it must be based on one of the grounds enumerated in the Directive, among which the most relevant to a pre-closing M&A-related disclosure are:

- *Legitimate interest of the data controller or the data recipient, provided it is not incompatible with the interests or the fundamental rights and liberties of the data subject*. The so-called "legitimate interest" ground is frequently relied on in M&A transactions since it is open-ended, making it possible to argue that it is in the legitimate interest of the purchaser to receive the data (i.e., to prepare for the acquisition). However, certain data subjects may claim to have an interest in keeping their data confidential, at least until the transaction is close to completion. In practice, it is often advisable to try to wait until all or most of the conditions to closing of the transaction have been satisfied before transferring personal data based on this ground.

- *Consent of the data subject.* In an M&A context, it often is impractical to rely on the consent of the data subjects. The "consent" ground is therefore only used when just a few individuals are concerned, and they have reason to be aware of the contemplated transaction (e.g., major customers whose approval is required in order to assign the customer contracts to the purchaser). Note that the data subject's consent to the transfer may be required in certain circumstances, including when "sensitive data" are involved (e.g., where health, religion, or union membership appear in, or can be deduced from, employee records).[13]

- *Performance of a contract with the data subject*. This ground is typically used in the M&A context when the assets sold include contracts and personal data that must be transferred for these contracts to continue to be performed.

In addition to the existence of one the foregoing grounds for pre-closing disclosure, compliance with EU law generally also would require that the personal data transferred to the purchaser prior to closing not be inadequate or excessive. In other words, the only data fields that should be transferred before closing are those that are necessary for the new employer to prepare for completion of the transaction (such as, in the case of data obtained for HR-related purposes, positions and salaries but potentially not home addresses or bank account details).

Finally, certain additional steps may be required in the EU, particularly notice, inclusion of the European Commission's standard contractual clauses (the "Model Clauses"), and potential Data Protection Authorities ("DPAs") filings. Since these steps are generally similar whether the disclosure/transfer occurs prior to or at closing, we discuss them in Part II.B below.

- ***Trap****: It is a mistake to assume that sharing personal data is allowed once an M&A deal is signed and before it is consummated. In the United States, language in privacy policies may not be broad enough to fully address this situation, and the purchaser's use of such data must be strictly circumscribed in light of state law and contractual obligations. In the EU, several steps must be taken before transferring personal data, and, as a general rule, because the disclosure of data is considered more legitimate as the deal progresses and closing becomes more certain, access to data should be tailored to what is necessary for each phase of the deal.*

B. Risks Associated with Transfers at Closing

At closing, the purchaser will expect to receive all of the personal data related to the acquired business. Depending on the nature of the transaction (e.g., a spin-off of a stand-alone subsidiary) the transferred personal data may in fact remain hosted on the target's systems that are sold as part of the transaction.

1. U.S. Law

Under U.S. law, it will again be important to consider both state law and the FTC Act, as well as any contractual commitments made by the target/seller in agreements involving collection of personal data. In a sale out of bankruptcy, the Bankruptcy Code also will be implicated. In all cases, a decisive factor in analyzing the legality of a transfer of personal data will be the promises contained in the target's published privacy policy.

Asset purchases vs. mergers or share purchases. Arguably, whenever a third-party entity gains access to personal data as a result of an M&A transaction, there is a "transfer" of such personal data that could violate privacy laws. In other words, a "transfer" may technically occur even in a share purchase of a target company pursuant to which all of the company's operations remain unchanged (other than its ultimate control) but following which the purchaser and its affiliates have access to such company's data. However, enforcement activity thus far has not focused on "transfers" that occur in mergers or share purchases and instead has focused only on the eventual uses of such data by the purchaser (as discussed in Part III below). By contrast, in the context of asset sales, even the *data transfer itself* has been subject to scrutiny by the FTC, state regulators, and (as applicable) bankruptcy courts. The fact pattern of notable cases has involved a company privacy policy that promised not to sell or transfer personal data to third parties (without any exceptions for sales in a restructuring, asset sale, insolvency, or bankruptcy) and a desire by the company to then sell personal data as a stand-alone asset or in the context of a broader asset sale transaction (such as a sale of a business).

FTC vs. state regulators vs. bankruptcy courts. As described below, the FTC, state regulators, and bankruptcy courts have taken slightly different approaches to such asset sales.

- *FTC approach—Either (A) opt-in consent to the data transfer or (B) purchaser must be in the same line of business as target, must comply with target's existing privacy policy, and must obtain opt-in consent to any material policy changes.* The FTC often cites a settlement it reached with internet retailer Toysmart in 2000 which allowed Toysmart, after it ceased operations, to transfer customer personal data to a third party in spite of its privacy policy stating that such personal data would "never be shared with a third party." The FTC had sued to block Toysmart's sale of its customer database, alleging a violation of Section 5 of the FTC Act. Under the Toysmart settlement, Toysmart was able to sell the customer data but: (i) not as a stand-alone asset; (ii) only to a purchaser engaged in substantially the same lines of business as Toysmart; and (iii) only to a purchaser who agreed to be bound by and adhere to the terms of Toysmart's privacy policy and to obtain affirmative (opt-in) consent from consumers for any material changes to the policy that affect information collected under the Toysmart policy (hereinafter, the "Toysmart Principles").[14] As an alternative to the Toysmart Principles, the FTC proposed (in the RadioShack and Borders cases, discussed below) requiring the target to obtain affirmative (opt-in) consent of the data subjects to the transfer of their data to the purchaser and to purge the data of those who did not consent.[15]
- *State regulators approach in RadioShack—Toysmart Principle "iii" plus notice of the data transfer and right to opt out*. In 2015, Attorneys General in 38 states challenged the bankruptcy sale by RadioShack of its personal data (RadioShack's privacy policy stated: "We will not sell or rent your personally identifiable information to anyone at any time."). The states reached a settlement with RadioShack that limited the type of information to be transferred (e.g., only customer e-mail addresses that were active within the two-year period prior to the petition date, and only specific data fields collected in the five-year period preceding the petition, such as store number, price, and SKU number for a transaction). In addition, the settlement required the purchaser to (a) accept clause "iii" of the FTC's Toysmart Principles (being bound by RadioShack's privacy policies and requiring opt-in consent for any material changes that would affect the transferred data) and (b) provide notice and opt-out opportunities to RadioShack customers to enable them to exclude their personal data from the sale.[16]
- *Bankruptcy court—RadioShack (opt in to material policy changes) vs. Borders (opt out of material policy changes*). While in 2015 the bankruptcy court for the District of Delaware endorsed the above settlement reached between the states and RadioShack, four years earlier, in 2011, the bankruptcy court for the Southern District of New York reached a somewhat different conclusion in the *Borders* case.[17] The FTC raised concerns when Borders planned to sell personal data of approximately 45 million customers to Barnes & Noble in a bankruptcy auction. Borders' privacy policy had changed over time, initially stating "we do not rent or sell your information to third parties" and later stating that customer information might be transferred if Borders engaged in an M&A transaction. The bankruptcy court declined to accept the FTC's approach described above and instead required Barnes & Noble to (i) adopt a privacy policy similar to the Borders' policy and provide existing customers an ability to opt out of any material changes to the policy and (ii) provide notice and a data transfer opt-out mechanism, as in *RadioShack*. The court also required Barnes & Noble to honor prior requests by consumers (made to Borders) to opt out of receiving marketing messages (unless such consumers were also Barnes & Noble customers who had not opted out of marketing messages).

In each of the above cases, there was no express provision in the applicable privacy policy allowing for the sale of personal data in the event of a restructuring, asset sale, or bankruptcy (or even in the event of a merger or acquisition). The inclusion of such a provision is advisable, not only in privacy policies but also in contracts containing commitments with respect to treatment of personal data.

- ***Trap****: While "transfers" of personal data in connection with mergers or share purchases have not been criticized by regulators to date, asset sales involving transfer of personal data have been subject to close scrutiny in the United States, and certain steps may be required when planning such transfers in order to prevent exposure to potential liability.*

2. EU Law

In the EU, a transfer of personal data at closing as part of an M&A transaction requires showing that at least one of the grounds for transfer discussed in Part II.A above ("legitimate interest," consent, or necessary for performance of a contract) is found. This should be easier than in the case of a pre-closing disclosure given that once the transaction has been completed, the purchaser should have a "legitimate interest" in processing the acquired personal data. In addition, the following steps should be considered:

- *The data subjects should be informed of the transfer*. The seller should give the data subjects certain information about the transfer of their data to a third party no later than at the time of the transfer, unless such disclosure would "involve a disproportionate effort." Such information does not necessarily need to be given to each data subject individually (a posting on a website may suffice, depending on the circumstances). A right to opt out of the transfer may need to be granted.[18]

- *Additional steps may have to be taken in the case of transfers of data outside the European Economic Area ("EEA").* EU law imposes stringent regulatory constraints on the transfer of personal data outside the EEA to a country that is not deemed to have an adequate level of data protection,[19] which includes the United States, unless the transfer is to a company that self-certified under the EU-U.S. Privacy Shield.[20] Consent of the data subjects will render the transfer lawful under EU law, but it is often difficult or very burdensome to obtain. In the absence of Privacy Shield certification or individual consent from the data subjects, an M&A-related transfer should be made only after a personal data transfer agreement that incorporates the Model Clauses has been entered into between the parties. The Model Clauses place recipients of personal data under contractual obligations similar to those required in the EU. Note, however, that as discussed below, in certain EU countries (e.g., France) the data transfer agreement (containing the Model Clauses) would need to be approved by the local DPA, which could take up to a few months and could render the Model Clause option inappropriate in some cases.

  - ***Trap****: The decisive factor for determining whether a transfer of personal data outside the EEA occurs (which may require usage of Model Clauses or self-certification under the EU-U.S. Privacy Shield) is not whether the seller/target is an EU corporation while the purchaser is not; it is whether personal data stored within the EEA is transferred (physically or electronically) to locations outside the EEA by an entity that is subject to EU jurisdiction.*

- *Verify whether filings with Data Protection Authorities must be made*. Depending on the national law applicable to the seller, the target, or the purchaser, the transfer of personal data may have to be notified to or authorized by one or several DPAs.[21] Filing requirements vary among Member States and should be reviewed on a case-by-case basis. Planning ahead is important, as a DPA approval, if needed, may take a long time. By preparing for this in advance, a purchaser can ensure minimum disruption to the target's personal data processing activities.

IV. Risks Associated with Post-Acquisition Integration of Personal Data

Immediately after closing, the purchaser must consider how to integrate the target's personal data and the target's IT systems into its own data and systems. Problems arise if either the target's practices do not comply with the purchaser's privacy policies (or contractual obligations) or if the purchaser's practices do not comply with the target's privacy policies (or contractual obligations that survived the sale, including those assumed by the purchaser).

A. Target's Practices and Policies More Robust Than Purchaser's

Even where the consummation of an M&A transaction and the correlating "transfer" of personal data to the purchaser does not violate privacy laws, problems arise when the purchaser's practices are below the standard the target committed to in its pre-acquisition privacy policy. For example, the target's policy may state that certain types of information are not collected or that personal data is used only for certain purposes, shared only with certain third parties, stored only in certain geographic regions, or is de-identified or encrypted. However, the purchaser may have different privacy policies and practices that may conflict with these statements.

Facebook is currently under scrutiny worldwide as it grapples with the aforementioned risks resulting from its acquisition of WhatsApp in 2014. Although at the time of the acquisition WhatsApp's privacy policy contained an express provision stating that it reserved the right to transfer users' personal data to a third party in the event of a merger or acquisition, the FTC took the position that post-acquisition, WhatsApp had to continue to abide by its original privacy policy (which promised not to share personal data with third-party companies for commercial or marketing use, except with users' consent or as part of programs or features, users would be able to opt in or opt out of). At the time the sale was announced, both Facebook and WhatsApp promised consumers that after the acquisition, WhatsApp would continue to operate autonomously and that nothing would change for its users. However, in August 2016, WhatsApp changed its privacy policy to allow it to share customers' personal data (including pre-acquisition data) with Facebook unless customers opted out of such sharing within 30 days. Consumer privacy watchdog groups and other organizations filed a formal complaint with the FTC and urged the FTC to investigate WhatsApp and Facebook.

Guidance on how the FTC views this issue in the context of M&A is found in the FTC's "business blog" published on March 2015, which was prompted at least in part by Facebook's acquisition of WhatsApp.[22] The FTC blog set forth several important principles:

- The target's pre-acquisition policies continue to govern with respect to personal data collected by the target. As the FTC stated: "One company's purchase of another doesn't nullify the privacy promises made when the data was first collected."
- With respect to data collected by the target prior to the acquisition, the purchaser may either comply with the target's pre-existing policies or allow opt in. The purchaser can simply abide by the target's pre-acquisition promises, i.e., handle the data as promised when the target collected it from consumers. Alternatively, if it wishes to materially change how the data is processed, it must obtain affirmative (opt-in) consent from the individuals to whom the data pertains.
- With respect to data collected by the acquired business or target (if it survives) post-acquisition, the purchaser must provide notice & opt out. If the purchaser desires to change its practices going forward with respect to newly collected personal data, it will need to provide sufficient notice of the change and an opportunity for users to opt out. Per the FTC blog: "Simply revising the language in a privacy policy or user agreement isn't sufficient because existing customers may have viewed the original policy and may reasonably assume it's still in effect. Although it may not be necessary to provide affirmative express consent, the notice and choice must be sufficiently prominent and robust to ensure that existing customers can see the notice and easily exercise their choices."
- With respect to any data of an individual who does not opt in (for pre-acquisition data) or who exercises the right to opt out (for post-acquisition data), the purchaser will have to comply with the applicable pre-acquisition privacy policy of the target.

