

Data Blueprinting: FRCP Compliance Depends On It

LEGAL E-DISCOVERY AND THE NEW E-DISCOVERY RULES

Under the recently amended Federal Rules of Civil Procedure (FRCP), the discovery of electronically stored information (ESI) is now a formally mandated part of discovery in all federal civil litigation. Moreover, in an increasing number of states, discovery rules are closely following these new federal rules. The amended FRCP require parties involved in litigation to know, beginning very early in the process, where all potentially relevant information lies and further, they require that parties must work with opposing counsel to prepare a formal discovery plan based on their initial assessment of ESI. Without an existing roadmap or “blueprint” of the ESI environment, however, organizations would be left in the precarious position of having to scramble to prepare for the requisite planning meetings and discovery requests, inevitably sacrificing much needed focus on legal strategy. Organizations without the ability to comply with e-discovery requests are thus more likely to subject themselves to fines, judgments, and other sanctions. In a worst case scenario, as seen in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, e-discovery missteps can directly impact the final disposition of the case and result in a legal defeat for the noncompliant party.

The upside to the FRCP amendments is that they provide some structure, definition, and a clear set of expectations for e-discovery. Although in many respects they may not go quite far enough in advising organizations on precisely how to steer clear of e-discovery pitfalls, the new e-discovery rules seem to reign in the process of legal discovery and provide some guidance on the limits of e-discovery as well as the burdens an organization may be expected to bear in complying with e-discovery requests. One of the biggest changes brought about by the recent amendments is the need for greater structure and transparency in how an organization prepares for – and responds to – an e-discovery matter.

PLANNING TO REDUCE RISK

One of the most critical measures any organization can take to meet the demands of an e-discovery matter and to reduce the risks of non-compliance is to engage in thoughtful, preemptive planning. Even a moderate

level of pre-planning can substantially mitigate e-discovery risk. This type of planning can include policy and procedure development and the implementation of formalized training and education to ensure that every information environment is managed according to stated policies. If a strong system of controls is already in place and is properly managing information, an organization will be very well equipped to quickly and successfully identify, preserve, and produce relevant ESI in manner that is legally defensible.

USING A BLUEPRINT TO MAP AND MANAGE INFORMATION SOURCES

Creating a data roadmap or “blueprint” is really a critical step organizations should take to prepare for the new e-discovery rules. A data blueprint is a continuously updated guide to an organization’s electronically stored information; it is often referred to as a “data map” or “content map” and its purpose is to provide an overview of where electronically stored information (ESI) exists within an organization. The blueprint presents the layout of IT systems that store corporate information, but the document does not focus on the technical IT infrastructure. Instead, it focuses on presenting a comprehensive picture of the content within each IT environment’s information repositories, using simple graphical representations and plain-text descriptions. The blueprint serves as a solid starting point for organizations to track and manage their ESI based on content, rather than size, format or repository.

Plain-English Descriptions of Key ESI Sources

The blueprint includes plain-English descriptors that detail the information contained within each data store. The attendant descriptions are arguably the most valuable pieces of the blueprint because properly constructed, they provide an easy to understand description of the ESI that serves as a centerpiece of corporate e-discovery response planning. They also serve in a key beneficial role for legal and cross-functional e-discovery teams, allowing all parties to be “on the same page” in terms of conceptualizing the organization’s picture of ESI and coordinating an appropriate discovery response.

The descriptions include information about who owns the information, who manages the information from an IT perspective, who uses and creates the information, the format and accessibility of the information (including any financial-reporting or human resources considerations accompanying it), the information’s designated retention period, and other storage flow attributes that may be relevant. The blueprint accounts for structured information sources such as databases, business applications, and traditional records management systems; it also details other information sources such as email, text documents, spreadsheets, web pages, and instant messages or other stored files that reside in unclassified, unstructured locations within the IT environment.

Usable Format for Cross-Discipline Teams

In order to serve its purpose as a roadmap and central planning document for e-discovery compliance and response purposes, the data blueprint must concisely bring together key information in a usable format. To achieve this objective, AdamsGrayson Consulting consultants interface both with IT and legal staff to form an informational “bridge” between disciplines within our client’s organizations. We specialize in extracting the necessary information from each business unit and assimilating the information into a “living” document that provides an easy-to-understand, functional view of an organization’s ESI. Our comprehensive, proprietary blueprinting methodology calls for – and fosters

development of – support from C-level executives, internal records management departments, legal and corporate compliance officers and IT risk management resources. We help identify the primary business operating units, break out the functions within those units, and finally, we detail the information generated from or associated with each of those units. This structured approach all serves to produce the blueprint – an extremely thorough and valuable end product.

Key Benefits – Risk Reduction and Return on Investment

Data blueprints create immediate return-on-investment. They serve to help organizations diminish or altogether avoid incurring substantial legal fees and costs for non-compliance or hasty “invent the wheel” compliance measures after an e-discovery matter arises. The amended FRCP require organizations to have a working knowledge of information systems. Therefore, when organizations take the initiative to create their own data blueprints, not only are they better prepared for any e-discovery matter that may arise, but they also will be saving themselves tens or even hundreds of thousands of dollars by educating legal counsel on their information environment, which will obviate the need to do it under intensive, litigation-based time pressures at huge hourly rates. Furthermore, by truly owning the data blueprint, every organization will be better positioned and informed to oversee the overall corporate response in terms of compliance and legal strategy.

Beyond the cost savings created by a thoughtful, well-planned approach to legal discovery, creating a data blueprint is a demonstration of the organization’s commitment to fulfilling their e-discovery obligations: organizations should think of a data blueprint as the ultimate demonstration of corporate good-faith when it comes to e-discovery compliance. And under today’s new federal e-discovery rules, the showing of good faith and overall good “citizenship” when it comes to e-discovery compliance can go a long way in hedging, diminishing, or altogether eliminating corporate information risks associated with legal discovery.

ABOUT ADAMSGRAYSON

AdamsGrayson Consulting is a corporate risk management and e-discovery consulting firm based in Washington, DC. AdamsGrayson’s Information Risk Management and E-Discovery practice helps organizations undertake a full range of information risk management issues, including data retention and e-discovery response planning. The practice brings together legal experts, risk consultants, and IT professionals to help organizations navigate legal discovery and streamline costs by assisting in the development and implementation of defensible e-discovery business processes.

Visit www.adamsgrayson.com for more information.