American Bar Association, Section of Litigation
Intellectual Property Litigation Committee

ARTICLES

Four Privacy Law Considerations for Trademark Counsel

Some data privacy laws interfere with trademark counsel's ability to investigate infringement and enforce marks.

By Tara Aaron-Stelluto – June 29, 2020

New legislation on privacy and data protection is sweeping the nation. From California to Illinois to Vermont, states are passing or considering laws related to data protection, breach notification, uses of artificial intelligence, and regulations on the data brokerage business. At the same time, breaches are a daily occurrence, and many consumers feel it is harder and harder to control their data and maintain any online privacy at all. It may seem obvious that trademark counsel should be concerned with their companies' data protection policies. Many businesses have already experienced a loss of consumer trust and brand goodwill after headline-making data losses. But a review of the privacy laws and regulations around the country and around the world, and the effects that they have had in some unexpected areas, reveals that there is more to the story.

Diligent compliance with relevant privacy laws is crucial to maintaining consumer trust, and law firms need to consider compliance as well. At the same time, though, some of these laws are interfering with trademark counsel's ability to investigate infringement and enforce marks. And some of the regulations accompanying some privacy laws may be creating the potential for even more user confusion. This article touches on each of these issues and suggests steps that trademark counsel can take to protect their clients and their companies' reputations in this new onslaught of privacy legislation.

1. Data Breaches
Companies will get hacked, and employees and third-party vendors will make security errors. One study by Risk-Based Security found that nearly 8 billion personal data points from consumers around the world were exposed either publicly or to hackers in the first three quarters of 2019 alone. Compared with the same time frame in 2018, the number of breaches was up 33 percent and the number of personal records exposed increased 112 percent.

Consumers are obviously distressed when a data breach occurs—identity theft from the most fulsome breaches is a real concern. But what creates outrage among a company's customers is not necessarily the breach itself, but the discovery that the company was negligent in the way it stored customers' information so that the risk of breach increased, or learning of the breach only months or years later and finding that the company attempted to conceal it. Federal Trade Commission (FTC) complaints against two major American companies are illustrative.

In 2015, the FTC filed a complaint against Wyndham Worldwide Corporation and its subsidiaries for negligent practices related to the check-in software it deployed in each of its franchised locations. The FTC alleged that Wyndham failed to use firewalls, allowed the

software to be misconfigured so that credit card numbers were stored in clear, readable text with all 16 digits, and used easily guessable passwords. *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (2015). The FTC investigation and the litigation cost Wyndham millions, and the embarrassment of a public statement from the FTC describing the allegations in detail was enormous.

In 2017, Uber announced that it had concealed a major data breach for nearly a year by paying the hackers $100,000. Revised Complaint, *In re Uber Techs., Inc.*, No. C-4662 (Fed. Trade Comm'n filed Oct. 24, 2018). Uber faces an onerous compliance burden as a result of its settlement with the FTC and paid $148 million in fines to settle a separate investigation by five state attorneys general. It also faced a surge of the #deleteuber hashtag on Twitter.

Consumers in 2015 and 2018 were taking to social media to complain, and trademark counsel are often called in to determine whether a ".sucks" campaign is protected criticism or trademark infringement. They were certainly numerous such campaigns in front of counsel for Wyndham and Uber after these instances. Obviously, neither of these incidents was helpful to the companies' brands.

To protect a company's goodwill and save counsel extra work dealing with online negative uses of the marks, the company's trademark counsel should be familiar with his or her client's data practices and stay updated on the conversations around compliance. Counsel should also be among the first to know and be given a full reporting of the company's response when a data breach occurs.

But data and privacy law compliance can cause other issues for trademark lawyers. Sometimes trademark protection and data protection clash in frustrating ways.

2. Infringement and Anti-Counterfeiting Investigations after GDPR and CCPA

The General Data Protection Regulation (GDPR) came into effect May 25, 2018, and affects businesses all around the world that process the personal information of persons in the European Union (EU). It governs the purposes for which businesses may process the information and sets forth notice and opt-out requirements.