Thus, where a target's privacy policy and data privacy practices are more robust than the purchaser's, if the purchaser wishes to integrate the target's personal data into its systems or otherwise use the data collected by the target before the acquisition, the purchaser may need to bring its own data privacy practices into compliance with the target's applicable privacy policy. If updating the purchaser's practices and systems is not feasible or desirable, the purchaser will need to segregate the data.

Finally, the target may collect certain personal data that is subject to additional regulation (such as health care data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the personal data of children younger than 13 subject to the Children's Online Privacy Protection Rule). If the purchaser wishes to integrate such personal data and use it, the purchaser will need to ensure compliance with all relevant regulations.

We note that the above discussion relates to U.S. law, where most of the focus is on the target's and purchaser's privacy policies and promises. In the EU, the focus in review of post-acquisition practices (assuming the transfer of the data itself is lawful as discussed in Part II.A above) is on the purposes for which the data initially was collected. The use of the data by the purchaser must be in a manner consistent with the specified (and legitimate) purposes for which it was obtained by the target in the first place. As an illustration, in the case of data obtained for HR-related purposes such as payroll and administrative management, the data should continue being used only for these same purposes by the purchaser.

- ***Trap**: As a purchaser, it is not enough to establish that the target's practices are compliant with your privacy policies. You may be violating the law if your use of data collected by the target does not comply with the target's policy (or, in the EU, if your use of such data is inconsistent with the specified purposes for which it was collected by the target).*

B. Target's Practices and Policies Less Robust Than Purchaser's

Another set of problems arises if a target's data privacy practices are less protective of privacy than the purchaser's and are therefore incompatible with the purchaser's privacy policies (e.g., the personal data collected by the target may contain credit card information or other data fields that the purchaser promises not to collect or store, or the target may use third-party service providers under terms that are inconsistent with statements in the purchaser's privacy policy). While the purchaser's privacy policies may be amended to remove promises that are incompatible with the practices of the target, the amended policy will be effective only for newly-collected personal data (data collected after the date the amended policy is made effective) and, consistent with the FTC blog, customers must receive notice of the change and an opportunity to exercise an opt-out choice. In addition, the purchaser may suffer a reputational hit from lowering the protections in its privacy policy. Furthermore, the purchaser will need opt-in consent for any changes that will affect customers' previously collected data.

The most reasonable approach will likely be for the purchaser to either (1) maintain the target as a separate entity/division that does not use the purchaser's data or (2) bring the target's practices into compliance with the purchaser's previous promises (though this could involve significant costs).

- ***Trap**: Even where the "transfer" of personal data to the purchaser resulting from an M&A transaction is lawful, post-closing processing of personal data, either by the purchaser (of target's data) or the surviving target (of purchaser's data) that conflicts with privacy policies applicable when such data was collected can lead to liability.*

V. Conclusion

We have outlined some of the complex privacy issues that arise at each stage of an M&A transaction. Prior to signing, a purchaser's due diligence will involve multiple areas of inquiry to determine all potential risks associated with the target's existing privacy-related liabilities, and for greatest protection, privacy-specific representations in M&A agreements may be warranted. Between signing and closing, both sellers and purchasers should remain cautious in the disclosure of personal data and should seek counsel both with respect to the content of any disclosures and the disclosure process. After closing of the transaction, the purchaser will need to consider carefully what steps must be taken to enable its use of the acquired data and to ensure such use complies with all applicable laws. Given the rapidly evolving nature of privacy laws, it is advisable to consult with privacy counsel at each stage of a transaction to most effectively mitigate these and other associated risks.

Endnotes

1. Throughout this article, we use the term "privacy" (or "privacy issues" or "privacy laws") broadly as including cybersecurity, data protection and data security as related to personal data (and related issues and laws).
2. This article focuses on U.S. and EU law, but we note that several other jurisdictions have passed or are adopting strict privacy laws. Among those are countries recognized by the European Commission as having an "adequate level" of protection for all or certain types of personal data processing (i.e., as of the date of this article, Andorra, Argentina, Canada (commercial organizations), the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay—please visit http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm) as well as other states such as Brazil, Singapore and South Korea. In any cross-border transaction, the laws of all relevant jurisdictions should be examined.
3. The FTC has also been successful in obtaining monetary awards against companies in actions enforcing its orders. Notably, in 2015, LifeLock agreed to a $100 million settlement with the FTC, after the FTC charged that LifeLock violated the terms of a 2010 federal court order requiring the company to secure consumers' personal information and prohibiting the company from deceptive advertising.
4. For further information on the new GDPR framework, please refer to our May 13, 2016 Alert Memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201650.pdf.
5. In 2014, the FTC filed a complaint against Fandango and Credit Karma charging that the companies had deceived consumers. Both had made representations that they could secure their customers' personal data, but according to the FTC, both had failed to properly implement SSL encryption.
6. The ICO's "*Privacy notices—code of practice*" can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.
7. Additionally, Member State consumer protection laws should also be considered as these may provide for additional information requirements (see, for example, the German Act Against Unfair Competition, which prohibits unfair commercial practices).
8. *See* https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf.
9. *See* https://www.ftc.gov/news-events/press-releases/2011/09/ftc-seeks-protection-personal-customer-information-borders.
10. For further information on New York's proposed cybersecurity regulations, please refer to our September 20, 2016 Alert Memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-word-version-201685.pdf.
11. For example, Massachusetts General Law Chapter 93H and its regulations 201 CMR 17.00 impose requirements on all companies who receive, store, maintain, process or otherwise have access to personal data of the state's residents to develop, implement and maintain a comprehensive information security program that contains administrative, technical and physical safeguards to protect the data.
12. While the Directive provides a harmonized regulatory data protection framework that is applicable throughout the EU, there are a few areas where national law differs in each Member State. Starting on May 25, 2018, the Directive and the national laws implementing it will largely be replaced by the GDPR, which will enhance existing legal requirements, create new rules and set out significant fines for organizations failing to comply. For further information on the key changes to be anticipated under the GDPR regime, please refer to our May 13, 2016 Alert Memorandum (https://www.clearygottlieb.com/news-and-insights/publication-listing/general-data-protection-regulation-key-changes-and-implications).
13. Sensitive personal data may be transferred only where the data subject has provided his or her explicit and fully informed consent, or where a legal obligation exists in the context of employment which makes the transfer necessary. The advice of local counsel should be sought before relying on the "legal obligation" ground in connection with the transfer of sensitive employee data.
14. For the Stipulation and Order Establishing Conditions on Sale of Customer Information, *see* https://www.ftc.gov/sites/default/files/documents/cases/toysmarttbankruptcy.1.htm.
15. *See* FTC letter to the court-appointed Consumer Privacy Ombudsman in *RadioShack*, dated May 16, 2015, https://www.ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf.
16. *See In re RadioShack Corporation, et al.*, No. 15-10197 (BLS) (Bankr. D. Del.).
17. *See In re Borders Group, Inc., et al.*, No. 11-10614 MG, 2011 WL 5520261 (Bankr. S.D.N.Y. Sept. 27, 2011).
18. In 2001, the French DPA declared (in the context of a merger of three companies) that personal data files may only be assigned or made available to a third party on the condition that data subjects be given advance notice as well as the right to object to such transfer. In Germany, it is necessary to provide notice of the transfer in the context of the transaction with a deadline to object where the transferred data goes beyond so-called "list data" (name and postal address). The Bavaria DPA issued fines to a buyer and target in an asset deal in 2015 where customer data was transferred without the parties providing the customers with a deadline to object to the transfer prior to the transaction.
19. *See supra* note 2.
20. Commission Implementing Decision of 12.07.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (the "EU-U.S. Privacy Shield"). For further information on the EU-U.S Privacy Shield and the invalidation of its predecessor (the EU-U.S. Safe Harbor), please refer to our August 2, 2016 Alert Memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201679.pdf).
21. The GDPR provides for a "*one-stop-shop*" mechanism under which data controllers established in the EU will be able to register with one DPA only (in their country of "main establishment").
22. *See* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

The Alliance for Open Media: The Latest Challenge to Patent Pools

By Brad Sarna and Jordan Salins

I. Introduction

The Alliance for Open Media (AOM) represents the latest challenge to patent pool licensing. Frustrated with licensing fees that they perceive to be unreasonably high, tech titans such as Microsoft, Amazon, Google, and Intel created AOM to develop and release a royalty-free, technically superior version of two widely used video encoding/decoding (codec) standards, H.264 and H.265. Although the success of AOM has yet to be determined, it will be interesting to see whether this challenge to the patent pool licensing business model spreads to other industries such as telecommunications, security, transportation and logistics, energy generation and distribution, and pharmaceuticals. Many in the codec industry will be watching to see the impact of this model on technological innovation, intercompany collaboration, and intellectual property-related litigation.

Intercompany collaboration related to the sharing of IP is becoming increasingly common as companies seek to both inspire growth and encourage innovation. In addition to increasing innovation, companies that engage in collaboration are looking to reduce or even eliminate licensing fees they are required to pay to other entities, such as patent pools and patent licensing organizations. Some argue that patent pools encourage competition and innovation through the sharing of intellectual property, as companies can use technology to which they otherwise would not have rights in various products and services. Others argue, however, that patent pools promote anti-competitive behavior by encouraging collusion. According to a study for the U.S. National Library of Medicine, National Institutes of Health, patent pools "enable a group of major players to form a cartel that excludes new competitors."[1]

II. Video Codecs in Practice

MPEG LA is one of many organizations that licenses patent pools. It describes itself as "the world's leading packager of patent pools for standards and other technology platforms used in consumer electronics, as well as in chemical, eCommerce, education, energy, environment, healthcare and biotechnology, manufacturing and materials, transportation, and wireless technology."[2] MPEG LA packages and licenses the H.264 and H.265 codec standards that are ubiquitous in the encoding, sharing, and decoding of streaming video around the world. Licensees include many large companies such as Netflix, Google, and Microsoft. Figure 1 lists the primary competing and related video encoding/decoding standards.

Figure 1. Video Encoding/Decoding Standards

Standard Name	Release Date	Licensors/ Owner	Commercial Applications	Royalties	Status
H.264 (aka AVC)	2003[3]	MPEG LA	YouTube, iTunes, Adobe Flash Player, cable TV, Blu-ray players, and others	<100K units/year[4]: no royalty; 100K–5M units/year: $0.20 per unit; 5M+ units/year: $0.10 per unit (royalty cap of $9.75M per year)[5]	In use
H.265 (aka HEVC)	2013[6]	MPEG LA, HEVC Advance, Technicolor SA	Same as H.264	<100K units/year: no royalty; 100K+ units/year: $0.20 per unit (royalty cap of $25M per year);[7] 0.5% of all revenue derived from HEVC-encoded video	In use
Thor[8]	Unknown	Cisco	Unknown	Royalty-free	In development
Daala[9]	Unknown	Mozilla, Xiph.org Foundation, and others	Unknown	Royalty-free	In development
VP9 and VP10[10]	Unknown	Google	Unknown	Royalty-free	In development
AV1	March 2017 (expected)[11]	Alliance for Open Media	Same as H.264 and H.265	Royalty-free	In development

The H.265 video compression standard was released in 2013 (and subsequently updated several times) as a successor to the H.264 video standard. As with H.264, MPEG LA is the primary licensing entity for H.265. However, MPEG LA is charging higher per-unit royalties at the 5M+ unit level and also has increased the royalty cap from $9.75M per year to $25.0M per year. In addition, a new patent licensing pool, called HEVC Advance, is now demanding payments for all streaming video using the H.265 technology: 0.5% of all revenue derived from HEVC-encoded video. This increase in licensing fees from those for H.264 has frustrated many companies and prompted licensees to scramble for alternatives. According to an analysis prepared by Cisco Systems, the cost per unit to license H.265 can be 16 times higher than that to license H.264.[12] A principal analyst at the research firm Frost & Sullivan described the new H.265 license fees as "unreasonable" and "greedy."[13]

III. Creation of the Alliance for Open Media

In September 2015, Amazon, Cisco, Google, Intel, Microsoft, Mozilla, and Netflix announced the creation of AOM. According to a press release, AOM is "an open source project that will develop next-generation media formats, codecs, and technologies in the public interest."[14] The goal of AOM is to create an interoperable, optimized, scalable, and royalty-free video codec, known as AV1, to replace both the H.264 and H.265 video standards, thereby obviating the need for companies to pay licensing fees to MPEG LA.[15]

Since AOM's founding, ARM, Nvidia, Vidyo, and several other companies have joined the alliance and are actively contributing to the development of the AV1 codec. Each member company is responsible for sharing its IP and for the joint development of new technology. By including both hardware (Nvidia, AMD, ARM, etc.) and software (Netflix, Google, Amazon, etc.) companies in the alliance, AOM ensures the codec will be hardware-friendly and will work seamlessly on a variety of Internet browsers and mobile devices. According to Gabe Frost, executive director of AOM, "It's crucial that hardware manufacturers are engaged in the designs so there are no barriers to transitioning hardware support into the hardware road map."[16]

A. Legal Risks to the AOM Model

Despite the many high-profile member companies in AOM, there is no guarantee AV1 will be able to replace H.264 and H.265 as the leading video codec standard. This new alliance could increase the likelihood of IP-related litigation, as AV1 may include certain IP that conflicts with existing video codec patents.[17] Most members of AOM own and aggressively protect large patent portfolios—a common IP strategy used by tech companies. For example, in 2013, Microsoft was awarded $14.5 million in a FRAND patent licensing case involving the fair use of video compression patents developed by Motorola.[18] While some argue that AOM opens the door to increased patent litigation, others believe close collaboration among AOM members will mitigate the risk of future IP-related litigation. In fact, Google and Microsoft, which have mutually engaged in lengthy patent-related litigation, released a statement shortly after the creation of AOM pledging to work together more closely on IP issues: "Google and Microsoft have agreed to collaborate on certain patent matters and anticipate working together in other areas in the future to benefit our customers."[19] How closely AOM members collaborate with one another on the development of AV1, and the effect of AOM on potential future IP-related litigation, remains to be seen.

