How Social Media, Technology and Privacy Laws Are Changing the E-Discovery Landscape

Skadden

04 / 23 / 19

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

Four Times Square
New York, NY 10036
212.735.3000

Historically focused on manually wading through large volumes of email and electronic documents, e-discovery is transforming in nuanced ways. Discovery of mobile devices, social media and other online applications raises novel issues with respect to the ways in which information is obtained and preserved. Additionally, technology-assisted review (TAR) has evolved to a point where litigants recognize its benefits in the document review process, and courts are more broadly accepting its use. Finally, global privacy concerns — and in some jurisdictions, accompanying privacy laws — will test how discovery in U.S. litigation can be reconciled with data protection requirements. To effectively, and ethically, engage in e-discovery, practitioners must stay apprised of cutting-edge technology in this area and the associated changing legal landscape.

Mobile Devices, Social Media and Text Message Apps

Relevant information previously could be found in hard-copy documents physically located at a party's office or in emails and electronic documents located on a party's computers. Today, however, the exponential growth in the methods people use to communicate means that relevant electronically stored information (ESI) often resides in entirely new forms, such as on social media and text messaging apps that are hosted by third-party platforms. In addition, these communications may be made using personal devices owned by employees, who are not often parties to the litigation. A key question, therefore, is whether a corporate defendant is in possession, custody or control of relevant information stored in employees' accounts and personal devices, and thus has certain obligations with respect to preserving, and ultimate discovery of, this ESI in litigation. While courts recognize that organizations do not always have control over data in employee devices or accounts, the inquiry is fact-specific and the legal standard varies by jurisdiction.

As an initial matter, the contents of users' private communications on social media generally cannot be obtained by subpoena from third-party providers such as Facebook or Twitter because the Stored Communications Act prohibits disclosure. Moreover, there may be limited access to ESI located on employees' personal devices, or those devices may be lost, destroyed or replaced. As soon as litigation is anticipated, counsel should determine both whether relevant ESI may be found in these mediums and the contours of access to this information. For example, an organization's policy regarding the use of personal devices or social media for business purposes is a relevant consideration. However, even organizations with a bring-your-own-device (BYOD) policy that allows employees to use their personal devices to conduct company business may not have access to the data in those devices absent a "legal right" to obtain it. This may be established if employees consent or acknowledge the employer's control over business information on personal devices, company policy states that business communications "remain the sole property" of the employer or potentially if the company pays for the data plan.

Companies that have control over data on personal devices or accounts need to work with their employees to take reasonable steps to preserve ESI that is relevant, unique and proportional to the needs of the case, but employers should not be required to force or pressure employees for information. And even when companies lack control, they nonetheless have an interest in preserving relevant evidence and should inform employees of their duty to preserve as a nonparty who may be subject to subpoena.

How Social Media, Technology and Privacy Laws Are Changing the E-Discovery Landscape

TAR

The document review process also is rapidly changing as both courts and litigants become more familiar with, and accepting of, TAR — courts first began formally approving its use in 2012 — and as that technology continues to evolve. While many litigants still rely on traditional methods such as keyword searches using Boolean logic to identify potentially responsive ESI — which document reviewers then manually review — TAR continues to gain traction, particularly in complex matters with large volumes of data or in matters with especially tight discovery deadlines. The first generation of TAR, also referred to as predictive coding or TAR 1.0, uses a sampling of documents coded by attorneys to train a computer to extrapolate concepts across the remaining documents and predict whether each document in the remaining review population is responsive to the defined criteria.

More recent iterations of TAR, or TAR 2.0, forego the sampling method and instead apply an "active learning" model that uses intelligence gained from an ongoing attorney review to continuously assess the relevance of the remaining review population and reorder it to prioritize the most likely responsive documents. Under this approach, the producing party may choose to discontinue further review at a point when the likelihood of identifying additional responsive documents is statistically low. This new generation of TAR allows parties to more quickly identify the truly key documents in both outgoing and incoming productions while also realizing the benefits of having reviewed all documents ultimately produced. Under either method, the application of TAR can significantly reduce the number of documents requiring manual attorney review.

Courts, too, have recognized the benefits of TAR and increasingly allow — if not encourage — litigants to consider such tools. Beyond cutting costs and increasing efficiency, courts have focused on the defensibility of the results as well as how counsel cooperate in this process. Moreover, courts have cited various studies concluding that TAR results are at least as accurate, if not more, than manual review. Indeed, several jurisdictions — including the U.S. Court of Appeals for the Seventh Circuit, New York, Illinois and Arizona — have adopted rules, pilot programs and model templates that encourage parties to discuss the use of TAR in negotiating discovery plans.

Privacy and Data Protection

Traditionally, U.S. litigation has favored broad civil discovery, permitting litigants a wide berth to explore the factual underpinnings of their cases. As a result, despite recent amendments to the Federal Rules of Civil Procedure that also require discovery to be "proportional to the needs of the case," large volumes of both business and personal data may be swept up in 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.

The European Union's General Data Protection Regulation (GDPR), which became effective on May 25, 2018, is a significant testing ground for how U.S. discovery can be reconciled with data protection requirements. Although not aimed at discovery in U.S. litigation, 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 business operations (such as a branch office or sales representative) located in the European Economic Area (EEA). Given the global economy, this scenario is increasingly common.

The GDPR addresses individuals' "fundamental ... right to the protection of personal data." It covers the personal data of individuals in the EEA (data subjects) and any processing of personal data either by organizations directly (data controllers) or by those acting under written instructions of data controllers. This is the case even if the entity is not located in the EEA but instead merely targets data subjects in certain circumstances. The GDPR defines personal data far more broadly than what typically is understood as personal information in the U.S. This includes identifying details of individuals that may be contained in such mundane places as the signature block of an email, a type of ESI that would be produced in many cases.

The GDPR's requirements govern the processing of personal data, which must be done "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. Processing itself may encompass, at a minimum, collection, review, deletion, production and cross-border transfer of personal data. Additionally, the GDPR calls for heightened transparency and notice requirements, as well as potentially significant administrative fines for violation. As a result, its application to data involved in U.S. litigation is more than mere theory. U.S. practitioners engaging in cross-border discovery and practitioners who may handle data covered by the GDPR would be well-advised to understand the intricacies and practical implications of this comprehensive regulation.

In addition, a number of other jurisdictions also have passed data protection laws that may impact the processing and transfer of covered data, including Brazil, China and Canada. Though the U.S. does not have a federal framework, California became the first state to enact comprehensive data protection legislation in June 2018, and several other states have now proposed or enacted various data and privacy protection laws. (See "Exploring the New California Consumer Privacy Act's Unusual Class Action Cure Provision.") Moreover, privacy bills circulating in Congress are aimed at creating federal standards for online privacy and advocating greater transparency from big-tech companies toward consumers on what data is collected and how it is used. If any of them become law, they could impact the preservation, collection and production of personal information for e-discovery purposes.

Contacts

Lauren E. Aguiar
Partner / New York
212.735.2235
lauren.aguiar@skadden.com

Richard T. Bernardo
Partner / New York
212.735.3453
richard.bernardo@skadden.com

Gretchen M. Wolf
Partner / Chicago
312.407.0956
gretchen.wolf@skadden.com

Giyoung Song
Discovery Counsel / New York
212.735.2564
giyoung.song@skadden.com

Eve-Christie Vermynck
Counsel / London
44.02.0751.9709
eve-christie.vermynck@skadden.com