Use Email Domains for Filtering and Privilege Review

Email discovery is at the nexus of high volume and low relevance. Businesses generate a tremendous amount of email that has to be sifted to find a relatively small number of useful communications. However, although email discovery is burdensome and expensive, it's also necessary and important. Filtering using email domains is a cost-effective means of culling significant volumes of non-relevant email with minimal human review, reports **QDiscovery**. That reports follows:

What Is the Email Domain?

The email domain is the part of the email address that comes after the @ symbol. For example, in the email address photosubmissions @ wikimedia.org, "photosubmissions" is the local part and "wikimedia.org" is the domain. Sender and recipient email addresses are captured in the metadata fields FROM, TO, CC, and BCC. Thus, there is no added cost associated with using email domains for data filtering.

Culling Non-Relevant Messages

The eDiscovery vendor or litigation support staff managing the document database can export a list of all the unique email domains in the dataset. There are several possible approaches to reviewing the list and marking non-relevant- or alternatively, relevant- email domains.

First, a lawyer or paralegal on the eDiscovery team can look for generally known domains. Project managers and eDiscovery consultants are also a good resource in this regard.

Second, the custodians can be asked to review the list. Since they’re the most familiar with the content of their own mail they can make the most comprehensive review. A second advantage of this strategy is that it imposes no out of pocket costs on the client. However, it obviously does require the custodians’ full cooperation, which may not always be possible or practicable.

Lastly, in dynamic culling the list is marked up on a rolling basis by the document reviewers in the course of making the substantive responsiveness review.

All email addresses that share a certain domain (e.g., amazon.com) can then be batch-tagged as non-relevant and filtered out of the dataset. Occasionally reverse culling may be appropriate; under this approach, email addresses from relevant domains (e.g., the other parties to the case) are batch-tagged to be retained and all other domains are filtered out.

Email domains can easily be used to identify messages in obviously non-relevant categories such as:

– Online shopping and other commercial solicitations;
– Customer loyalty rewards programs;
– Travel-related websites and notifications;
– Professional associations;
– Newsletters, digests, and other mailing list alerts;
– Social media notifications;
– Spam.

In the same spirit, full email addresses can be used to identify and exclude communications with friends and family.

Using Email Domains for Privilege Review

Email domains can likewise be used to identify potentially privileged communications and segregate them for later privilege review. The email domain list is reviewed for outside counsel, consulting experts, eDiscovery vendors, and other litigation consultants. Tagging email domains is a safety net to catch messages from and to email addresses of people whose names didn’t make the search list, such as support staff and others with limited client contact.