B. Industry Risks

Furthermore, there are two notable absences from the AOM membership list: Apple and Facebook. Apple uses a different standard for videos sold in the Apple iTunes store, so it has not had to pay royalties to MPEG LA.[20, 21] Also, it is believed that Facebook is ramping up its video efforts as it attempts to create a proprietary video codec technology.[22] These two companies ultimately could compete with AOM, and their absence from the group poses another risk to the potential success of AV1. If either company creates its own video codec technology or blocks AV1 from being implemented and used on its platforms, AV1 could lose out on much of the commercial prevalence that H.264 and H.265 have enjoyed in recent years.

C. Technical Risks

In addition, it is not clear that AV1 will be released on schedule. When AOM was originally announced in September 2015, the expected release date of AV1 was listed as late 2016/early 2017. As of this writing, however, there have been no updates on AV1's release status for several months. If AV1 falls behind schedule, is delayed, or fails to make significant progress, it is possible that a different video codec technology will be released and lead the industry in a different direction, rendering AOM obsolete.

Finally, there are questions about AV1's ability to match the technical capabilities of H.264 and H.265. Although AV1 aims to improve bitrate efficiency over H.265 by 50 percent,[23] the complexity of the technology and the scope of the project pose challenges for the AV1 developers. If AV1 does not ultimately hit its goals and technical specifications, companies may continue using the H.264 and H.265 codecs, rendering AV1 and AOM obsolete.

Brad Sarna is a Director—Intellectual Property Services at Stout Risius Ross, Inc., and **Jordan Salins** is a Senior Analyst—Intellectual Property Services at the firm. This article is intended for general information purposes only and is not intended to provide, and should not be used in lieu of, professional advice. All opinions expressed in these articles are those of the authors and do not necessarily reflect the views of Stout Risius Ross, Inc.

IV. Will AOM Influence Other Industries?

AOM is just one of several recent moves by companies to create royalty-free alternatives to technologies and standards through technical collaboration and open sourcing of IP. In another recent instance, Panasonic pledged in March 2015 to open source and share certain IP in order to provide royalty-free access to technology aimed at speeding the development of the Internet of Things.[24]

Although the alliance is an unproven one with risks and uncertainty, it could, if successful, end the era of royalty-based video codecs while creating an open, innovation-based platform. In addition, AOM's success might inspire companies in other industries to follow suit. Patent pool licensing of standard essential patents exists in almost every industry—telecommunications, security, transportation and logistics, energy generation and distribution, pharmaceutical, etc.—and companies in these industries pay patent licensing fees to firms like MPEG LA. If these companies begin to view these licensing fees as unfair or unreasonable (or if companies believe they can develop alternative, non-infringing technologies), perhaps they will develop alliances similar to AOM. It will be interesting to see how the success or failure of AOM will impact future patent pool licensing in other industries.

Endnotes

1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2831195/.
2. http://www.mpegla.com/main/Pages/About.aspx.
3. https://www.itu.int/rec/T-REC-H.264.
4. A unit is defined as a decoder, an encoder, or a product consisting of one decoder and one encoder.
5. http://www.mpegla.com/main/programs/AVC/Documents/avcweb.pdf.
6. http://www.streamingmedia.com/Articles/Editorial/What-Is-.../What-Is-HEVC-(H.265)-87765.aspx; updated versions of H.265 have since been released.
7. http://www.mpegla.com/main/programs/HEVC/Documents/HEVCweb.pdf.
8. http://blogs.cisco.com/collaboration/world-meet-thor-a-project-to-hammer-out-a-royalty-free-video-codec.
9. https://xiph.org/daala/.
10. https://gigaom.com/2014/01/02/youtube-4k-streaming-vp9/.
11. http://www.streamingmedia.com/Articles/Editorial/-110383.aspx.
12. http://blogs.cisco.com/collaboration/world-meet-thor-a-project-to-hammer-out-a-royalty-free-video-codec.
13. http://www.huffingtonpost.com/dan-rayburn/new-patent-pool-wants-05-_b_7851618.html.
14. http://aomedia.org/press-releases/alliance-to-deliver-next-generation-open-media-formats/.
15. http://aomedia.org/press-releases/alliance-to-deliver-next-generation-open-media-formats/.
16. http://www.streamingmedia.com/Articles/Editorial/Featured-Articles/A-Progress-Report-The-Alliance-for-Open-Media-and-the-AV1-Codec-110383.aspx.
17. http://www.streamingmedia.com/Articles/Editorial/What-Is-.../What-is-AV1-111497.aspx.
18. http://www.law360.com/articles/470243/jury-orders-motorola-to-pay-microsoft-14-5m-in-frand-row.
19. https://www.bloomberg.com/news/articles/2015-09-30/google-microsoft-resolve-global-patent-fight-over-phones-xbox.
20. http://www.businessinsider.com/amazon-google-microsoft-netflix-form-alliance-for-open-media-2015-9.
21. https://www.wired.com/2015/09/techs-biggest-names-unite-create-new-video-format/.
22. https://www.cnet.com/news/tech-giants-join-forces-to-hasten-high-quality-online-video/.
23. https://www.epiphan.com/blog/4k-codecs-simplified-and-what-they-mean-for-you/.
24. http://shop.panasonic.com/about-us-latest-news-press-releases/Content03232015092444644.html.

Using Third Parties’ Trademarks: Unpacking Commerciality, Competition, and Confusion

By Brooke Erdos Singer and Maxine Sharavsky

I. Introduction

Drawing the line between permissible and impermissible uses of a third party’s trademark (whether in a competitive context or otherwise) is a matter of some complexity, involving consideration of the bounds of First Amendment protected speech, the distinctions between commercial and non-commercial use, defenses to infringement and dilution that are available for purposes of allowing competition and critique, and, of course, the likelihood of consumer confusion as to the source or endorsement of goods or services. Further complicating the analysis is the lack of consistency in the treatment of these topics from jurisdiction to jurisdiction.

This article sets forth a basic framework for considering whether the use of a third party’s trademark is permissible, with particular emphasis on uses in advertising and digital contexts. It also presents some hypothetical examples to explore the boundaries and potential pitfalls associated with uses of third-party marks.[1]

II. A Framework for Use of Third Parties’ Trademarks

A. Distinguishing Between Commercial and Non-Commercial Use

Both the Supreme Court’s First Amendment jurisprudence and the Lanham Act afford a higher level of protection to non-commercial speech than to commercial speech, including, in the context of the Lanham Act, with respect to uses of third-party trademarks. Under the First Amendment, non-commercial speech may be subject to governmental regulation only if the regulation survives strict constitutional scrutiny.[2] Commercial speech also is entitled to First Amendment protection,[3] but the regulation of commercial speech is subject to a less rigorous level of judicial scrutiny.[4]

First Amendment protections and the favored treatment of non-commercial speech are reflected in the fact that under the Lanham Act and related case law, it is a defense to both trademark infringement and trademark dilution claims that the challenged use of another’s trademark is non-commercial. Specifically, with respect to trademark infringement claims, it is a defense that the use of another’s mark is not “on or in connection with a good or service.”[5] With respect to trademark dilution claims,[6] it is a defense that the use of another’s mark is “noncommercial.”[7]

Although there is little uniformity in judicial approaches to determining whether a use is non-commercial for purposes of infringement, dilution, and First Amendment defenses,[8] the following sections provide insight into how courts draw the boundary between commercial and non-commercial use in various contexts.

1. Advertising

The use of a mark “in connection with a good or service” does not require use of the mark in connection with offering a *specific* product or service: an advertisement’s general promotion of patronage or intent to enhance consumer goodwill is likely to be found to constitute commercial use, as explained by the Seventh Circuit in *Jordan v. Jewel Food Stores, Inc.* [9] Time, Inc., the publisher of *Sports Illustrated* magazine, published a commemorative issue of the magazine devoted exclusively to Michael Jordan in celebration of his induction into the NBA Hall of Fame. Jewel-Osco supermarket placed a full-page spread in the magazine congratulating Jordan on his induction (but not advertising any particular product or offer). Jordan sued Jewel-Osco alleging, *inter alia*, false endorsement under the Lanham Act.[10] The district court held that the ad was fully protected noncommercial speech, but the Seventh Circuit reversed, explaining that “[a]n advertisement is no less ‘commercial’ because it promotes brand awareness or loyalty rather than explicitly proposing a transaction in a specific product or service.”[11]

2. Gripe Sites

In *Bosley Medical Institute, Inc. v. Kremer*[12] the Ninth Circuit held that the defendant’s maintenance of a gripe site located at www.BosleyMedical.com (incorporating the plaintiff’s registered trademark), where the defendant “to put it mildly, was uncomplimentary of the Bosley Medical Institute”[13] and its hair restoration services, was not infringing because the defendant was not using the mark “in connection with the sale of goods or services” where the defendant’s website “contain[ed] no commercial links . . . offer for sale any product or service or contain paid advertisements from any other commercial entity.”[14] However, businesses considering using their competitors’ trademarks to critique the competitors’ products and services should note that the identity of the critic matters: the *Bosley* holding was based, in large part, on the fact that the defendant was not offering competing services to the public (such that the defendant’s use of the Bosley Medical mark could not have misled consumers into purchasing a competing product).[15]

Brooke Erdos Singer is a partner at Davis & Gilbert, LLP in New York, Secretary of the Section, and Chair of the Section’s Advertising Law Committee. **Maxine Sharavsky** is an associate at Davis & Gilbert.

3. Fan Sites

In *Taubman Co. v. Webfeats*,[16] the defendant, a web designer, operated a website using the name of the plaintiff's shopping mall as its domain name; the website included information about the mall and links to the websites of tenant stores. The defendant described the site as a "fan site" with no commercial purpose, but it contained links to the defendant's web design business and to his girlfriend's apparel business. The inclusion of these links led the Sixth Circuit to conclude that, "though minimal[ly]," the defendant was using the plaintiff's mark in a commercial manner.[17] The court was clear, however, that aside from the commercial links on the website, it found "no use 'in connection with the advertising' of goods and services" and that the Lanham Act therefore could not properly be invoked.[18] Case law regarding fan sites or other fan content is limited, likely because, as a practical matter, businesses stand to benefit from fan content and thus are more likely to tolerate or encourage it and/or to resolve conflicts with fan content creators without litigation.[19]

4. Social Media Platforms

Courts have not directly addressed the commerciality of content posted on social media and other user-generated content platforms, but generally speaking, such content, when published by or on behalf of a business, is treated in the same manner, for trademark purposes, as other commercial content promoting the business.[20] Insofar as businesses use their (and their sponsored influencers') social media pages to build support for their brands, products, and services in much the same manner as they use their websites and other online advertising, businesses should assume that their uses of third-party trademarks on social media platforms will be treated as commercial uses for Lanham Act purposes (although, depending on the context, such uses may be susceptible to descriptive or nominative fair use defenses, discussed further below, or may not give rise to a likelihood of consumer confusion).

That the use of a third party's mark is commercial in nature does not automatically make it impermissible; as discussed below, one of several other available defenses may apply.

B. Descriptive Fair Use

The classic or "descriptive" fair use defense to trademark infringement under the Lanham Act involves the use of another's mark not as a trademark (i.e., not to refer to the trademark owner or its goods or services), but solely as a descriptor of the advertiser's own goods.[21] For example, in *Sorensen v. WD-40 Co.*,[22] a chemical company's use of the word "inhibitor" to describe its corrosion inhibition product was found to be a descriptive fair use and not an infringement of the registered mark THE INHIBITOR owned by a company selling other corrosion inhibition products.[23] Courts also have extended descriptive fair use beyond purely literal identification of goods and services to permit the use of certain figurative expressions, such as the words "love potion" to advertising a perfume despite the ownershisp by a competing fragrance company of a trademark registration for LOVE POTION.[24] In *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*[25] the Supreme Court held that a party raising a descriptive fair use defense does not have the burden to negate a likelihood of consumer confusion,[26] although the ability of the party claiming infringement to prove a likelihood of consumer confusion is relevant to the fair use analysis.[27]

The availability of the descriptive fair use defense provides reasonable comfort to businesses that third parties' (including their competitors') trademark ownership of terms that are descriptive or suggestive of key goods or services in an industry will not prevent the use of the same terms to describe such goods or services in a non-trademark manner. However, businesses expecting to rely on a descriptive fair use defense must take care to use the terms "in good faith,"[28] meaning, according to at least some circuits, without intent "to trade on the good will of the trademark owner by creating confusion as to the source of the goods or services."[29] To avoid any inference of lack of good faith, businesses expecting to rely on a descriptive fair use defense should avoid using more of the third party's mark than is required. For instance, the use of a third party's particular stylization of a word, as opposed to just the word itself, would not be appropriate in the context of a descriptive fair use, as it would be inconsistent with the concept of describing the business's *own* goods (although, as described below, some uses of third parties' stylizations may constitute nominative fair use).

C. Nominative Fair Use

Nominative fair use as a defense to trademark infringement is a judicial creation: it was first developed by the Ninth Circuit in *New Kids on the Block v. News Am. Publ'g, Inc.*, where the court described it as the use of another's mark as "the only word reasonably available to describe a particular thing."[30] Although nominative fair use can take many forms, of particular interest from a commercial perspective is the nominative use by a business of competitors' trademarks for purposes of referring to the competitor or its goods or services in comparative advertising. Such uses generally are permissible so long as the comparison does not disparage the competitor, make claims that are inaccurate or untruthful or mislead consumers,[31] or cause consumers to be confused about the source of goods or services or the relationship between the businesses.[32] Nominative uses in comparative advertising can include consumer surveys, references to the brand in stating facts about products or services, and assurances as to the advertiser's product's compatibility with a competitor's product.