ICANN is the governing body of the internet, including the database of registrants of domain names, known as the WHOIS database. For many years, when trademark owners discovered cyber squatters or other infringement of their marks online, the first step would be to access the WHOIS database through any internet registrar and look up the primary, administrative, and technical contact information for the owner of the website. A simple cease-and-desist letter using that information would often be enough to put a stop to the infringing activity. The GDPR put a solid end to this avenue of investigation.

ICANN was faced with two competing directives—first, its own bylaws state that in carrying out its mandates, ICANN should "adequately address issues of competition, consumer

protection, . . . and rights protection." (ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers § 1.1(a)(i) (June 18, 2018). Second, the GDPR put obligations on registrars not to make personal information of registrants publicly available without a legitimate purpose (as defined by the GDPR) for doing so. The European Data Protection Board, which is the agency in charge of enforcement of the GDPR, confirmed to ICANN that it must update its regulations to require registrars to redact all information of persons in the EU (known as "data subjects" under the GDPR), including name, personal email, physical address, and phone and fax numbers for the registrant and including the administrative and technical contact information. The registrars have mostly responded to this regulation by redacting WHOIS in full, regardless of whether the registrant is in the EU and included company information, although that was not a requirement under the ICANN regulations.

In short, the WHOIS database has at least for now lost its value as an investigation and contact tool in trademark investigations. There are efforts at ICANN to address this issue, possibly through a registry for legitimate trademark investigators, but as of this writing, no such registry exists.

In addition, the GDPR is short on clarity as to whether or not private investigations into anti-counterfeiting and trademark infringement fall under any of the Article 6 legitimate purposes. These purposes include "processing to protect the vital interests of . . . natural persons," "processing . . . for the performance of a task carried out in the public interest," and "the legitimate interest of the processor."

Trademark investigations are unlikely to be for the protection of natural persons, except perhaps in the context of investigating and preventing the import of counterfeit medicines or automobile parts, for example. "Public interest" is referred to again in Article 89 of the GDPR and appears to be limited to archiving. Companies may wish to rely heavily on this "legitimate interest" purpose, but data subjects can object to the processing of their information under this purpose. Recital 47 states that a company has a "legitimate interest" when the information is used strictly to "prevent fraud," which may cover many contexts of infringement investigations, but companies need to be cautious that the information is used for no other purpose and that the infringement indeed constitutes fraud. Further, it is debatable whether every episode of trademark infringement—apart from the most egregious cases, in which counterfeit goods are marked with the legitimate manufacturer's mark with the intent to deceive consumers—rises to the level of "fraud," at least under U.S. law. Professor Mark McKenna at Notre Dame Law school touched on this in his 2018 article "Criminal Trademark Enforcement and the Problem of Inevitable Creep," 51 *Akron L. Rev.*, Apr. 22, 2018.

If none of the three processes listed above fit the scenario, then investigators are left with GDPR Article 6(1)(a)—getting consent from the targets of their investigation. Success here may be limited.

On January 1 of this year, California's version of the GDPR came into effect, in the form of the California Consumer Protection Act (CCPA). There are significant differences between the two laws, adding to the difficulty of the compliance task. The CCPA at least allows companies to hold on to personal information for the purpose of detecting and prosecuting both fraudulent and "deceptive" practices, which broadens the scope from what the GDPR offers in terms of a data collector's ability to use data to protect itself, but again, not all trademark infringement is "deceptive." But it also allows for businesses to use information for exercising or defending a legal claim, which would almost certainly cover most trademark investigations. As long as we live in the United States without a federal privacy law, however, variations in state law will persist and may not always be drafted in favor of the investigators.

None of the privacy laws referenced above relate to how public authorities and police may process information. Often a matter moves into the criminal realm, particularly if counterfeiting is involved, and counsel may involve the police, Customs and Border Patrol, or the Federal Bureau of Investigation. However, the transfer of information from private entity to public authority is not entirely outside the purview of the GDPR. (For an in-depth and fascinating look at this topic, see Nadezhda Purtova, "Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships," *Int'l Data Privacy L.*, 2017.)

