Privacy Law Issues for Trademark Lawyers

INTA Data Protection Committee, Education & Awareness Subcommittee

Chair: Philip V. Marano (Greenberg Trauring LLP)

Vice Chair: Nicola Benz (MLL Legal)

Subcommittee Chair: Stephanie O. Sparks (Hoge Fenton Jones & Appel)

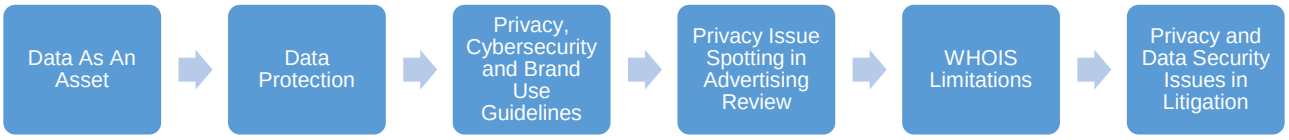
Author: Liisa M. Thomas (Sheppard Mullin Richter & Hampton LLP)

INTA Liaisons, Lori Schulman, Erica Vaccarello

October 2023

Privacy Law Issues for Trademark Lawyers

Trademark lawyers, when thinking about how organizations can protect brand value, often see issues that go well beyond standard intellectual property issues. Practitioners may get involved in public relations matters, management of third-party partners, and more. One area that arises with increasing frequency is privacy. When a deal involves personal information, there are several key privacy and data security issues trademark practitioners should keep in mind. These are outlined below, along with some key concerns in each category.



Data As An Asset

Data takes many forms. IP practitioners typically think about assets that fall under trademark, copyright, patent, or trade secret protection. In some cases, data assets will include personally identifiable information, and when that is the case, privacy concerns will come into play. The following are top considerations to keep in mind when thinking about data assets that include personally identifiable information:

1. **What type of personal information is involved?** Certain types of personal information receive additional protections. Understand if there is "sensitive" information (in the US, this typically includes financial and health data or information about children; in the EU, this typically includes religion, race, and ethnic origin). Think too, about where the individuals reside, and thus what privacy laws will be involved.

2. **How will the asset be used?** Unlike trademark, copyright, patent or other IP assets, the ability to use personal information does not center on ownership. As between the individual whose information it is and the company, most privacy laws (and courts) hold that the individual owns the information. Thus, the question to ask is whether the company has the right to use the information. Under most privacy laws, the ability to use information turns on providing individuals with notice of how their information will be used, and in some circumstances, giving them the ability to opt out of (or opt into) those uses. Thinking through how the information will be used is thus an important step in ensuring that the asset can be exploited as intended.

3. **Will the data be shared with a third party?** The fact that data is an asset often arises in deals with third parties. It might be a license agreement where a variety of assets are being transferred. Or maybe it is a development agreement, where a third party is engaged to help create content. If personal information is one of the transferred data assets, think about whether the parties have the underlying rights to share that information. Data sharing agreements where personal information will be transferred will also need data use limitations, as well as protection obligations. These will either be required under certain

privacy laws (think GDPR or some US state privacy laws) or be things that companies want to include to protect the information they are sharing.

4. **How was the asset originally obtained?** Was the information gathered from the individual directly? Did the individual provide consents to having their information used as intended? Did they give consent to -or were they aware of- sharing with third parties for the third parties' purposes? These questions - and more - will impact the ability to exploit personal information.

5. **Special considerations for assets obtained as part of an acquisition**: These days, most deals will be staffed with specialists who focus on privacy and data security, and the IP practitioner will not support that part of the deal. If, though, you do find yourself on a deal that does not have a privacy practitioner, what steps should you take? Think about whether the platforms or content you have reviewed as part of your diligence involve personal information. Did you see as part of your review use of trademarks on a website or in domain names? You can look at those sites to see if there is also information collection occurring (it is rare to find a site without it).

Data Protection

Many jurisdictions have laws that require protection of personal information. Failure to properly protect information can carry significant consequences, including diminishing brand value. Trademark practitioners who find themselves involved in projects that involve these assets can support their privacy colleagues by keeping the following in mind:

1. **Most jurisdictions require "appropriate" security measures**: Most US states, as well as almost every country with a data privacy law, require that companies protect the personal information they maintain. Some of these laws limit protection obligations to "sensitive" data. Others permit protections that are appropriate and reasonable to the type of information the company maintains. Several of these laws include specific steps that companies must take. These might include contractual controls when sharing personal information, encrypting data in motion, appointing someone to oversee data security, or training personnel.