In *New Kids* the Ninth Circuit set forth a three-factor nominative fair use test, requiring that (i) the plaintiff's

Continued on page 23

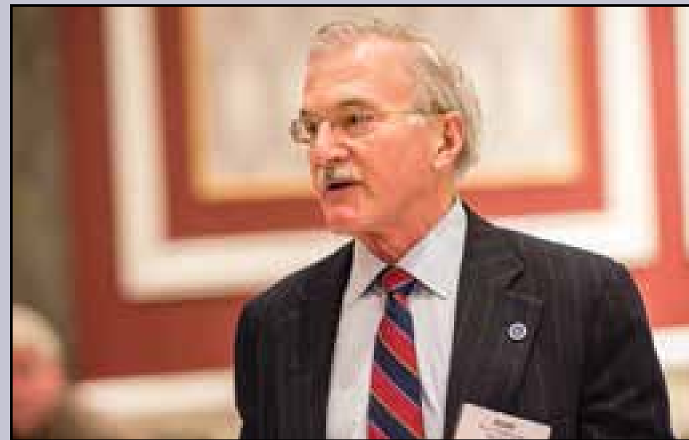
Ad or Fad?

NYSBA Annual Meeting
Intellectual Property Section Program
January 24, 2017
New York Hilton Midtown

Above left, panelists Adrienne Montes, Joseph Lewczak and Hal Hodes. Above right, panelist Phillips Nazro. Above and left, audience members listen to the discussion. Bottom left, panelists Hal Hodes, Phillips Nazro, Adrienne Montes, Joseph Lewczak and Section Chair Erica D. Klein. Below right, panelists Hal Hodes and Phillips Nazro.

Year in Review

NYSBA Annual Meeting
Intellectual Property Section Program
January 24, 2017
New York Hilton Midtown



Above left, Program Chair William R. Samuels, panelists David H. Faux, Charles L. Mauro and Barbara Kolsun. Above right, Rory Radding, former Section Chair. Below, Robert L. Raskopf.

Right, panelist Sapna Palla. Below left, panelists Professor David Hricik and Philip Furgang. Below right, panelist Magdalena Berger.

Above left, Program Chair William R. Samuels, Robert L. Raskopf, Jane Chuang, Sapna Palla, Magdelana Berger and Section Chair Erica D. Klein. Above right, Jane Chuang. Below left, Richard R. Ravin, former Section Chair. Below right, Gerald F. Fisher.

IPS 2017 Reception

Section Members enjoy the 2017 Intellectual Property Law Section's reception.

Data Privacy

NYSBA Annual Meeting
Intellectual Property Section Program
January 24, 2017
New York Hilton Midtown

Above left, panelist Daniel F. Forester. Above right, Max E. Iori, Duncan Campbell and Douglas B. Bloom. Above, Charlotte Roederer. Right, panelists Daniel F. Forester, Akiva Miller and Daniel Ilan. Below left, Daniel Ilan, Max E. Iori and Duncan Campbell. Below right, panelists Daniel F. Forester and Akiva Miller.

Using Third Parties' Trademarks: Unpacking Commerciality, Competition, and Confusion

CONTINUED FROM PAGE 18

product or service not readily be identified without the use of the trademark; (ii) the defendant has used only so much of the mark as is necessary to identify the product or service; and (iii) the defendant has not done anything that would suggest the plaintiff had sponsored or endorsed the defendant.[33] Businesses expecting to rely on the defense should be aware, however, that there is a lack of consistency among the circuits in the application of the nominative fair use defense (although the principles underlying the *New Kids* factors remain relevant across the circuits).

In particular, in 2016 the Second Circuit held in *International Information Systems Security Certification Consortium, Inc. v. Security University, LLC*[34] that a modified likelihood-of-confusion analysis, using the *Polaroid* factors[35] to the extent applicable,[36] still should apply in the nominative fair use context but with the addition of factors substantially similar to the *New Kids* factors.[37] This means that, in the Second Circuit, a use that complies with each of the nominative fair use factors still could be impermissible to the extent it is likely to result in consumer confusion when considered in light of the *Polaroid* factors. Conversely, a nominative use that would not pass muster under the Ninth Circuit's approach (for example, because it uses a third party's logo rather than just its name, which may be more of the mark than necessary to identify the relevant product or service) might nevertheless be permissible under the Second Circuit's approach if the *Polaroid* factors suggest that no confusion is likely.

In January 2017, the Supreme Court denied the petition for certiorari in *Security University*,[38] leaving businesses uncertain as to the appropriate nominative use analysis, particularly in national advertising campaigns or other multi-jurisdictional speech. A conservative approach, therefore, would include consideration of the traditional likelihood-of-confusion factors[39] as well as of the nominative fair use factors in determining appropriate comparative trademark uses and would not assume that because the use is nominative, there is no confusion.[40]

The Trademark Dilution Revision Act of 2006 codified the nominative fair use doctrine as a complete defense in trademark dilution suits,[41] although it remains solely a common-law defense in the context of infringement suits. The codification of fair use in the dilution context specifically references and permits use of famous marks in comparative advertising and in parodying, criticizing, or commenting on the owner of the famous mark or on the owner's goods or services.[42]

Given the lack of a uniform judicial approach to nominative fair use, and taking into account the principles that all of the circuits' approaches have in common, prudent nominative uses of third parties' marks, whether in comparative advertising or otherwise, will do the following:

1. Use the mark for the sole purpose of identifying the competitor or its goods or services, not as an indicator of the source of the speaker's goods or services or to suggest any association between the speaker and the mark owner.
2. Use only so much of the mark as is necessary to achieve the intended reference. The use of a word mark only is a more conservative approach where practicable.
3. Where third parties' logos or stylized word marks are used, particularly those of competitors, avoid altering the form in which the mark appears from the form traditionally used by the mark owner.[43]
4. Make sure there is adequate substantiation for any claims regarding the mark owner or its goods or services.
5. Where practicable, include disclosure as to the owner of the mark and a disclaimer as to any endorsement or sponsorship of the speaker by the mark owner.

D. News Reporting and Commentary

Separate from nominative use (but often overlapping with it) are news reporting and news commentary, which, under the Federal Trademark Dilution Act of 1995, are statutory defenses to trademark dilution claims.[44] Although there is very little case law on this defense, a Southern District of California court has extended it beyond traditional news media to a blogger who reported critically on a company that resells goods on eBay.[45] The court stated that the content, not the format, should be examined for purposes of determining whether material constitutes journalism and that the blogger's article was written "for the purpose of conveying information to the public."[46]

E. Parody

The Federal Trademark Dilution Act of 1995 and the Trademark Dilution Revision Act of 2006 also provide a statutory dilution defense for parody.[47] Although the statute does not expressly protect parody, courts typically recognize parody as fully protected speech.[48] In addition to the First Amendment interests at stake, courts have recognized that since parody "must convey two simultaneous and contradictory messages—that it is the original but also that it is *not* the original"[49]—likelihood of confusion is low where a parody is effective.[50]

F. Considerations Regarding Use of Third-Party Marks in Special Contexts

1. Keyword Advertising

Keyword advertising platforms such as Google AdWords allow an advertiser to "purchase" particular search terms for purposes of ensuring that links to websites controlled by the advertiser and featuring the advertiser's products or services are the top results for searches that include the purchased search terms. One technique some businesses have employed is to purchase their competitors' trademarks as search terms so that a search for the competitor's mark yields, as the top result, the "sponsoring" advertiser's website rather than that of the competitor/trademark owner.

Although courts have made clear that purchasing trademarks as keyword advertising search terms constitutes the use of a trademark in commerce (despite the keyword purchase not being consumer-facing),[51] such purchases are not necessarily infringing; rather, the appropriate inquiry is whether the purchase of a competitor's trademark for keyword advertising purposes gives rise to a likelihood of consumer confusion as to the source of the advertiser's paid search result.[52] Addressing that question requires fact-based analysis of the particular heading and content of the paid search result: if seeing the search result (or its heading, before clicking on the result) would lead a consumer to make incorrect inferences regarding the source of the result or the association between the trademark owner and the party controlling the search result, then the keyword, together with the search result to which it is linked, could constitute trademark infringement. Advertisers purchasing competitors' trademarks as advertising keywords should take care that the web results to which paid search terms are linked make the source of the web result clear by, for example, including the name of the party controlling the website in the page heading (and *not* including the competitor's name in the page heading).

2. Social Media and Vanity URLs

Many social media platforms allow users to select "vanity URLs," personalizing the URL that redirects to a particular social media account. For example, Jane Doe might choose, for her personal Facebook page, www.facebook.com/janedoe; an automotive repair shop called John Doe Auto Body Shop might choose, for its business Facebook page, www.facebook.com/johndoeauto).[53] Businesses would be well-advised to avoid claiming competitors' trademarks as vanity URLs. Although the use of competitor trademarks in post-domain paths is largely untested in court,[54] such uses are very likely to be considered commercial in nature and do not appear to be susceptible to available fair use defenses.[55] Further, there would seem to be a strong case for consumer confusion where consumers are accustomed to typing in the name of an individual or business as a post-domain path to reach the social media page controlled by that individual or business.[56] In addition to (or in lieu of) raising any Lanham Act claims that may be available, a trademark owner typically need look no further than the platform terms of use for a venue for reporting alleged trademark infringements. Facebook, for example, established a trademark dispute resolution process wherein trademark owners can use a form to report infringements.[57] Twitter has a similar form.[58]

3. User-Generated Content

User-generated content (UGC) is, broadly speaking, any form of content produced by consumers through the use of an online platform (social media or otherwise). Examples of UGC include social media posts, discussion forum posts, chats, tweets, blog content, digital images, audio files, and video files.[59] There is no explicit special legal treatment of the use of third-party trademarks in UGC; analysis of such uses should include consideration of commerciality, likelihood of confusion, and the defenses described herein. In many cases, by virtue of its creation by consumers, UGC is non-commercial and nominative in nature and therefore likely to constitute permissible use. Case law on use of trademarks in UGC is limited, but at least one court has, in dicta, acknowledged the importance of protecting consumers' rights to use UGC as a vehicle for discussing trademarked products.[60]

III. Hypotheticals

The following hypotheticals are intended to illuminate certain of the principles discussed above. Although some aspects of these examples are based on case law, the circumstances and parties are entirely fictional. Further, the discussion of these examples is for limited illustrative purposes only and therefore intentionally omits consideration of other factors and areas of law that would be relevant to a complete legal analysis. It is not intended to constitute legal advice applicable to any particular real-life situation.

> **Example A:** Company A, a manufacturer of energy drinks, is interested in producing a video, which it will post on its YouTube, Facebook, and other social media channels, in which real-life consumers (not paid actors) are approached in public and asked to compare Company A's product with a competing product sold by Company B and to discuss their reactions (in hopes of demonstrating that Company A's product is preferred). Company A approaches you for counsel prior to beginning production and asks for tips on limiting its risk of infringing the trademarks of Company B. What suggestions can you offer Company A?

Discussion: First, Company A must understand that posting the video in social media channels only (as opposed to, for example, posting it on Company A's primary website or running it as a network television ad) will not make the video a non-commercial use for purposes of trademark analysis. Company A should characterize its use as a nominative fair use in the context of comparative advertising and look to comply with the strictures necessary to qualify for such fair use protection.

Assuming the video will be accessible nationwide, it may not be clear to Company A which jurisdiction's law would apply if Company B brought a trademark infringement claim, so Company A should assume that both likelihood-of-confusion factors *and* the factors specific to nominative fair use will apply and should consider its use of Company B's marks from both a confusion perspective and a nominative use perspective. Since the circuits agree that advertisers using a third party's trademark in a nominative manner must not use more of the third party's mark than is necessary to identify the product or service, Company A should consider how it can limit its use of Company B's marks while still achieving its intended purpose. For example, it would be impossible to reliably illustrate for viewers a consumer drinking from a bottle of Company B's product without showing the bottle, including any word marks, logos, or trade dress embodied on or in it. (The bottle should be shown the way it ordinarily appears when distributed by Company B, not altered in any manner.) In contrast, it probably is *not* necessary for Company A to approach customers inside Company B's physical premises, thereby showing the trade dress used to outfit the Company B store.

To guard against confusion as to the ownership of Company B's trademarks, Company A may want to consider whether it is practicable to include a text disclaimer in the video making clear that the Company B name and any other Company B marks depicted in the video are the property of Company B.

Finally, but perhaps most importantly, Company A should be sure that it can substantiate the claims made or implied in the video. For example, if 80 percent of the individuals approached in production identify Company B's product as the favored product, Company A should consider refraining from posting the ad. Likewise, Company A should pay close attention to the nature of the statements individuals make about Company B's products and refrain from including any statements that are untrue or likely to mislead viewers of the video (e.g., a statement that Company B's product tastes more sugary than that of Company A, if Company A's product in fact contains a higher sugar concentration than that of Company B).

> **Example B:** Suzie Smith is a beauty blogger who reviews new products she finds while shopping. She selects all of the products to review without input from any brands and is not sponsored or provided with any free products or other benefits by any brands. The blog includes an "About Me" tab that identifies Suzie as a trained makeup artist available for hire by appointment. On the blog, in addition to sharing her views on various aspects of the product, including the pricing, branding, size, and product quality, she (i) identifies each of the brands she reviews by name, (ii) includes an image of the brand's primary logo, and (iii) shows a picture of herself holding the beauty item in its original packaging. Are her uses of the beauty brands' trademarks permissible, assuming the Ninth Circuit's *New Kids* factors apply to any nominative use analysis?

