Reasonable Data Access for Enforcement Purposes

15 November 2021

SPONSORING COMMITTEE: Data Protection Committee

RESOLUTION:

WHEREAS, it is universally recognized that individuals are entitled to the right of privacy and should not be subject to arbitrary interference with that right;

WHEREAS, a robust trademark system enables identification of the source of goods and services, protects goodwill and reputation, and helps consumers make safe and informed choices;

WHEREAS, the privacy rights of individuals and robust trademark protection are not mutually exclusive societal interests;

WHEREAS, brand owners require access to personal data belonging to individuals who are alleged infringers or connected with other, alleged infringing entities to enforce their trademark rights and thus protect consumers against infringement and counterfeit goods;

WHEREAS, when interpreted too broadly, certain data privacy laws restrict access to personal data making it unreasonably difficult or impossible for brand owners to enforce their trademark rights and protect consumers;

WHEREAS, online platforms, domain name registries and registrars, and other organizations responsible for controlling and/or processing the personal data that brand owners need to enforce their trademark rights and protect consumers must comply with applicable data privacy laws and may be liable for the penalties that can arise from their non-compliance;

WHEREAS, certain data privacy laws do not contain provisions that explicitly recognize enforcement of trademark rights as a lawful purpose for disclosing personal data;

WHEREAS, certain data privacy laws do not contain provisions clarifying how a brand owner can demonstrate a legitimate purpose and obtain access to the portions of the personal data information that are necessary for a brand owner to identify and contact the alleged infringer and prosecute or resolve the infringement issue;

WHEREAS, certain data privacy laws contain provisions allowing the disclosure of personal data for legitimate third-party purposes and the benefit of the public, but those exceptions are not currently clearly articulated, leaving brand owners, online platforms, domain name registries and registrars, and other organizations responsible for controlling and/or processing personal data

with no concrete guidance on the circumstances under which data can be disclosed without incurring liability;

WHEREAS, certain data privacy laws do not contain provisions allowing the disclosure of personal data for legitimate third-party purposes;

BE IT RESOLVED, that it is the position of the International Trademark Association that enforcement of intellectual property rights should be explicitly recognized, addressed, and accounted for in data privacy laws, regulations, and treaties.

BE IT FURTHER RESOLVED, that any data privacy laws, regulations and treaties must include specific and detailed mechanisms by which a rights holder can obtain access to personal data for purposes of enforcing the rights holder's intellectual property rights, provided that such mechanisms:

A. Provide that such access will be limited to that portion of the data that is reasonably necessary to allow the rights holder to identify and contact the alleged infringer and prosecute or resolve an infringement issue; and

B. Ensure that any restrictions imposed on such access be proportional to the potential harm associated with release of the specific personal data and balance the interests of the rights holder and the data subject; and

C. Provide that online platforms, domain name registries and registrars, and other organizations responsible for controlling and/or processing personal data are shielded from liability when they appropriately disclose personal data to rights holders who request access and demonstrate a good faith legitimate interest in enforcing such rights.

BACKGROUND:

Different interpretations of some data privacy regulations have created unintended challenges for accessing data for the purpose of trademark enforcement. Some early examples are the implementation of the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Similar laws have been passed across globe and many other jurisdictions are likely to follow this trend.

Not all data privacy laws contain provisions that explicitly recognize enforcement of intellectual property rights as a lawful purpose for disclosing personal data. Most current privacy laws do not contain provisions clarifying how a brand owner may demonstrate a legitimate purpose and obtain access to the portions of the personal data information that are necessary for a brand owner to identify and contact the alleged infringer and pursue legal remedies or other resolutions of the infringement issue. Some data privacy laws contain provisions allowing the disclosure of personal data for legitimate third-party purposes and the benefit of the public, but many times those

exceptions are not currently clearly articulated, leaving brand owners, online platforms, domain name registries and registrars, and other organizations responsible for controlling and/or processing personal data without concrete guidance on the circumstances under which data can be disclosed without incurring liability.

When interpreted too broadly, data privacy laws restrict access to personal data such that it is unreasonably difficult or impossible for brand owners to enforce their rights and protect consumers. We have seen this effect most dramatically in the domain name system (DNS) where access to critical domain name registration information has been essentially "blacked out" due the Internet Corporation for Assigned Names and Numbers (ICANN's) interpretation of GDPR. The severity of penalties and doubt about how to appropriately apply an untested law have created little to no risk tolerance for disclosing data for almost any purpose absent a court order. Government enforcement authorities themselves have been stymied under the broad interpretation of GDPR with the result that information requests by Law Enforcement and Data Protection Authority officers are also being denied.

Some government authorities have taken steps to amend or clarify their privacy laws to provide guidance addressing legitimate access of the data; however, when those clarifications take the form of a balancing test, brand owners must still wait for courts to provide guidance on interpretation of the balancing test in order to have clear guidelines, and it is likely not all courts will start out applying the balancing test in the same way. There should be an explicit recognition that sharing personal data with a brand owner when the brand owner's trademark rights are alleged to have been infringed, is a lawful processing.

In addition to the challenges described, certain data privacy laws do not contain provisions clarifying how a brand owner may demonstrate a legitimate purpose and obtain access to the portions of the personal data information that are necessary for a brand owner to identify and contact the alleged infringer. This uncertain landscape has created the need for strong advocacy on the behalf of brand owners, platforms, and intermediaries to ensure that there is a reasonable understanding of and limited liability for the exchange of data for legitimate purposes.

The adoption of this resolution will clarify INTA's position recognizing the need for a clear and balanced approach to requests for information for enforcement, whether the requests are related to the domain name system, anti-counterfeiting, anti-piracy, or other measures designed to protect consumers. Brand owners must not have vital avenues for information cut off, and intermediaries must be able to operate in a predictable environment when cooperating with requestors.