Bloomberg BNA

Internet Law Resource Center™

Source: Electronic Commerce & Law Report: News Archive > 2017 > Latest Developments > Bloomberg Insights > Trademarks: Trademark Licensor Quality Control Should Extend to Licensee Data Protection

DATA PROTECTION

Data breach incidents are occurring at alarming rates, yet businesses' collection of consumer data is still on the rise, Patrick J. Concannon of Nutter McClennen & Fish writes. He discusses the steps brand owners should take to ensure that businesses licensing their trademarks are properly safeguarding consumer information.

Trademarks

Trademark Licensor Quality Control Should Extend to Licensee Data Protection

By Patrick J. Concannon

Patrick J. Concannon is a partner in Nutter's intellectual property and corporate and transactions departments. He focuses his practice on U.S. and international trademark clearance, trademark portfolio management, trademark and copyright licensing, and privacy matters. Patrick can be reached at pconcannon@nutter.com.

Data breach incidents have dominated headlines in recent months, stirring consumer concerns about identity theft and business concerns about breach liability. The risk of reputational harm can't be understated. It is looming large for all types of businesses—including those that don't collect financially sensitive information like account numbers, social security numbers, or other information typically associated with identity theft. Wherever consumer information is collected by or in connection with a branded product or service, including in the course of promotional activities and marketing practices, there is inherent brand vulnerability.

Trademark licensors need to exert control over the quality of a licensee's products or services sold under a licensed mark. That much is axiomatic. Where a trademark licensee sells products or services that entail data collection, the proper handling and safeguarding of the collected data is an important aspect of the quality of the product or the service. Careful cybersecurity and data protection diligence is called for where a brand owner licenses its trademark for use by another.

The best way to avoid data breach liability is to avoid or curtail data collection. This is not a practical option for many brand owners, however, in view of the emergence of the "internet of things" phenomenon. Functional products of all types, products that in the past operated independently from one another, are communicating with each other to adjust to consumer and service provider specifications. Data collection and product and service functionality increasingly are intertwined. The ability to provide a customized user experience requires collecting and sharing data about behaviors and preferences among complementary, branded devices.

Apart from the internet of things phenomenon, there also is a broader trend toward providing seamless user experiences across product and service platforms. Multi-layered, cross-platform brand engagement increasingly is important for businesses ranging from consumer electronics manufacturers to professional services firms. Behind the veneer of these seamlessly interactive experiences demanded by consumers are complicated business relationships and the "stuff" that does the businesses' bidding: computer servers, sensors, processing chips, operational software, and databases, to name a few. Delivering these experiences often requires trademark licensing. It also often requires both overt and more passive (i.e., "behind the scenes") consumer data collection and sharing.

Hacked and mishandled consumer data incidents are occurring at alarming rates, yet consumer data collection and sharing is rising sharply with no end in sight. While as a society we bemoan the privacy risks, nevertheless with a louder voice we demand products and services that offer the kind of user experience that requires data

collection, usage, and sharing. Trademark licensors who leverage their brands across platforms entailing third-party use, and license their marks to new product lines manufactured by others, should engage in careful licensee data protection diligence.

An Example: Smart Toy Privacy Risks

One example of privacy-related brand vulnerability has arisen in the field of interactive smart toys, which also happens to be a hot area for brand licensing. Global sales of products and services bearing licensed trademarks generated $54.6 billion in 2016, according to a study by the International Licensing Industry Merchandisers' Association. The study found that toys closely followed apparel as the leading product sector in terms of licensed retail sales. This field obviously is an attractive one for brand owners seeking to monetize their trademarks.

In June, the Federal Trade Commission acknowledged toy-related privacy as an area of special concern in updating its guidance on complying with the Children's Online Privacy Protection Act (COPPA). The updated guidance makes clear that the data collection and handling practices that COPPA and its regulations require extend beyond websites and mobile apps to interactive devices including "connected toys and other products intended for children that collect personal information, like voice recordings or geolocation data." In July, the FBI released a consumer notice that stressed the privacy risks associated with internet-connected toys.

In 2011, Disney subsidiary Playdom agreed to pay $3 million—the largest civil penalty assessed for a COPPA violation—to settle a federal lawsuit alleging Playdom failed to provide a proper privacy notice or obtain parental consent. The lawsuit alleged Playdom had allowed children to post personal information on public pages. That was inconsistent with its privacy policy, which indicated that children under 13 were prohibited from posting personal data on the internet. Although Playdom was a subsidiary and not a licensee *per se*, it isn't hard to imagine the same privacy failures in the context of a product or service bearing a licensed trademark.

Due Diligence

Brand owners need to understand the types of data brand licensees collect, whether consent for such collection is necessary, what promises licensees make to consumers about data use and safeguarding, why they collect it, where it resides, how it is used, how it is protected (in terms of technical security and physical/procedural security measures), when and how the data is disclosed, how long it is held, and how it is disposed of when the reason for collecting it in the first place has passed. This requires the creation of policies, including meaningful sanctions for noncompliance, mapping the flow the data, and high-level organizational accountability. It also requires careful planning for when things go wrong.

Trademark licensors in particular should consider the following measures to better understand the risks associated with a trademark license relationship and to control the quality of trademark licensees' products and services.

1. Read the potential licensee's outward facing privacy notice to understand the promises made to consumers.

2. Read the potential licensee's internal policies, including its information security program, data breach and security incident response policy/process, and employee training policies. If there is an unusual delay in providing these policies, or awkward silence in response to a verbal inquiry about them, that is a yellow flag.

3. Take the steps necessary to fully understand how the licensed product or service operates and map the flow of the data. Is the data used for marketing purposes of behavioral advertising purposes, or shared with third parties for those purposes?

4. Inquire about and assess the licensee's network security, including use authentication protocols.

5. Inquire about the licensee's vendor oversight practices as they pertain to collected and shared data.

6. Cross-reference and incorporate privacy and cybersecurity practice standards into quality control license contract provisions and include audits as an extension of traditional trademark license agreement quality control measures.

These privacy diligence considerations appropriate for assessing the risks associated with licensing a trademark are also applicable more widely to the licensee's business partners and vendors, the licensor's non-trademark licensee business partners, and the brand owner itself.

Privacy Law Compliance

Unlike the U.S.'s segmented patchwork approach to legislating in the privacy arena, the European Union has implemented a comprehensive data protection regulation, and a revised General Data Protection Regulation (GDPR) will take effect May 25, 2018. The GDPR applies where EU resident data is collected, even if the data

collector and the computer servers upon which the data resides are outside Europe. Its enforcement provisions include steep fines for violations.

It is important to ask questions about and assess a prospective licensee's compliance with data protection laws such as EU law as opposed to merely seeking contractual representations about compliance. Regulatory schemes can be triggered by data subject location (the comprehensive EU law is triggered by collecting EU resident data), data subject age (COPPA applies to the collection of data about children aged under 13 years), or the collecting party's business sector (the Health Insurance Portability and Accountability Act addresses the protection of consumer medical information, the Gramm Leach Bliley Act addresses the protection of consumer medical information, etc.).

Brands involve trust, and protecting consumer (and business) information from ending up in the wrong hands should be viewed as a fundamental aspect of a brand's promise. Brands will best be served by custodians who recognize the data protection risks inherent in interconnected products and services and engage in diligence efforts and quality control with data protection at front of mind.

ISSN 2159-3051