New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

E-DISCOVERY

WWW.NYLJ.COM

VOLUME 261—NO. 23

MONDAY, FEBRUARY 4, 2019

Privacy: What You Should Know About New Laws

BY LAUREN E. AGUIAR, GIYOUNG SONG AND EVE-CHRISTIE VERMYNCK

The increased focus on protecting personal privacy may pose a new challenge to the bounds of e-discovery in U.S. litigation as courts reconcile whether and how new data protection laws apply to a litigant's obligation to produce relevant information.

Discovery in the U.S.

Traditionally, U.S. litigation has favored broad civil discovery, permitting litigants a wide berth to explore the factual underpinnings of their cases. Until its amendment in 2015, Federal Rule of Civil Procedure 26(b)(1) was read to empower litigants to obtain discovery with respect to any non-privileged matter provided it generally was "relevant" to a party's claim or defense. However, partially in response to the burden associated with the exponential growth of electronic discovery, this rule as amended now underscores that discovery not only be relevant, but also "proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). Some state rules, including in New York's Commercial Division, have followed suit by emphasizing proportionality in discovery.

In theory, this focus on proportionality could result in discovery requests and productions that are more tailored to the issues and electronically stored information (ESI) in question. What potentially complicates the process, however, is that relevant information can be mixed with certain additional data of both a business and personal nature; accordingly, even under a proportionate approach, that data may be swept up in a production. The U.S. legal system typically addresses any resulting privacy concerns with confidentiality agreements or protective orders and in limited instances redactions, but this approach may still result in some personal information—that may not otherwise be relevant to the case—being reviewed and produced.

A new challenge to the bounds of U.S. discovery, therefore, will be addressing the intersection of discovery with the increased awareness and focus on privacy and data protection.

General Data Protection Regulation

The European Union's (EU) General Data Protection Regulation (GDPR) became effective on May 25, 2018, and already is presenting a significant testing ground for how U.S. discovery can be reconciled with data protection requirements.

The GDPR addresses individuals' "fundamental … right to the protection

RAWPIXEL.COM VIA SHUTTERSTOCK

of personal data." GDPR, art. 1(2). It covers the personal data of individuals in the European Economic Area (EEA) (data subjects) and any *processing* of personal data by organizations directly (data controllers) or those acting under written instructions of data controllers (data processors), even if the entity is not located in the EEA but provides goods and services to data subjects in the EEA or monitors data subjects' behavior taking place in the EEA. GDPR, art. 3. As such, the GDPR impacts cross-border discovery sought in U.S. litigation because its requirements could reach parties that are foreign organizations, or domestic entities with a presence abroad, that have relevant sources of information located in the EEA. Given the global economy, this scenario is increasingly common.

This article describes some of the primary ways in which U.S. practitioners engaging in cross-border discovery may encounter the GDPR's requirements, but practitioners who

LAUREN E. AGUIAR *is a partner,* GIYOUNG SONG *is discovery counsel and* EVE-CHRISTIE VERMYNCK *is counsel at Skadden, Arps, Slate, Meagher & Flom. Associates* COLLIN A. ROSE *and* JACK A. BROWNE *and law clerk* CAITLYN A. CHELEDEN *assisted in the preparation of this article.*

may handle data covered by the GDPR would be well advised to understand the intricacies, and practical implications, of this comprehensive regulation.

Personal Data. As a threshold matter, the GDPR defines "personal data" far more broadly than what typically is understood as personal information in the United States and includes "any information relating to an identified or identifiable natural person," such as "a name, an identification number, location data, an online identifier" or "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of a person. GDPR, art. 4(1). At least some of this information may be included in such mundane places as the signature block of an email, a type of ESI that necessarily would be produced in many cases.

Processing Personal Data: The GDPR governs "processing" of personal data, which covers a wide range of actions, including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, art. 4(2).

In terms of U.S. discovery of GDPR protected data, processing encompasses, at a minimum, collection, review, deletion, production and cross-border transfer of that data. Under the GDPR, personal data must be processed "lawfully, fairly and in a transparent manner" and in accordance with the data minimization principle, which requires that processing be "adequate, relevant and limited to what is necessary in relation to the purpose" for which the data is processed. GDPR, art. 5(1). There are six lawful bases for processing, including consent, where it is necessary for the legitimate interests of a data controller or third party, compliance with a legal obligation or a contractual obligation. GDPR, art. 6(1).

Notably, litigants may have a legitimate interest in accessing information that is necessary to make or defend a legal claim, subject to demonstrating that the data subject's privacy rights do not override the litigant's legitimate interests in processing the data. Moreover, corporations may have a legitimate interest in conducting internal investigations and in responding to government investigations. Where special categories of personal data are present—such as data that reveals racial or ethnic origin, political, religious or philosophical beliefs, or health or biometric data—litigants also will be required to fulfill additional conditions.

In exceptional circumstances, consent by the data subject can serve as a basis for processing, but it must be a "freely given, specific, informed and unambiguous indication of the data subject's … agreement to the processing of personal data." GDPR, art. 4(11). Consent should be relied on cautiously because (1) it is unlikely to be valid in the common employer and employee context due to an imbalance of power and (2) if a data subject does not consent (or later withdraws consent), the litigants can no longer process the data.

Practitioners should be aware of the GDPR's heightened transparency requirements. Data subjects must be provided with notice of the intended processing activity, which should be communicated to data subjects prior to processing any of their personal data. The notice must be "concise, transparent, intelligible," in "clear and plain language," and may be incorporated directly or by reference into legal hold notices. GDPR, art. 12(1).