Trademark counsel should stay aware of the relevant legislation and consider what new risks may arise from the processing of personal information in infringement and counterfeit investigations. They should define the scope of the investigation as much as possible prior to starting the investigation, so that the purposes for which the information has been processed are on record and the investigators are aware of them. Many of the questions about how privacy laws will collide with trademark investigations are still open—if counsel can demonstrate a responsible accounting of the use of the personal information even of alleged criminals and infringers, any risks from these open questions will be manageable.

3. Law Firms Are Data Processors Too

The CCPA says that the law applies only to companies processing the information of 50,000 or more "consumers, households or devices." The GDPR has no such minimum threshold. To the extent you maintain the personal information, including work emails and phone numbers, of people in the European Union, you are a data processor. Certainly, trademark lawyers who attend the International Trademark Association meetings have a database full of the contact information of European lawyers; to that extent, we are all subject to the GDPR. For most law firms with European clients, compliance should not be terribly onerous. Best practices will include making sure any third-party vendors who host your client and contact information or manage your contact database warrant (or at least state) that they are GDRP-compliant. Otherwise, a law firm should be certain that it knows what information it has on European data subjects, who has access to it, and all the places where the firm stores that information. Is it only on the firm server, or are there copies in the cloud or on a third-party platform? This is generally good security hygiene, but knowing where those records live will also make the process of retrieving them in

order to respond to a data subject request much simpler. It seems unlikely that foreign contacts who have given over their business card will ask to have their data deleted, but a data processor should be prepared.

Another important step will be ensuring that the firm privacy notice is compliant with the GDPR. Articles 12 through 14 govern the privacy notice. It must be written in clear language. It must identify the Article 6 basis for processing the information, and if that basis is the legitimate interest of the data controller, then it must identify that basis. It must describe the purposes for processing the information, the data subject's rights under Articles 15 through 22, and how the subject may contact the company to exercise those rights.

If the information is transferred to any other country, the safeguards put in place around that transfer must be described. Part of the mission of the GDPR was to make sure that data were treated consistently regardless of where the data went. This means different things for different countries, but most of the non-European world now must transfer information across borders under "standard contractual clauses" provided by the European Data Protection Board that require all parties to cooperate in the protection of the information.

U.S. state laws are also likely to include requirements for a privacy notice, which means many businesses are moving to regional privacy notices or addendums for each territory.

Make sure your company's or law firm's public notice is up-to-date and accurate and that it includes all the information required by the relevant privacy laws.

4. Confusing Regulations Will Lead to Frustrated Consumers
The California Attorney General's Office recently released the updated regulations to accompany the CCPA. The CCPA requires companies that sell information to allow California consumers to opt out using a "DO NOT SELL MY INFORMATION LINK." The revised regulations included a proposed optional design for an opt-in/opt-out toggle next to this link.

Designers and privacy lawyers both had quite a few comments about this design. Does the X mean that the "DO NOT SELL" link is turned off, or does it mean "NO, DO NOT SELL MY INFORMATION"? This example is illustrative because the design issues are so glaring, but this will certainly not be the last example of privacy regulations that may lead to confusing consumer experiences. Anyone at a company who works on protecting the brand, while considering all of the compliance obligations and notices required, should also work to keep the customer-facing experience seamless and minimally frustrating. All of this will increase goodwill and reduce complaints from consumers over data protection.

Conclusion
Privacy laws are coming fast and furious, and we are likely to see several more across the U.S. this year. Trademark counsel may wish to insulate themselves from this new regulatory landscape, but just as corporate social and environmental responsibility have become touchstones

for consumer goodwill, so too will a company's data protection practices and respect for its consumers' privacy. Having a basic knowledge of the relevant laws, working with the privacy team, the information technology team, the C-suite, and even design, and keeping in mind how these laws might affect trademark investigatory work will help protect both in-house and external clients.

Tara Aaron-Stelluto, CIPP in U.S. and EU law, is a founding partner of the law firm Aaron | Sanders PLLC in Nashville, Tennessee.