Discussion: Although Suzie is an individual presenting commentary and criticism, her blog is commercial in nature insofar as it promotes Suzie's services as a makeup artist. Therefore, Suzie is not subject to the heightened protection afforded to non-commercial speech, but she may be able to characterize her uses of the brands' marks as nominative fair use. As an initial matter, to avoid "do[ing] [any]thing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder,"[61] Suzie ought to include easily visible, clear disclaimers on the blog explaining that she is not endorsed by or provided with other benefits by any of the brands she reviews. Assuming no implication of sponsorship or endorsement, Suzie's use of the brands' *names* constitutes classic nominative use in that the name of the brand is, practically speaking, "the only word reasonably available to describe [the] particular thing."[62] Without using the brand name, readers will not be able to use Suzie's commentary because they will not be able to identify what she is reviewing. The use of the packaging image, although less clear-cut than the use of the name, is also arguably necessary to identify the product (thereby allowing readers to identify it by appearance while shopping). The appropriateness of Suzie's use of the logos is more questionable than her use of the brand names and packaging images, as the applicable product or service would still be "readily identifiable without use of the [logo],"[63] and, relatedly, Suzie has seemingly used more of the mark than necessary to identify the product or service.[64]

Given that in the Ninth Circuit the *New Kids* test "replaces the multi-factor test that the Ninth Circuit typically employs to determine consumer confusion,"[65] the application of the *New Kids* test in this case may result in a determination that there is a likelihood of confusion from a legal perspective where, from a practical perspective, there may have been none. The application of the Second Circuit's combined *Polaroid* and nominative use considerations, using the ordinarily applicable likelihood-of-confusion factors, might have resulted in a different and more permissive outcome regarding Suzie's use of the brand logos.

> **Example C:** In an attempt at search optimization, AB Gaming purchases a keyword for "XY Adventures," the name of a competing video game enterprise. As a consequence of AB's keyword purchase, the first result arising from a Google search for "XY Adventures" is a page entitled "What You Need to Know About

XY." Visitors who click on the search result are taken to a web page controlled by ABC that compares its games to those of XY, including discussing (accurately) some defects that have been found in XY's product software. The page is located at the URL www.abgames.com/why-we-win/, has the AB logo at the top, and appears in the color scheme typical of AB product branding. The XY name is used on the website solely to reference XY in comparing and critiquing its product offerings. No XY logos or other XY marks are used on the website in any manner. Is AB's keyword advertising use of XY Adventures' trademark permissible?

Discussion: AB Games is using the XY Adventures trademark in two ways: (i) as a purchased advertising keyword and (ii) on the AB website for purposes of comparing AB to XY. That the nominative use of the XY mark on the AB website itself presents accurate critique and is fairly limited in degree and unlikely to result in consumer confusion as to the source of the website is irrelevant to the analysis of whether the use of the mark in keyword advertising presents a likelihood of confusion as to the source of the website to which the purchased keyword is linked. In *Rescuecom*, the Second Circuit stated that "[i]f the searcher sees a different brand name as the top entry in response to the search for 'Rescuecom,' the searcher is likely to believe mistakenly that the different name which appears is affiliated with the brand name sought in the search and will not suspect, because the fact is not adequately signaled by [the] presentation [of the entry], that this is not the most relevant response to the search."[66]

That concern may be all the more salient if the title of the search result bears, in fact, the *same* name the searcher was looking for: a result titled "What You Need to Know About XY" is unclear as to its source and in no way indicates that the source could be AB. Some consumers may assume that clicking on the result will lead them to a website controlled by (and offering firsthand information about) XY. That the consumer would promptly discover her error once she reached the website does not resolve the issue; she has already, by the time of her discovery, experienced initial interest confusion.[67] AB Games should revise the title of its search result page such that there is complete clarity as to the source of the page (e.g., "Welcome to AB Games" or "AB Games: How We Win").

IV. Conclusion

Use of a third party's trademark can be a powerful tool to allow or enhance a critique of a business or its products or services, whether from the perspective of a disgruntled consumer, a public informer, or a savvy competitor. In particular, businesses should take some comfort in the knowledge that commercial speech, notwithstanding its subsidiary position relative to non-commercial speech, is entitled to a significant degree—and many types—of protection from a trademark perspective; businesses need not assume that they have no right to criticize third-party products and services due solely to the commercial nature of their critiques. However, given the inconsistent law across jurisdictions as to when speech is commercial and as to trademark defenses such as nominative fair use, a customized consideration of facts and a detailed search for supporting cases involving comparable facts is in order each time the use of a third party's trademarks is contemplated.

Endnotes

1. This article focuses on use of third parties' trademarks from a U.S. law perspective. The analysis may differ for trademark uses outside the United States, including for advertisers undertaking global campaigns or those targeted at non-U.S. jurisdictions.
2. The government must demonstrate a compelling state interest in regulating non-commercial speech, and the regulation must be narrowly tailored to achieve that interest. *See, e.g.*, *Citizens United v. FEC*, 558 U.S. 310, 340 (2010); *FEC v. Wis. Right to Life, Inc.*, 551 U.S. 449, 464 (2007); *Austin v. Michigan State Chamber of Commerce*, 494 U.S. 652, 655 (1990); *Boos v. Barry*, 485 U.S. 312, 334 (1988) (plurality); *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 786 (1978); *Buckley v. Valeo*, 424 U.S. 1, 44-45 (1976).
3. *See Bigelow v. Virginia*, 421 U.S. 809, 818-26 (1975); *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 758-70 (1976); *see also Edenfield v. Fane*, 507 U.S. 761, 767 (1993) ("The commercial marketplace, like other spheres of our social and cultural life, provides a forum where ideas and information flourish. Some of the ideas and information are vital, some of slight worth. But the general rule is that the speaker and the audience, not the government, assess the value of the information presented. Thus, even a communication that does no more than propose a commercial transaction is entitled to the coverage of the First Amendment.").
4. The test, as articulated in *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 566 (1980), requires, with respect to speech that is lawful and not misleading (a prerequisite to First Amendment protection), that (i) the asserted governmental interest is substantial; (ii) the regulation directly advances such interest; and (iii) the regulation is not extensive than necessary to serve such interest.
5. 15 U.S.C. § 1125(a)(1) (defining trademark infringement as the use of another's mark "on or in connection with any goods or services" in a confusing or misrepresentative manner).
6. The Lanham Act defines dilution as a claim available to the owners of a famous mark against uses of a similar mark that, irrespective of any likelihood of confusion, is likely to impair the distinctiveness of the famous mark ("dilution by blurring") or harm the reputation of the famous mark ("dilution by tarnishment"). 15 U.S.C. § 1125(c)(1)-(2).
7. 15 U.S.C. § 1125(c)(3)(C).
8. Further complicating the commerciality analysis is that the term "commercial" is used to represent multiple concepts in overlapping bodies of law, including First Amendment case law, trademark non-infringement case law, trademark dilution case law, and case law regarding the meaning of "use in commerce" for purpose of determining the limits of Congressional regulation. For a detailed discussion of the multiple and conflicting ways the concept of commerciality is defined and used, *see* Jennifer E. Rothman, *Commercial Speech, Commercial Use, and the Intellectual Property Quagmire*, 101 Va. L. Rev. 1929 (2015).
9. *Jordan v. Jewel Food Stores, Inc.*, 743 F.3d 509 (7th Cir. 2014).
10. *Id*. at 511.

11. *Id*. at 518.

12. *Bosley Med. Inst., Inc. v. Kremer*, 403 F.3d 672 (9th Cir. 2005).

13. *Id*. at 674.

14. *Id*. at 678. *See also Lamparello v. Falwell*, 420 F.3d 309 (4th Cir. 2005) (rejecting a claim that the defendant's use of the domain name "fallwell.com" to operate a gripe site criticizing Reverend Jerry Falwell constituted trademark infringement). Although such holding was ultimately based on an absence of likelihood of confusion rather than a determination that the use was not commercial, the discussion of confusion cited the fact that the site was being used solely to criticize the markholder, not to capture the markholder's customers and profits. *Id*. at 317-18.

15. *Bosley*, 403 F.3d at 679-80. Consumers also may be able to avail themselves of non-trademark protections in connection with their public posting of (non-libelous, non-defamatory, non-slanderous) gripe content. Consider, for instance, the Consumer Review Fairness Act of 2016 (15 U.S.C. § 45b), enacted in 2016 to protect consumers' ability to "share their honest opinions about a business's products, services, or conduct, in any forum, including social media." Federal Trade Commission, *Consumer Review Fairness Act: What Businesses Need to Know* (Feb. 2017), https://www.ftc.gov/tips-advice/business-center/guidance/consumer-review-fairness-act-what-businesses-need-know. Certain states had similar bills prior to the enactment of the CRFA. *See, e.g.*, Cal. Civ. Code § 1670.8.

16. *Taubman Co. v. Webfeats*, 319 F.3d 770 (6th Cir. 2003).

17. *Id*. at 775.

18. *Id*.

19. Some businesses have established written policies specifically applicable to the development and distribution of fan content. That approach is particularly popular in the gaming industry. *See, e.g.*, Epic Games' policy (https://www.epicgames.com/about/fan-art-policy/); Dungeons & Dragons policy (http://dnd.wizards.com/articles/features/fan-site-kit); Habbo policy (https://help.habbo.com/hc/en-us/articles/221643408-Habbo-Fansite-Policy).

20. For example, the FTC treats social media content as commercial content in the context of endorsements and social influencer speech, where a lack of transparency can result in consumer confusion as to the independence of the speaker on a particular product or service. *See, e.g., In the Matter of Lord & Taylor, LLC* (FTC 2016) (treating content posted by Lord & Taylor-sponsored influencers on, *inter alia*, Instagram as commercial content subject to regulation); *In the Matter of Warner Bros. Home Entertainment, Inc.* (FTC 2016) (treating influencer postings on YouTube as commercial content subject to regulation).

21. 15 U.S.C. § 1115(b)(4).

22. *Sorensen v. WD-40 Co.*, Case No. 14-3067 (7th Cir. June 11, 2015).

23. *Id.*

24. *Dessert Beauty, Inc. v. Fox*, 568 F. Supp. 2d 416 (S.D.N.Y. 2008) (stating that the defendant "did not use 'love potion' as a trademark because the source of its fragrance products was not identified by that term" (*id.* at 424) and that the words were instead used "to describe the effects that the products may have [when] worn by the wearer" (*id.* at 425).

25. *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*, 543 U.S. 111 (2004).

26. *Id*. at 114.

27. The Supreme Court remanded the case for further proceedings on the issue of confusion, specifically, whether a cosmetics seller's use of the term "microcolor" was likely to result in consumer confusion with a competitor's incontestable trademark registration for MICRO COLORS). *Id.* at 124.

28. 15 U.S.C. § 1115(b)(4).

29. *Int'l Stamp Art, Inc. v. United States Postal Serv.*, 456 F.3d 1270, 1274 (11th Cir. 2006); *see also Kelly-Brown v. Winfrey,* 717 F.3d 295, 312 (2d Cir. 2013).

30. *New Kids on the Block v. News Am. Publ'g, Inc.*, 971 F.2d 302, 308 (9th Cir. 1992).

31. Claim substantiation, while important in all advertising, is especially critical in the comparative advertising context, where the advertising is likely to draw the competitor's attention. In addition to the spectre of private claims under the Lanham Act and/or its counterparts at the state level, competitors also could raise claims with the National Advertising Division of the Council of Better Business Bureaus, and false advertising may be subject to regulatory discipline by the Federal Trade Commission.

32. *New Kids*, 971 F.2d at 308.

33. *Id*.

34. *Int'l Info. Sys. Sec. Certification Consortium, Inc. v. Sec. Univ., LLC*, 823 F.3d 153 (2d Cir. 2016).

35. The Second Circuit's *Polaroid* factors are (1) strength of the senior user's trademark; (2) similarity of the marks; (3) proximity of the products and their competitiveness with one another; (4) evidence that the senior user may "bridge the gap" by developing a product in market of the alleged infringer's product; (5) evidence of actual confusion; (6) evidence that the imitative mark was adopted in bad faith; (7) quality of the defendant's product; and (8) sophistication of buyers in the relevant market. *Polaroid Corp. v. Polarad Elecs. Corp*., 287 F.2d 492, 495 (2d Cir. 1961).

36. The Second Circuit acknowledged that certain of the *Polaroid* factors are "a bad fit" in the nominative use context. *Int'l Info. Sys.*, 823 F.3d at 168.

37. *See also Century 21 Real Estate Corp. v. Lendingtree, Inc.*, 425 F.3d 211 (3d Cir. 2005), in which the Third Circuit treated nominative fair use as an affirmative defense, applicable only after a plaintiff proves a likelihood of confusion, and articulated its own test with factors derived from the *New Kids* test. *Id.* at 222. For a more in-depth discussion of the Second Circuit's analysis of nominative fair use, *see* Jonathan Bloom and Jessica Falk, *Second Circuit Weighs in on Nominative Fair Use, Certification Marks*, Bright Ideas, Fall 2016, Vol. 25, No. 2, at 30-33.

38. *Int'l Info. Sys.*, 823 F.3d 153, *cert. denied*, 2017 U.S. LEXIS 521 (U.S. Jan 9, 2017).