2. **Failure to protect data may result in obligations to make public statements**: Almost every jurisdiction now has a breach of notification law. In other words, a law that imposes an obligation to publicly disclose if a company has suffered an incident that resulted in the unauthorized access or acquisition of personal information. These laws may require notification to impacted individuals, regulatory authorities, or both. Regardless of whom the company *must* notify, the notification made usually results in the press -and the public- becoming aware of the incident. This, as noted earlier, can have a negative impact on brand value.

3. **Security obligations should be incorporated into agreements with third parties**: IP practitioners are used to conducting diligence when entering into agreements with third parties. Licensing a trademark from another company? You will first check to ensure that the entity has sufficient rights to the mark. Similarly, when entering into an agreement with a third party where personal information will trade hands, diligence is needed. Here, you

can partner with your security team. If you are the transferor, does the recipient have appropriate security measures in place? Most security professionals have routine checklists or audit procedures in place to evaluate these measures.

Privacy, Cybersecurity, and Brand Use Guidelines

Are you a franchisor? Do you allow others to use your trademark? Will others be collecting or using personal information when they use your brand? If so, the following are key issues to keep in mind when establishing brand use guidelines:

1. **Will you allow the franchisee/licensee to use the information collected in connection with your brand?** It may seem that letting the franchisee or licensee use information (or not use information) is a foregone conclusion. However, this is still a conversation worth having. Perhaps, though, the relationship has been in place for some time. These brand guidelines may then be an opportunity to discuss the pros and cons with the business team. There are benefits to having the franchisor serve as the central clearinghouse of data use. And often individuals -unaware for example of a franchise relationship- may believe that the communications they receive are coming from the franchisor. But being the sole data user comes with administrative burdens as well. Once these practical considerations have been taken into account, applicable trademark-use related guidelines can be drafted – or updated.

2. **Ensure that the franchisee/licensee uses at least the same data protection measures you use as the brand owner**: Your brand use guidelines can provide directions on how to protect information. Obligations might go further than mere compliance with the law. To the extent that franchisees or licensees are processing credit card data, for example, you will want them to adhere to PCI-DSS (payment card industry security standards). Your organization may also adhere to NIST, ISO, or other voluntary standards programs that you want your franchisees/licensees to follow as well.

3. **What do you want the franchisee/licensee to do in the event of a data breach?** Often, as the brand owner, individuals will turn to you in the event of a data breach. Regulators, too, may bring action as the result of a licensee or franchisee suffering a breach. Getting notification in the event of a potential incident, and cooperation should one occur, is thus important. Brand guidelines might not be the place -or the only place- where you insert processes for breach notification. They might instead exist in the master franchise agreement or separate data security addenda. But reviewing the brand guidelines is a good reminder to check the underlying agreement for these kinds of provisions, to help support brand value protection.

4. **What representations will be made to the individual about how their information will be used?** Here, the answer will turn in large part on who will be using the information. Will it be you, the brand owner? Or will it be the licensee? Or both? Individuals will need to know what will be done with their information, including who will use it.

5. **How do you need the franchisee or licensee to coordinate with you in the event that an individual wishes to exercise privacy rights?** Many privacy laws provide for individuals to exercise rights like having their information corrected. The laws may also permit individuals to get access to the information a company holds, or -with exceptions-

to have their personal information deleted. When franchisors and franchisees are jointly collecting and using information, they will need to address how they will jointly respond to these requests.

6. **Will you permit the franchisee/licensee to share information with third parties?** It may initially appear that the answer to this question is a resounding "no." However, there may be circumstances where personal information needs to be shared, or where the need to share information is not readily apparent. For example, vendors performing technical backend services on the franchisee or licensee's behalf may need access to personal information belonging to customers. When this is the case, data security provisions should be contemplated, as well as limitations on onward transfer. There may also need to be localization requirements in place (not exporting to certain countries, for example).

7. **Are you operating in a regulated space?** In addition to the previous considerations, companies in regulated spaces (think health care, financial services) should keep in mind that additional restrictions may exist. In the US, for example, the Health Insurance Portability and Accountability Act (HIPAA) impacts how health care service providers can use -and share- personal information. Gramm-Leach-Bliley does the same for financial service providers in the US.

Privacy Issue Spotting in Advertising Review

Trademark practitioners often review advertising copy for compliance issues. In addition to thinking about advertising law concerns (which are outside of our scope here, but – as discussed below - can also include between data privacy laws, truth-in-advertising requirements, and related disclosures to customers), there are many privacy items to issue spot as well. These include the following:

1. **Rights to people's image or likeness**: Does the ad content include images of individuals? If so, ensure that appropriate consents have been obtained for use of their image and likeness for advertising purposes.

