LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

March 2021

A Balancing Act: Mitigating Data Privacy Risks in Cross-Border Discovery

The intersection of foreign laws governing data collection and cross-border discovery operations continues to be a potentially volatile conjunction.

By Ryan Costello

The intersection of foreign laws governing data collection and cross-border discovery operations continues to be a potentially volatile conjunction. Global enterprises have been cautioned to tread carefully when responding to U.S.-driven discovery requests, as expansive discovery exercises, so common in the U.S. under federal and state laws of civil procedure, can be completely foreign and often legally problematic in jurisdictions abroad.

Accordingly, discovery requests implicating custodians and data outside the U.S. can potentially put organizations in a Catch-22: either fall short of their discovery obligations on the one hand or fall afoul of legislation in other nations prohibiting or limiting data collection and transfer to the U.S. on the other. Laws potentially conflicting with discovery obligations include blocking statutes, requirements pertaining to works council agreements and, perhaps most significantly, data privacy regulations.

In particular, it has been EU data privacy regulations, including the General Data Protection Regulation and its predecessor the Data Protection Directive of 1995 that have threatened to pose the most significant potential roadblocks to discovery requests. Given the care with which personal data must be treated under the GDPR (security requirements, data minimization obligations, rights afforded data subjects), accountability for those handling such data and the regulatory and civil fines possible under the regulation, cross-border discovery across the EU seems to warrant an especially heightened level of scrutiny.

View in the Courts

U.S. courts do not view conflict with foreign laws as a de facto bar to discovery and generally will require discovery to proceed, notwithstanding data privacy laws or other foreign legislation that may stand in the way. Relying on a Supreme Court case from 1987, *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, 482 U.S. 522, courts across the U.S. applying Aerospatiale's five-part balancing test or "comity analysis," which weighs the interests of foreign laws against U.S. discovery, almost always find that the U.S. legal process of pre-trial discovery takes precedent. In fact, as of this writing, there has not been a single case in the U.S. where a party was permitted to fully withhold production of documents based on foreign data privacy regulations.

Discovery can be **limited or curtailed** for factors such as undue burden or expense or even to protect trade secrets and intellectual property. However, the reason that such exemptions generally don't apply for conflict with foreign data protection and privacy laws is largely because the risk of enforcement has been so low.

Enforcement under the GDPR, while always possible, has indeed been limited. Unless courts see a real risk of prosecution for a company under foreign data privacy laws, they are **typically reluctant** to allow limitations to the discovery process or withholding of documents based on GDPR grounds alone. With more significant enforcement action in the future, this may change. For the time being, however, U.S. courts are likely to continue to stipulate that:

1. "[foreign] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though that act of production may violate that statute"; and

2. "the party resisting the discovery burden bears the burden [of proof] in these cases." *[Rollins Ranches, LLC et al v. Watson*, S.C. May 22, 2020]

Accordingly, while parties will almost assuredly be required to proceed with discovery, they also must consider the requirements of GDPR compliance back in the EU, as well as the specter of enforcement and/or civil proceedings for GDPR violations. So how have parties managed this transcontinental juggling act?

Solutions have comprised varying approaches including:

- Protective orders
- Redactions for anonymizing personal data in datasets
- A "privacy log" that accounts for certain documents withheld from production

Each of these has relative advantages and disadvantages; however, one crucial element underlies all approaches: seeking and identifying the breadth of personal information and personal data scattered across the datasets.

Protective Orders

Protective orders are court instructions included in production sets, such as "attorneys' eyes only," which are intended to protect against the proliferation of personal information or/sensitive data and reduce risk. U.S. courts will typically acknowledge such protections as **sufficient for GDPR compliance purposes** and allow discovery productions to proceed on that basis. However, whether or not such protective orders are sufficient from a European perspective for GDPR compliance remains to be seen.

In any event, a party will want to be clear on what documents contain what information in order to ensure that a protective order stands to reduce GDPR risks for any data subjects implicated. If challenged by an EU regulatory authority or data subject, the producing party must be able to show that it fully complied with GDPR via the protective order and can stipulate precisely what information, and what data belonging to whom, may have been produced.

Redactions

Another approach regularly taken involves redacting personal information in datasets wherever possible (provided the data is not relevant to the discovery request). Courts have, in some cases, allowed **redactions for personal information in discovery**, and it arguably offers even greater protection for EU data subjects, given that data is essentially anonymized.

However, redactions can be costly if applied manually by a review team, error-prone, time-consuming and technically difficult to achieve at scale. Innovative approaches for identifying personal information in datasets prior to, or as a part of, the review workflow can cut down on the expense and difficulty inherent in

attempting redaction of personal information. Technical processes for identifying information, prioritizing review and setting aside a workstream that focuses on redaction of personal information and QC checks can be an effective and protective means for meeting discovery obligations and ensuring GDPR compliance.

The Privacy Log

The privacy log can be one of the most comprehensive means for protecting EU personal information. Such a log allows a court to examine a summary of documents that a party wishes to withhold based data privacy grounds. The court is then **better positioned to weigh the interests of discovery against data privacy concerns** on a more concrete basis and can allow for a measured approach that significantly minimizes the GDPR compliance risk.

There is a precedent for using privacy logs with similar processes involving documents withheld for privilege, including attorney-client privilege, bank examiners' privilege and other grounds, such as intellectual property concerns. However, as noted above, courts are reluctant to withhold documents from discovery based on GDPR concerns alone. Parties are therefore encouraged to be extremely precise in noting why documents should be withheld based on data privacy, and a full accounting of the personal data contained in documents and the potential risks to data subjects must be fully understood and indicated in the privacy log.

Further Considerations

Regardless of the approach a party chooses to minimize conflicts of law and impact on data subjects, narrowing the scope of personal data implicated in discovery will be critical at each step of the discovery process. The **Sedona Conference's International Principles on Discovery, Disclosure and Data Protection** (2017) offer great guidance to this end.

However, while this article has focused on the production phase of discovery, a sufficient understanding of personal data implicated in discovery from collection to review and on to production — or at each stage of the EDRM — is essential. With the explosion of chat collaboration tools and medical information related to the COVID-19 pandemic now proliferating datasets across organizations in varied industries, innovation and creative approaches to data privacy considerations and discovery are as valuable as ever.

Conclusion

Absent knowing what personal data may be present in a given dataset, it is difficult for parties to know how best to proceed in a manner that meets the obligations of both U.S. discovery and EU data protection requirements. Solutions and best practices for highlighting personal information implicated in a discovery set, in a manner that's efficient, reliable and cost-effective, have never been more important.

***Ryan Costello**, Esq., CIPP/E/US, is head of data privacy services at ProSearch, a leading provider of comprehensive discovery solutions to corporate legal departments and law firms. A U.S.-licensed attorney and expatriate based in Europe for more than 10 years, Costello has cultivated an expertise in data protection and data privacy compliance. He assists organizations in remediating cross-border discovery risks, utilizing data management solutions and innovative technologies.*

PROSEARCH

ProSearch.com
info@ProSearch.com
877.447.7291

—❖—