39. Most jurisdictions have established likelihood-of-confusion factors analogous to the Second Circuit's *Polaroid* factors. *See, e.g.*, *Interpace Corp. v. Lapp, Inc.*, 721 F.2d 460, 463 (3d Cir. 1983); *AMF, Inc. v. Sleekcraft Boats*, 599 F.2d 341, 348-49 (9th Cir. 1979); *Helene Curtis Indus. v. Church & Dwight Co.*, 560 F.2d 1325, 1330 (7th Cir. 1977).

40. Note also that the Second Circuit made clear that "confusion" analysis applies not only with respect to the source of goods, but also with respect to sponsorship, affiliation or connection between the parties. *Int'l Info. Sys.*, 823 F.3d at 161.

41. 15 U.S.C. § 1125(c)(3)(A).

42. 15 U.S.C. § 1125(c)(3)(A)(i)-(ii).

43. *See, e.g.*, *Deere & Co. v. MTD Products, Inc.*, 41 F.3d 39 (2d Cir. 1994) (defendant's use of a modified form of the famous "leaping deer" trademark of Deere and Company constituted dilution of a famous mark).

44. 15 U.S.C. § 1125(c)(3)(B). There is no explicit statutory news reporting defense to trademark infringement claims, but most news reporting and commentary is, by its nature, likely to be subject to a nominative use defense.

45. *See BidZirk, LLC v. Smith*, No. 6:06 709-HMH, 2007 U.S. Dist. LEXIS 78481 (D.S.C. Oct. 22, 2007) (holding that an article titled "Special Report: You Gotta Be Berserk to Use an eBay Listing Company! The Whole Story," depicting BidZirk's trademark and relating the author's experience utilizing an eBay listing company

such as BidZirk, qualified for a news reporting defense under 15 U.S.C. § 1125(c)(3)(B)).

46. *Id.* at *17-18.

47. 15 U.S.C. § 1125(c)(3)(A)(ii).

48. *See, e.g.*, *Mattel, Inc. v. MCA Records*, 296 F.3d 894 (9th Cir. 2002); *Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC*, 507 F.3d 252, 260 (4th Cir. 2007); *People for the Ethical Treatment of Animals v. Doughney*, 263 F.3d 359 (4th Cir. 2001); *Jordache Enters. v. Hogg Wyld, Ltd.*, 828 F.2d 1482 (10th Cir. 1987).

49. *People for the Ethical Treatment of Animals*, 263 F.3d at 366 (internal quotations and citation omitted).

50. *Louis Vuitton*, 507 F.3d at 261.

51. *See Rescuecom Corp. v. Google, Inc.*, 562 F.3d 123, 127 (2d Cir. 2009); *Network Automation, Inc. v. Advanced Sys. Concepts, Inc.*, 638 F.3d 1137, 1145 (9th Cir. 2011).

52. *See Rescuecom*, 562 F.3d at 130 ("[A] defendant must do more than use another's mark in commerce to violate the Lanham Act. The gist of a Lanham Act violation is an unauthorized use, which 'is likely to cause confusion…as to the origin, sponsorship, or approval of . . . goods [or] services.'").

53. Google+, LinkedIn, Twitter, Pinterest, and Instagram also provide for the selection of personalized URLs. *See, e.g.*, Ericka Lewis, *How to Claim Vanity URLs for Your Social Media Accounts*, Adhere Creative (Sept. 15, 2015), https://www.adherecreative.com/blog/bid/187942/How-To-Claim-Vanity-URLs-For-Your-Social-Media-Accounts.

54. In 2009, Major League Baseball manager Tony La Russa sued Twitter and the holder of an account that used La Russa's name in its post-domain path, i.e., twitter.com/TonyLaRussa). *La Russa v. Twitter, Inc. and Does 1-25*, Case No. CGC-09.488101 (Cal. Super. Ct. filed May 6, 2009). The case ultimately settled, however, without a ruiling on the merits. http://www.dmlp.org/sites/citmedialaw.org/files/2009-06-26-La%20Russa%20Notice%20of%20Voluntary%20Dismissal.pdf.

55. *Contrast Bosley*, 403 F.3d at 679, where the holding was based on the non-commercial nature of the use and that the defendant was not offering competing services to the public.

56. *See Brookfield Commc'ns, Inc. v. West Coast Entm't Corp.*, 174 F.3d 1036, 1062 (9th Cir. 1999) (explaining that initial interest confusion online, even if later corrected, can damage a plaintiff trademark owner because web surfers who navigate to the defendant's site by mistake may not bother to course-correct).

57. *See* Facebook's trademark report form at https://www.facebook.com/help/contact/284186058405647.

58. *See* Twitter's trademark report form at https://support.twitter.com/forms/trademark.

59. Kyle S. Richardson, *The Content Corner: How to Leverage User-Generated Content to Resonate With Your Audience*, U.S. Technology Transformation Service—DigitalGov (July 11, 2016), https://www.digitalgov.gov/2016/07/11/how-to-leverage-user-generated-content-to-resonate-with-your-audience/.

60. *See Stevo Design, Inc. v. SBR Mktg.*, 968 F. Supp. 2d 1082 (D. Nev. 2013).

61. *New Kids*, 971 F.2d at 308.

62. *Id*.

63. *Id*.

64. *Id*.

65. *Int'l Info. Sys.*, 823 F.3d at 166.

66. *Rescuecom*, 562 F.3d at 131.

67. *See Brookfield Commc'ns*, 174 F.3d at 1062 (explaining that web surfers who navigate to the defendant's site by mistake will find a product offering similar enough to plaintiff's "such that a sizeable number of consumers who were originally looking for [plaintiff]'s product will simply decide to utilize [defendant's] offerings instead.").

The Designer Formerly Known as…Intellectual Property Issues Arising from Personal Names as Fashion Brands

By George C. Sciarrino and Matthew D. Asbell

I. Introduction

Kate Spade, Paul Frank, Joseph Abboud, Catherine Malandrino, and Karen Millen—aside from being well-known designers, all have something else in common: they no longer own the right to use their personal names as their brands. In the fashion industry, it is common for designers to use their personal names to refer to their clothing designs and related products. However, this practice raises concerns that designers, as well as companies purchasing the brands of those designers, should consider when starting or acquiring an eponymous brand.[1]

While developing their personal names as fashion brands, designers should be aware that there are a number of risks that they could encounter at the outset. Initially, they may encounter hurdles when clearing and attempting to register their personal names as trademarks in the United States and worldwide, and if they eventually decide to sell their companies, they could lose the right to use their personal names in future fashion ventures or as a trademark for similar products.[2] Often this predicament is discovered after a purchase agreement has been made, and it can result in onerous and expensive disputes that do not benefit either party. In dealing with an international fashion brand, such disputes can arise on multiple fronts around the world.

With this in mind, designers still may prefer to use their personal names as their brands. Ultimately, for an emerging designer, achieving fame and widespread name recognition may outweigh any potential risks, and the sale of their companies often comes with a large price-tag, as acquiring entities are willing to pay sizable sums for successful fashion brands. In any event, both the designer and the purchasing company should perform due diligence when developing or contracting for the sale of an eponymous brand. It is imperative for both parties to consider the various ways designers may use or be required to use their names in connection with future ventures, such as in press releases, third-party websites, keyword advertising, social media posts, domain names, and other related intellectual property documents, including, for example, design patent applications. Designers also should strategically manage their intellectual property portfolios in the event they ultimately sell their assets. After selling their brands, designers may need to rebrand themselves by taking on a new name and becoming "the designer formerly known as . . . ."

George C. Sciarrino is an associate and **Matthew D. Asbell** is a partner in the New York office of Ladas & Parry.

II. Clearing and Registering Personal Names as Trademarks

For designers, it may be difficult to clear and register a personal name as a trademark. First, the marketplace and applicable trademark register may be crowded with marks that include the designer's given name. Such marks may pose obstacles to registration and use even though the designer may plan to use his or her given name only in combination with other elements such as his or her surname. In the United States, a mark can be refused registration for its surname significance; under the Lanham Act, a mark that is "primarily merely a surname" is not federally registrable on the Principal Register without proof of secondary meaning, which requires a showing that in the minds of relevant consumers, the surname indicates the source of the goods or services.[3] In addition, depending on the markets in which they do or plan to sell their products, designers must consider early on whether to clear and register versions of their names in non-Latin characters in certain jurisdictions.

Whether a trademark is "primarily merely a surname" depends on a number of factors, including (1) whether the term is a rare surname; (2) whether the term is the surname of anyone connected with the applicant; (3) whether the term has any recognized meaning apart from being a surname; (4) whether the term has the "look and feel" of a surname; and (5) whether the mark has a unique text stylization that creates a distinct commercial impression.[4] This is a highly subjective test that looks at the probable reaction of consumers in the marketplace. Before preparing an application for a surname by itself or even in combination with additional elements such as a first initial, it is important to formulate ways to build and demonstrate secondary meaning to increase the likelihood of the mark being registered. Fortunately, designers who adopt the combination of their given name and their surname are unlikely to face such a refusal, which occurs only when the mark consists of little more than a surname.

If the designer's surname is already well-known, and substantial resources have been allocated to promoting the mark, the designer may consider making a claim of acquired distinctiveness to show that the mark has established a secondary meaning.[5] Otherwise, the designer may register the surname mark on the Supplemental Register and use it in commerce for at least five continuous years in order to eventually acquire distinctiveness.[6] In other countries, there may be similar rules with regard to the distinctiveness of personal names as trademarks.

When considering possible rights outside the United States, designers who wish to own and use their names as trademarks also should contemplate whether they will use or need to prevent others from using a phonetically equivalent version of their name in the local language. Former basketball star Michael Jordan learned this the hard way when he spent nearly five years fighting in the Chinese courts to finally get the rights to a Chinese character version of his surname, 乔丹, from Qiaodan Sports Co., Ltd., which registered the mark and operated nearly 3,000 retail locations in China under it.[7] As Jordan's success in court was largely a result of his fame, designers who are less well-known are wise to consider applying to register their names in non-Latin characters in relevant jurisdictions as early as possible rather than discover later that another party has adopted and registered the name before them.[8]

III. Global Disputes over Personal Names

When managing a global brand, disputes may arise contemporaneously in different locations around the world. This is happening in a legal battle involving London-based international fashion brand Karen Millen Fashions Limited (KML) and designer Karen Millen over the right to use her name.[9]

By way of background, Karen Millen sold her company in 2004 to KML's predecessor-in-interest, the Icelandic group Baugur, along with the rights to use her name on future competing ventures, by way of a purchase agreement. Years later, Millen proceeded to challenge the agreement and attempted to register a number of trademarks in the United States that included her name.[10] The conflict escalated, and Millen filed cancellation actions in the United States against several KML marks that included her name. KML initiated litigation in the Eastern District of Virginia, claiming, *inter alia*, breach of contract. After the district court dismissed the case, KML appealed but then voluntarily dismissed the appeal on October 11, 2016.[11] Relying on a forum selection clause in the purchase agreement that allegedly required contractual disputes be litigated in the United Kingdom, Millen brought an action in the High Court of England and Wales that included a claim for declaration that she could use the marks KAREN and KAREN MILLEN in the United States.[12] Previously, in 2015, Millen had reached a settlement with regard to use of her name in the United Kingdom and European Union, which generally prevented her from using her name on products in these jurisdictions.[13]

In the High Court decision in England and Wales, *Millen v Karen Millen Fashions Ltd. & Anor,* Judge Meade ruled that the designer Karen Millen no longer had the right in the United States to use her name KAREN MILLEN as a trademark for homewares and lifestyle ventures or KAREN for any goods and services.[14] The court noted that it would have been inclined to allow the mark KAREN to be used had the designer claimed limited rights with respect to the geographic scope and description of goods and services that did not conflict with KML's rights. Millen was further ordered to consent to additional registrations by KML that include her name.[15]

Since the High Court decision, Millen has abandoned most of the U.S. trademark applications and registrations for marks that include her full name.[16] At the same time, a pending application filed by Millen for HOME BY KAREN has proceeded to publication and been opposed by KML.[17] Without successfully appealing the High Court's decision, Millen will most likely need to redevelop her new brand under a different name.

IV. Possible Ways Around Losing One's Own Name and Likeness

After selling their brands, designers may not realize that they can no longer use their names in connection with their new fashion ventures. In many cases, they still can identify themselves as the designer of the new brand without using their name to identify the brand itself. The distinction often made in these scenarios is between the trademark, which identifies the source of goods or services, and the designer's right of publicity in his or her name and likeness independent of the products he or she designs.

In most U.S. states, a person's right to use his or her name and likeness commercially falls under the category of the right of publicity, which has been derived from the right of privacy. The nature of the right, as well as the term used to describe it, and the assignability of the right may be different from one state or country to the next. In some jurisdictions, like France and other European countries, copyright law may recognize a fashion designer's moral rights over his or her design at the moment the original work is created. Moral rights normally include the right of attribution (the right to be identified as the author); the right of integrity (the right to prohibit modification or destruction of the work); the right of disclosure (the right of control over publicizing of the work); and the right of withdrawal (the right to take back the work from the public after it has been released).[18] In jurisdictions that recognize moral rights, the law typically does not allow assignment of the right of attribution. Therefore, after selling their eponymous brands, designers may retain the moral right to identify themselves as the creator of their past and future designs.