2. **Using contact information (especially for texting)**: Does the ad campaign include collection of personal information? Examples might be loyalty programs, sweepstakes, or rebate deals. Typically, the business team will want to use the information collected for advertising purposes. Consent for these advertising purposes often needs to be expressly obtained. That express consent requirement usually exists outside of the US, but even in the United States express consent may be necessary (in the texting context, for example).
3. **Restrictions on biometric data collection:** Many campaigns or programs reviewed by trademark lawyers may use biometric identifiers. This might include facial recognition (checking in for hotel visitors) or fingerprint technology. Many jurisdictions require express consent for collection and use of this information (with Illinois notably providing for a private right of action).

4. **Employing tracking technologies in ad campaigns**: It's rare that a company will launch a digital campaign without some form of tracking. These tools measure click and open rates, ad reach, and more. The sophistication of the tools is rapidly growing, and with it regulatory concern over these practices. Whether enacted specifically by law or enforced

by regulators under concepts of deception or unfairness, companies are expected to clearly disclose if they use tracking technologies, and what those technologies will be doing. The tools also require use of an extensive network of vendors, who should be required to follow not only privacy laws, but industry standards (DAA, NAI, etc.) as well.

5. **Disclosing keystroke loggers:** A related concern is around keystroke logging technology. Here, too, companies will want to ensure that appropriate disclosures are made, so make sure to ask if the platform you are reviewing will include this technology. If so, what is being tracked, and why?

6. **Incorporating chat bots**: Many websites, including those developed for particular ad campaigns (like sweepstakes) are incorporating automated "chat" tools to answer user questions. A few jurisdictions (with California leading the way) require disclosing the "chat" is a bot, not a person.

7. **Avoiding deceptive "dark pattern" activities**: There is rising concern by regulators and pundits alike that consumers are being deceived into either providing too much personal information, or agreeing to have their information used in ways that they would not have done if they truly understood a company's plans. The typical recommendation provided by regulators to avoid these practices is to be "clear and upfront" with consumers. This requires a review of the platform or tool from the perspective of the user.

WHOIS Limitations

In the early days of the internet, one of the primary concerns for trademark lawyers were domain names that infringed on their companies' brands. Website users, they feared, might believe that a domain name that contained a company's brand was associated with that company. Holding the domain registrant accountable under trademark law was a straightforward option – provided you could figure out who had registered the URL.

Originally, WHOIS (the database and technical protocol where domain name ownership could be researched) contained unredacted contact information for domain registrants. That changed with a rising concern over protecting privacy and heightened regulatory penalties imposed under the GDPR. Currently, entities responsible for publishing WHOIS data redact the identity of registrants or mask them with proxy registration services. Regulatory changes are in the works, and some form of publicly available WHOIS data may thus one day return. In the interim, what steps can a company take in the face of ownership anonymity?

1. **Old fashioned sleuthing**: Whether through a close review of the website in question, web searches more broadly, historic WHOIS data, or other public data still associated with domain names (such as the registration dates and associated nameservers), contact or ownership information may be available even if it isn't listed in the WHOIS database.

2. **Submit a request to the registrar**: Registrars -those who sell domain name registrations to registrants- are required to receive complaints of abuse and registrant reveal requests. Often, they will not provide contact information. However, depending on the nature of

infringing, malicious, or otherwise illegal activity associated with a domain name, they may assist in disclosing underlying registration data or disabling the domain name.

3. **Send a Cease-and-Desist**: Beginning a "conversation" with the registrant by sending a cease-and-desist letter through the contact point they have provided with the registrar might be a good starting point. However, depending on the nature of the concern, this may not result in much movement.

4. **File a trademark infringement suit or use complaint procedures (like a UDRP complaint)**: Most jurisdictions allow for expedited trademark infringement claims to be filed in the event that a domain name contains a company's trademark. Similarly, there are administrative quasi-arbitral avenues that can be exercised, such as the URS, UDRP, or equivalent procedures adopted within ccTLDs. Most of these claims and procedures provide a means to deanonymize a domain name registrant.

Privacy and Data Security Issues in Litigation

Trademark litigators -like all litigators- are faced with privacy concerns during discovery. This is especially true in jurisdictions like EU countries, where the ability to disclose personal information, including in litigation, is limited. With this in mind, what should the litigator keep in mind when faced with discovery that includes personal information?

1. **Know that the other side may resist disclosing personal information**: This is especially true when you are involved in multi-country litigation, and one of the countries is in the European Union.

2. **Consider if redacted or anonymized information will be sufficient**: In some cases, the aims of the discovery may be served even if you do not have personally identifiable information. Perhaps you want, for example, to review an email thread, but don't need to have the sender's full name or their email address.

3. **Evaluate whether legal exceptions exist to releasing personal information**: These exceptions may assist in fighting against the other side's disclosure resistance. They may, similarly, be important in deciding what to share in response to a discovery request.