Transferring Personal Data. There are additional requirements for the cross-border transfer of personal data outside of the EEA, such as to the United States for use in a litigation. Generally, transfer is only permitted to a country that the European Commission (EC) has designated as providing an adequate level of protection, or through a valid transfer mechanism providing for appropriate safeguards. The EC does not consider the United States to offer an adequate level of protection, so impacted parties must make the transfer to the United States subject to appropriate safeguards or rely on one of the legal exceptions or "derogations." GDPR, arts. 46, 47 and 49. In some cases, organizations transferring data may rely on appropriate standard contract clauses or the EU-U.S. Privacy Shield, a framework allowing U.S. companies that have aligned with certain provisions of the GDPR to self-certify and transfer data from the EEA to the United States.

Explicit consent by the data subject can be a basis for transferring data to a country that is not considered by the EC to offer an appropriate level of protection, but, as with processing, this method should be used cautiously. Moreover, derogations to the transfer requirements should only be relied upon sparingly and in addition to other safeguards, if applicable.

Potential Fines. The GDPR is notable in terms of the fines it prescribes for violation: up to €20 million (approximately $23.5 million) or 4 percent of the violating company's total annual global revenue, whichever is higher. GDPR, art. 83(5). The GDPR also grants individuals the right to compensation for material and non-material damage caused by a data controller's or processor's breach of the GDPR requirements, as well as discretion for EEA countries to legislate for additional criminal sanctions for infringements.

The threat of these penalties, even if remote, makes it even more crucial to understand, and comply with, the

GDPR in the context of cross-border discovery.

Protections in Other Jurisdictions

A number of other jurisdictions, including in the United States, also have passed privacy and data protection laws which may impact discovery of covered data.

U.S. Jurisdictions. On June 28, 2018, California became the first state to enact comprehensive data protection legislation with the California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100 to 1798.199, which will become operative in approximately one year, on January 1, 2020. Like the GDPR, the CCPA has an expansive definition of covered personal information for California residents. The CCPA applies to businesses that, among other things, do business in California with annual gross revenue exceeding $25 million, as well as certain service providers processing personal information on behalf of a covered company. The CCPA focuses on the sale of personal information and includes giving consumers the right to know specifics about the personal information a business has collected from them and to have that personal data deleted. The CCPA prescribes that in case of any conflict with another California law, the law that affords the greatest privacy protections shall control. The CCPA also instructs that the new law "shall be liberally construed to carry out its purposes."

Notably, although the U.S. does not have comprehensive national data protection legislation, in mid-January 2019, a new bill was introduced in Congress aimed at creating federal privacy standards in the context of consumer protection, which could (if enacted) pre-empt state laws such as the CCPA. Laws such as these might impact the preservation, collection and production of personal information for e-discovery purposes.

Foreign Jurisdictions. Laws that may impact the processing and transfer of data exist in foreign jurisdictions in addition to the EU—including in Canada, Latin America, and Asia. As but one example, Brazil's first General Data Protection Law, which goes into effect in February 2020, applies not only to companies that collect or process data in Brazil but also extraterritorially to companies that process data related to persons in Brazil or for the purpose of offering goods or services in Brazil. Therefore, when conducting cross-border discovery in these or other jurisdictions, privacy or data protection requirements should be carefully considered.

Reconciling U.S. Discovery Rules and Various Data Protection Laws

Undoubtedly, U.S. courts will continue to examine the breadth of permissible discovery and balance it against the need to protect personal privacy, particularly as electronic data and the technology that handles it proliferate.

Undoubtedly, U.S. courts will continue to examine the **breadth of permissible discovery** and balance it against the **need to protect personal privacy**, particularly as electronic data and the technology that handles it proliferate.

However, how U.S. courts specifically will enforce discovery rules in response to the breadth of the GDPR requirements or new national privacy legislation may be somewhat unchartered territory. In reconciling foreign data protection laws with U.S. discovery rules, courts have, to date, applied a balancing test the U.S. Supreme Court established in its 1987 decision, *Société Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, which held that a French blocking statute did *not* preclude American courts from ordering discovery from a party subject to U.S. jurisdiction. 482 U.S. 522 (1987). More recently, courts have continued to hold that the interests of U.S. discovery outweigh foreign data protection laws. See, e.g., *Royal Park Invs. SA/NV v. HSBC Bank USA, N.A.*, No. 14 Civ. 8175, 2018 WL 745994 (S.D.N.Y. Feb. 6, 2018) (Belgian Data Privacy Act); *Knight Capital Partners Corp. v. Henkel AG & Co.*, 290 F. Supp. 3d 681 (E.D. Mich. 2017) (German Data Protection Act); *Laydon v. Mizuho Bank, Ltd.*, 183 F. Supp. 3d 409 (S.D.N.Y 2016) (EU privacy laws). In a different test of privacy concerns, the New York Court of Appeals, while recognizing privacy rights, has held that photographs and information posted under a privacy setting on Facebook were material and necessary evidence subject to civil discovery. *Forman v. Henkin*, 30 N.Y.3d 656 (2018).

In one of the first cases involving the GDPR since it became effective, Microsoft recently argued that retention and production of data relevant in a patent infringement case "raises tension" with the GDPR and would require burdensome steps to anonymize the personal data. *Corel Software, LLC v. Microsoft Corp.*, No. 2:15-cv-00528, 2018 WL 4855268, at *1 (D. Utah Oct. 5, 2018). Nonetheless, the court ordered retention and production, finding that the benefit of the data, which was relevant and proportional, outweighed the burden or expense of compliance.