As menswear designer Joseph Abboud stated, "The consumer has a right to know the creator of a work."[19] After selling his trademarks to JA Apparel Corp. for $65.5 million in 2000, Abboud sought to create a new line called "Jaz" and to use the tagline "a new composition by designer Joseph Abboud." JA Apparel sued in the Southern District of New York for breach of contract.[20] The court held that "Abboud did not sell, and JA Apparel did not purchase, the exclusive right to use the 'Joseph Abboud' name commercially. Rather, Abboud sold, and JA Apparel purchased, the 'Joseph Abboud' name as a trademark."[21] The court went on to grant Abboud certain qualified rights, like the ability to use his name "in the context of a complete sentence or descriptive phrase," as long as it be "no larger or more distinct than the surrounding words in that sentence or phrase." [22] However, he would have to display the term "Jaz" prominently in advertisements to make the source clear and include a disclaimer of any affiliation with JA Apparel and its related products. Thus, Abboud effectively could no longer use his name in any manner on any "Jaz" labels, packaging, or hang-tags.[23]

In a similar case, also in the Southern District of New York, the court ruled that Paulo Gucci, former chief designer of Gucci, could not use the name "Gucci" as a trademark.[24] However, he could continue to use his personal name to identify himself as the designer of products sold under a different brand name, as long as his name "always appear[ed] after the trademark in advertisements and on labels" and was less prominent than the trademark. He was also required to disclaim any affiliation with the Gucci entities in connection with the use of his name on his designs.[25]

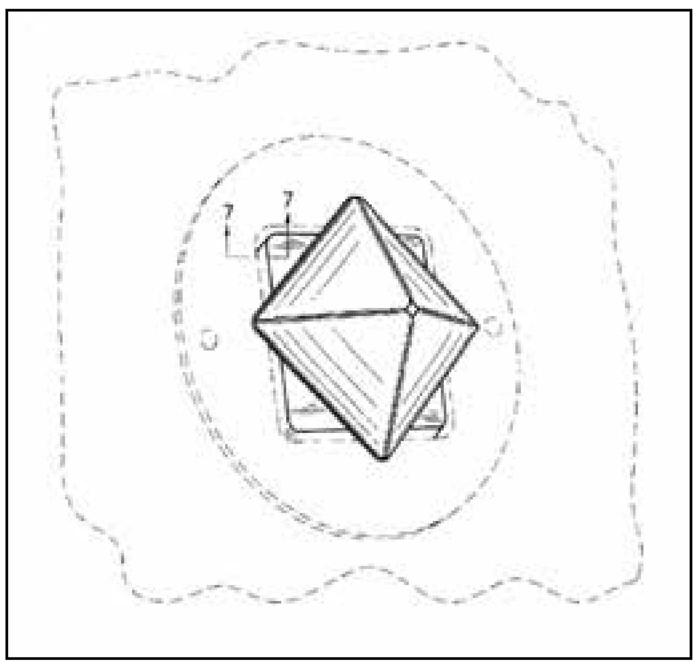
The designer Paul Frank Sunich also found himself in a legal battle with the owners of his former company Paul Frank Industries, Inc. over his use of his full name on T-shirts.[26] A court in the Central District of California ruled that Sunich could not use his name on T-shirts, which the public had come to associate with his former company, but that he could identify himself as designer of his newly developed products (e.g., on business cards or on his website) so long as in doing so he disclaimed affiliation with his former company.[27]

While these designers were able to use their own names in some way in connection with their new brands, some designers find themselves not as free to do so. For instance, after a legal battle with and separation from her business partners, Catherine Malandrino lost the ability to use her name as her brand to CM Brand Holdings LLC.[28] The owners of Malandrino's trademarks apparently claimed the right to control Malandrino's "likeness, being and persona." Malandrino's attorney was quoted as saying that would "make her an indentured servant."[29]

When Malandrino launched her new collection for the Home Shopping Network (HSN) at a much lower price point, HSN sent out promotional emails labeling the brand as French Rendez Vous by Catherine Malandrino. HSN later reportedly stopped using Malandrino's name in connection with the line, possibly in response to a demand letter, and there is now no use of Malandrino's name on the HSN webpage for that product line.[30]

Whether knowingly or not, HSN is able to draw the connection between the new brand and the designer without directly using her name. A number of articles in major fashion publications, including Vogue,[31] InStyle,[32] and WWD,[33] have connected Malandrino with the new HSN fashion line. While Malandrino may have lost the ability to use her name and likeness in connection with new ventures, she appears to still be able to influence the media to use her name and draw the connection for her. In addition, search engine queries for Malandrino's name also include references to her new collection on the HSN website (even though the website itself does not use her name). In fact, there are a variety of Search Engine Optimization strategies that designers may use to disseminate the news and draw the link between their new brands and their personal names. For example, when a designer purchases keywords from a search engine operator that include his or her name, the triggered ads can make a connection without necessarily causing consumer confusion.[34]

Designers also must use their personal names in connection with certain legal documents, including, for example, any design patents they pursue for their new companies. When filing a design patent in the United States, applicants must designate the legal name of the actual inventor(s), which often will be the individual designer(s) and cannot be a juristic entity, although the patent may be assigned to one. For example, the "individual" designer Kate Spade signed a U.S. design patent application for an ornamental design of a bag clasp, depicted below, listing herself as the inventor and the company Kate Spade LLC as the assignee.[35] After selling the right to use his or her name, a designer may not be precluded from listing his or her name as the inventor in a design patent application or in other documents requiring his or her legal name. As designers seek to redefine themselves and their work, this practice may provide a nexus between the designers' new brands and their personal names, even where designers are otherwise precluded from using their names.



Other often overlooked assets associated with intellectual property rights that must be considered in relation to the sale of an eponymous brand are domain names and social media accounts that incorporate the designer's name. Upon the sale of their rights, designers may need to transfer domains comprising their names. A subsequent effort by the designer to register and use a version of her name that she has clearly sold may be considered "bad faith" that would support the assignee's Uniform Domain Name Dispute Resolution Proceeding or Uniform Rapid Suspension proceedings to transfer, suspend, or cancel the domain. With regard to the designer's social media accounts, the purchasing company should contemplate acquiring any login information or administrative privileges at the time of closing, as it could later be in violation of a social media website's privacy policy for the website to release such information or facilitate a transfer of ownership. Before reaching an agreement, the designer and purchasing company should come to a mutual understanding as to which, if any, domain names and social media accounts will be transferred and which may be retained and used, and as to whether the designer will be able to include his or her name in future domain names and social media accounts. It may be advisable for the designer to immediately reserve a mutually acceptable domain name and/or social media account before closing a deal.

When a designer can no longer use his or her name or likeness, he or she may consider alternative ways of identifying themselves as designers of their new brands that comply with the terms of their purchase agreements, such as press releases, third-party websites, keyword advertising, social media posts, domain names, and even design or utility patents.

V. Name Changers Can Be Game Changers for Designers

The designer formally known as Kate Spade was actually first named Katherine Noel Brosnahan.[36] When she married her business partner Andy Spade, she adopted the name Kate Spade, allegedly without ever legally changing her name. Since then, the name Kate Spade has not only become synonymous with high-end handbags and shoes, it also has become the well-known identifier of the designer herself.[37]

In 2006, Brosnahan sold her company to Liz Claiborne Inc., which rebranded it as Kate Spade & Co., along with the right to use the name as her brand. She then took on the name Katherine Noel Frances Valentine Brosnahan and now designs under the label Frances Valentine.[38]

There are several U.S. federal registrations and pending applications for the mark FRANCES VALENTINE in the name of Quince New York Shoes, LLC, covering, *inter alia*, sunglasses, handbags, clothing, and shoes. Before one of the registrations issued, Reg. No. 4965459, the Examining Attorney inquired whether the mark identifies a living person.[39] Under the Lanham Act, if the mark identifies a living person, the Applicant is required to provide a written consent.[40] Interestingly, the Applicant for the mark FRANCES VALENTINE responded that the name portrayed in the mark "does not identify a particular living individual." This appears to be contrary to media reports that the mark is connected with the designer's new personal name. As a result of this statement, Brosnahan was not required to provide her written consent, and the mark proceeded to registration.

While a personal connection was not made in the U.S. trademark prosecution history for the new brand, retail partners of Frances Valentine were able to connect the brand with the designer by using clever language in promotional materials. In April 2016, Nordstrom Inc. hosted a reception for the designer in Boca Raton, Florida, and the invitations reportedly described her as the "former designer and founder of [the] Kate Spade brand."[41] Carefully drafted language like this was likely vetted by an attorney in order to introduce Brosnahan's new brand in connection with her former brand without infringing the trademark rights of Kate Spade & Co.

According to the Wall Street Journal, the CEO of Kate Spade & Co., Craig Leavitt, stated that his only concern is that the brand not be "confusing to our customers or infringing on our trademarks."[42] Brosnahan's name change is somewhat of a game changer for designers who have sold their eponymous brands, as it shows how designers can start new ventures under different personal names while apprising consumers of a connection between the designer's former and new name.

VI. A Final Consideration When Using or Acquiring a Personal Name as a Brand

Before designers use their personal names as their brands, they should consider whether they can accept the possibility of eventually having to forfeit the right to use their names on future ventures in exchange for reputational and financial gains that may be achieved if they decide to sell the company and rights to the company's trademarks and related rights. If this happens, it is important to have a carefully drafted purchasing agreement, preferably with exhaustive consideration of the various types of name uses. When designers sell the rights to their personal names, they may consider alternative ways to connect themselves with their new brands, including whether to take on a different name, e.g., "the designer formerly known as…."

Endnotes

1. *See* Marc Misthal, *Trademarks and Trade Dress*, in Fashion Law: A Guide for Designers, Fashion Executives, and Attorneys 28 (Guillermo C. Jimenez & Barbara Kolsun eds., 2014).
2. *Id.*

3. *See* 15 U.S.C. § 1052(e).

4. *See TMEP* § 1211.01.

5. *See TMEP* § 1211.

6. *See Inherent and Acquired Distinctiveness and the Principal and Supplemental Registers for U.S. Trademarks*, L&P Education Center (Mar. 22, 2017), http://ladas.com/education-center/inherent-acquired-distinctiveness-principal-supplemental-registers-u-s-trademarks/.

7. *See* Yixian Chen, *CHINA: SPC Rules on Michael Jordan's Chinese Name Rights: Decision and Applications*, INTA Bulletin (Mar. 15, 2017), http://www.inta.org/INTABulletin/Pages/China_7205.aspx.

8. *Id.*

9. *See Karen Millen Loses Right to Trade under Her Name*, WIPR (Aug. 18, 2016), http://www.worldipreview.com/news/karen-millen-loses-right-to-trade-under-her-name-12052.

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.*

14. *See Millen v. Karen Millen Fashions Ltd. & Anor* EWHC 2104 (Ch) (2016).

15. *Id.*

16. *See*, *e.g.*, Notice of Abandonment, U.S. App. No. 86246014 for KAREN BY KAREN MILLEN (Sept. 9, 2016); *see also*, *e.g.*, Notice of Abandonment, U.S. App. No. 86246046 for KAREN MILLEN (Sept. 9, 2016); *see also*, *e.g.*, Notice of Abandonment, U.S. App. No. 86246059 for HOME BY KAREN MILLEN (Sept. 9, 2016).

17. *See* U.S. App. No. 86246065 for HOME BY KAREN; *see also*, TTAB Opposition No. 91230754.

18. *See* Francesca Montalvo, *Protecting Fashion: A Comparative Analysis of Fashion Design Copyright Protection in the U.S. and Europe*, Cardozo Arts & Ent. L.J. Blog (Sept. 19, 2014), http://www.cardozoaelj.com/2014/09/19/protecting-fashion-a-comparative-analysis-of-fashion-design-copyright-protection-in-the-u-s-and-europe/#footnote_plugin_tooltip_47.

19. *See* Susanne Kapner, *When Is Kate Spade Not Kate Spade? When She's Frances Valentine*, W.S.J. (Aug. 23, 2016), https://www.wsj.com/articles/when-is-kate-spade-not-kate-spade-when-shes-frances-valentine-1471971817.

20. *Id.*

21. *See JA Apparel Corp. v. Abboud*, 682 F. Supp. 2d 294 (2010).

22. *See* 15 U.S.C. § 1115(b)(4).

23. *See supra* note 22.

24. *See Gucci v. Gucci Shops, Inc.*, 688 F. Supp. 916 (1988).

25. *Id.*

26. *See Paul Frank Industries, Inc. v. Paul Sunich*, 502 F. Supp. 2d 1094 (2007).

27. *Id.*

28. *See supra* note 20.

29. *Id.*

30. *See* http://www.hsn.com/search?query=catherine+malandrino (March 22, 2017).

31. *See* Emily Farra, *Catherine Malandrino Is Back with a See-Now-Buy-Now Collection*, Vogue (July 20, 2016) http://www.vogue.com/article/catherine-malandrino-new-see-now-buy-now-hsn-collection.

32. *See* Eric Wilson, *Catherine Malandrino's French Collection for HSN Is as Crave-Inducing as a Baguette*, InStyle (June 24, 2016), http://www.instyle.com/fashion/preview-catherine-malandrino-hsn-collection.

33. *See* Lisa Lockwood, *Catherine Malandrino's Rendez Vous With HSN*, WWD (June 14, 2016), http://wwd.com/business-news/retail/catherine-malandrinos-rendez-vous-hsn-10454729/.

34. *See*, *e.g.*, *1-800 Contacts, Inc. v. Lens.com, Inc.*, 722 F.3d 1229, 1242 (10th Cir. 2013); *see also*, *e.g.*, *Network Automation, Inc. v. Advanced Sys. Concepts, Inc.*, 638 F.3d 1137, 1145 (9th Cir. 2011); *Rescuecom Corp. v. Google Inc.*, 562 F.3d 123, 127 (2d Cir. 2009).

35. See U.S. Patent No. D533, 719.

36. *See supra* note 20.

37. *Id.*

38. *Id.*

39. *See* USPTO Office Action, Reg. No. 4965459 FRANCES VALENTINE (Feb. 1, 2015), http://tsdr.uspto.gov/documentviewer?caseId=sn86421476&docId=OOA20150201200019#docIndex=21&page=1; *see also*, Response to Office Action, Reg. No. 4965459 FRANCES VALENTINE (Feb. 3, 2015), http://tsdr.uspto.gov/documentviewer?caseId=sn86421476&docId=ROA20150204173616#docIndex=19&page=1.

40. *See* 15 U.S.C. § 1052(c); *see also TMEP* § 813.01(a).

41. *See supra* note 20.

42. *Id.*

Section Activities and Notices

Join New Committee on Data Privacy and Cybersecurity

The Data Privacy and Cybersecurity Committee is a newly formed Section committee the mission of which is to help Section members become familiar and keep up to date with the complicated and ever-changing set of data privacy and cybersecurity laws, regulations and practices of which IP practitioners are increasingly expected to have mastery.

The Committee will do this through formal and informal presentations, panels and gatherings to bring together and be a community for interested members of the Bar—whether practiced in, or just beginning to explore, the exciting legal areas of data privacy and cybersecurity.

If you are interested in these or other aspects of data privacy and cybersecurity and would like to become involved in the committee, please contact Committee Chair Daniel Forester (dforester@cgsh.com) for more information.

Welcome New Intellectual Property Section Members

The following members joined the Section from November 1, 2016 to March 20, 2017.

First District

Aldo A. Badini

Magdalena Berger

Emma Louise Burrows

Robert W. Clarida

Katherine Jane Daniels

Andrea Silvia De Vos

Danielle Efros

Jill Amy Ellman

Kimberly Endelson

Jordan Fletcher

John Allison Flippen

Wendy B. Heilbut

Marijan Stephan Hucke

Eirini Ioannidi

Robert Rand Isen

Samantha Nicole Kevitch

Evan D. Krauss

Jessica Garrett Kraver

Alan R. Kusinitz

David Jacob Leffler

Elizabeth Lin

David Avrum Manspeizer

Amanda Joy Matossian

Kailee D. McMahon

James C. McPherson

Amanda Mergel

Alexander J. Mise

Grace Lorraine Pan

Robert J. Reicher

Matthew S. Schweber

Karan Singh

Jacqueline E. Suarez

Jameelah Hanan Tucker

Delton Lee Vandever

Lisa Marie Willis

Bryan J. Wolin

Dongyuan Yin

Second District

Steven Deolus

Ryan Weest Fox

David Gerard

Zachary Isaac Gold

Brett E. Lewis

R. James Madigan, III

Keesha U. McCray

Richard J. Moylan

Abimbola Olusegun Onafuwa

Arthur Shalagin

Third District

Hon. Walter J. Forman

Fourth District

Erica M. Hines

Sixth District

Derek Lewis Burrows

Edward Thomas Lentz

Seventh District

Joseph Ambrose D'Angelo

Eighth District

Robert C. Atkinson

Meaghan Phelan Kelsey

Charlotte D. Roederer

Benjamin Thomas White

Ninth District

Richard M. Blank

Natascha Bianca Maria Feenstra

Peter T. Mastroianni

Brad Alan Schwartz

Tenth District

Peter A. Ackerman

David J. Fryman

Barry Maxwell Golden

Philip M. Kazin

Christopher V. Lerch

James J. Lillie

Jennifer A. McLaughlin

David Michael Mott

James A. Notaris

Lois M. Sicignano Rowman

Sherry L. Singer

William Valet

Andrew F. Young

Eleventh District

Avish Dhaniram

Saverio LoMonaco

Diane Mantaring

Yi Wang

Thirteenth District

Zoya Shpigelman

Out of State

Khwaja M. Ahmad

Adam S. Bialow

Kerry Brockhage

Matthias Amiel Brown

Daniel Richard Brownstone

Gina Bucciero

Patrick William Carrington

Samuel S. Chi

Ellen Diner

Grace Marie Duffin

Tianqi Fang

Aaron Samuel Fischer

Nicole Jie Shan Foo

Eric J. Fues

Jayita Guhaniyogi

David Haffner

Alex Hanna

Laurence R. Hefter

Laura Irazoque

Edward M. Kabak

Evi T. Katsantonis

Allen J. Klein

Eugene David Kublanovsky

Steven J. Levine

Maryann Eileen Licciardi

Wenzhuo Liu

Nancy Livak

John David Mayberry

Taketo Nasu

Kaitlyn A. Pacelli

Alix Phillips

Shari L. Pire

Briana Polan

Binwu Qin

Ryan Andrew Raichilson

Joanna Michelle Rotenberg

Timothy G. Rothwell

Christopher M. Scott

Leslie Joan Shanley

Priya Sudersan

Michael Vincenti

Zhenghui Wang

Xue Wang

Zi Wang

Tatsuo Yabe

Ayman Elfatih Yousif

Shuhua Zhang

Feifei Zhang

Section Committees and Chairs

The Intellectual Property Law Section encourages members to participate in its programs and to contact the Section Officers or Committee Chairs for information.

Advertising Law
Brooke Erdos Singer
Davis & Gilbert LLP
1740 Broadway
New York, NY 10019
bsinger@dglaw.com

Copyright Law
Alexandra Goldstein
380 Riverside Drive
Apt. 4K
New York, NY 10025
alex@alexandragoldstein.com

Diversity Initiative
Joyce L. Creidy
4617 6th Avenue
Brooklyn, NY 11220
joyce.creidy@thomsonreuters.com

Deborah Robinson
Viacom Inc.
1515 Broadway
New York, NY 10036-8901
deborah.robinson@viacom.com

Ethics
Philip Furgang
Furgang & Adwar, LLP
1325 Avenue of the Americas, 28th Fl.
New York, NY 10019
philip@furgang.com

Rory J. Radding
Locke Lord LLP
3 World Financial Center, Ste 2001
New York, NY 10281-2101
rory.radding@lockelord.com

In-House Initiative
Joseph John Conklin
Coty Inc.
350 5th Avenue
New York, NY 10118
Joseph_Conklin@cotyinc.com

International Intellectual Property Law
Stacy Lynn Wu
CBS Corporation
51 West 52nd Street
New York, NY 10019
stacywu@gmail.com

Dinisha Fernando Nitkin
Ladas & Parry LLP
1040 Avenue of the Americas
New York, NY 10018
dnitkin@ladas.com

Internet and Technology Law
Richard L. Ravin
Hartman & Winnicki, PC
115 West Century Rd
Paramus, NJ 07652
rick@ravin.com

Yitzy Nissenhaum
268 High Street
Passaic, NJ 07055
yitzniss.attorney@yahoo.com

Legislative/Amicus
Charles Eric Miller
Eaton & Van Winkle LLP
3 Park Avenue, 16th Floor
New York, NY 10016
cmiller@evw.com

Litigation
Marc A. Lieberstein
Kilpatrick Townsend & Stockton LLP
1114 Avenue of the Americas, 21st Fl.
New York, NY 10036-7709
mlieberstein@kilpatricktownsend.com

Paul W. Garrity
Sheppard, Mullin, Richter
& Hampton LLP
30 Rockefeller Plaza, 39th Fl.
New York, NY 10112-0015
pgarrity@sheppardmullin.com

Membership
William Robert Samuels
W.R. Samuels Law PLLC
280 Madison Avenue, Ste. 600
New York, NY 10016
bill@wrsamuelslaw.com

Robin E. Silverman
Golenbock Eiseman Assor Bell
& Peskoe LLP
437 Madison Avenue
New York, NY 10022
rsilverman@golenbock.com

Patent Law
Douglas A. Miro
Ostrolenk Faber LLP
1180 Avenue of the Americas, 7th Fl.
New York, NY 10036
dmiro@ostrolenk.com

Michael A. Oropallo
Barclay Damon LLP
One Park Place
300 South State Street
Syracuse, NY 13202-2078
moropallo@barclaydamon.com

Trademark Law
William Robert Samuels
W.R. Samuels Law PLLC
280 Madison Avenue, Ste. 600
New York, NY 10016
bill@wrsamuelslaw.com

Andrew Ashford Tucker
Fross Zelnick Lehrman & Zissu
866 UN Plaza
New York, NY 10017
atucker@fzlz.com

Trade Secrets
Victoria A. Cundiff
Paul Hastings Janofsky & Walker, LLP
75 East 55th Street
New York, NY 10022
Victoriacundiff@paulhastings.com

Andre G. Castaybert
Castaybert PLLC
830 Third Avenue, 5th Fl.
New York, NY 10022
acastaybert@ac-counsel.com

Transactional Law
Robin E. Silverman
Golenbock Eiseman Assor Bell
& Peskoe LLP
437 Madison Avenue
New York, NY 10022
rsilverman@golenbock.com

Danielle Ella Maggiacomo
Locke Lord LLP
750 Lexington Avenue
New York, NY 10022
danielle.maggiacomo@lockelord.com

Young Lawyers
Nyasha S. Foy
IILP
185 West Broadway
New York, NY 10013-2921
nyasha.foyesq@gmail.com

NEW YORK STATE BAR ASSOCIATION

☐ I am a Section member — please consider me for appointment to committees marked.

Name ____

Address ____

____

City ________________ State _____ Zip ________________

The above address is my ☐ Home ☐ Office ☐ Both

Please supply us with an additional address.

Name ____

Address ____

City ___________________ State _____ Zip ____________

Office phone (_______) __________________________

Home phone (_______) __________________________

Fax number (_______) __________________________

E-mail address ______________________________________

Date of birth _______ /_______ /_______

Law school ____

Graduation date _____________

States and dates of admission to Bar: ____________________

Please return this application to:

MEMBER RESOURCE CENTER,

New York State Bar Association, One Elk Street, Albany NY 12207

Phone 800.582.2452/518.463.3200 • FAX 518.463.5993

E-mail mrc@nysba.org • www.nysba.org

Join a committee

Professional Growth

Intellectual Property Law Section Committees address unique issues facing attorneys, the profession and the public.

Committees allow you to network with other attorneys from across the state and give you the opportunity to research issues and influence the laws that can affect your practice. Committees are also an outstanding way to achieve professional development and recognition. Attendance at some committee meetings can earn you MCLE credits. Law students are welcome to join the Young Lawyers Committee. Young lawyer members may apply for the Section's Young Lawyer Fellowship Program designed to provide leadership opportunities for young lawyers. Section members may join more than one committee.

Intellectual Property Law Section Committees

Please designate from the list below, those committees in which you wish to participate. For a list of committee chairs and their email addresses, visit the executive committee roster on our website at www.nysba.org/ipl

___ Advertising Law (IPS3000)

___ Copyright Law (IPS1100)

___ Cyber Security and Data Privacy (IPS3200)

___ Diversity Initiative (IPS2400)

___ Ethics (IPS2600)

___ In-House Initiative (IPS2900)

___ International Intellectual Property Law (IPS2200)

___ Internet and Technology Law (IPS1800)

___ Legislative/Amicus (IPS2300)

___ Litigation (IPS2500)

___ Membership (IPS1040)

___ Patent Law (IPS1300)

___ Pro Bono and Public Interest (IPS2700)

___ Trademark Law (IPS1600)

___ Trade Secrets (IPS1500)

___ Transactional Law (IPS1400)

___ Website Task Force (IPS3100)

___ Young Lawyers (IPS1700)

Submission of Articles

Anyone wishing to submit an article, announcement, practice tip, etc., for publication in an upcoming issue of *Bright Ideas* is encouraged to do so. Articles should be works of original authorship on any topic relating to intellectual property. Submissions may be of any length.

Submissions should preferably be sent by e-mail to Jonathan Bloom, Editor-in-Chief, at the address indicated on this page. Submissions for the Summer 2017 issue must be received by July 14, 2017.

Accommodations for Persons with Disabilities: NYSBA welcomes participation by individuals with disabilities. NYSBA is committed to complying with all applicable laws that prohibit discrimination against individuals on the basis of disability in the full and equal enjoyment of its goods, services, programs, activities, facilities, privileges, advantages, or accommodations. To request auxiliary aids or services or if you have any questions regarding accessibility, please contact the Bar Center at (518) 463-3200.

Bright Ideas is a publication of the Intellectual Property Law Section of the New York State Bar Association. Members of the Section receive a subscription to the publication without charge. Each article in this publication represents the author's viewpoint and not that of the Editors, Section Officers or Section. The accuracy of the sources used and the cases, statutes, rules, legislation and other references cited is the responsibility of the respective authors.

ISSN 1530-3934 (print)   ISSN 1933-8392 (online)

QUALIFIED. CONSISTENT. TRUSTED.

LAWYER REFERRAL

As the world evolves, so does the New York State Bar Association Lawyer Referral and Information Service.

In the age of online marketplaces, the legal profession is experiencing a moment of opportunity. By deeply embedding these tools in our program, we have laid the foundation for seamless connection between our LRIS members and the public.

Better yet, the NYSBA LRIS meets the ABA Standards for Lawyer Referral. You can trust the growth of your practice to a top-notch referral service.

NEW, QUALITY REFERRALS

Our trained, experienced staff screens these calls and passes on the vetted legal matters to our panel members.

COST EFFECTIVE

With one low yearly cost to join our panels, our goal is for every attorney to receive referrals that allow them to earn back the cost of joining the panel and then some.

TRUSTED

Meets ABA Standards for Lawyer Referral

WEB & MOBILE BASED

Our platform offers a range of benefits to members, including online access to your referrals and disposition reporting.

FOR MORE INFORMATION

www.nysba.org/JoinLR | LR@nysba.org | 800.342.3661

NYSBA

NEW YORK STATE BAR ASSOCIATION
INTELLECTUAL PROPERTY LAW SECTION
One Elk Street, Albany, New York 12207-1002

NON PROFIT ORG.
U.S. POSTAGE
PAID
ALBANY, N.Y.
PERMIT NO. 155