TIP JAR

Metadata: Insight from an Industry Expert

July 2017
Number 2

In our technology-driven world, a California Public Records Act request typically seeks some form of electronic communication or record created using a computer and software program. Frequently, an agency's response is to send an email attaching the requested record if it is not otherwise exempt from disclosure. Public agencies must be careful when responding to these requests. Without taking adequate precautions, this common response may actually reveal hidden electronic data, called "metadata." In some instances, a requester of records may specifically ask for metadata. If a request for metadata involves an employee's personal account or device, this could implicate an employee's privacy rights. Best practices may warrant that the public agency take an active role in searching for the information or guiding the employee to search his or her personal electronic device or account.

In *City of San Jose v. Superior Court*, the California Supreme Court looked in part to the Washington Supreme Court for guidance on how a public agency could establish the adequacy of a search for public records on an employee's personal device or account. The Court offered as an example the Washington Supreme Court's approach, which relies on employee affidavits to verify that the employee searched his or her personal devices and accounts and to explain why any records were not produced. The California Supreme Court held that this struck an appropriate balance between a public agency's "responsibility to search for and disclose public records without unnecessarily treading on the constitutional rights of its employees."

While not yet addressed by California law or mentioned in *City of San Jose*, Washington is also one of the few states in the nation with case law establishing that metadata is a disclosable public record. In *O'Neill v. City of Shoreline* (2010) 240 P.3d 1149, the Washington Supreme Court found that metadata associated with an email was subject to disclosure after a public records act request was made in order to determine its original sender. In that case, the city's failure to respond to the court's satisfaction proved costly. After deciding against the city, the Court ordered the city to pay over $500,000 in fees to the plaintiff.

As California law continues to evolve, it is foreseeable that the Public Records Act may be interpreted to include metadata associated with personal electronic devices or accounts used by officers and employees of public agencies. Consequently, it is in the best interest of public agencies to better understand what metadata is, how to control the creation and maintenance of metadata and how to respond to requests for it.

To explain metadata within the context of an employee or employer search of personal electronic devices or accounts, we consulted Digital Mountain, a leading global provider of electronic discovery, computer forensics, cyber security and next-generation Web-based solutions. In response to our questions, Digital Mountain's founder and CEO, Julie Lewis, provided the following information.

Darren C. Kameya
Partner
Los Angeles Office
dkameya@lozanosmith.com

Penelope R. Glover
Senior Counsel and Chair
Technology & Innovation Practice Group
Walnut Creek Office
pglover@lozanosmith.com

Julie Lewis
Founder and CEO of Digital Mountain, a leading global provider of electronic discovery, computer forensics, cyber security and next-generation Web-based solutions.

Lozano Smith
ATTORNEYS AT LAW

TIP JAR

July 2017
Number 2

Q: What is metadata and what types of information does it provide?

A: Metadata is simply data about data. For email, metadata may be information such as sender, mail size, subject, sent date, sent time, received date, received time, to, cc, bcc, message ID, mail internet headers, sensitivity and importance. For files at a file system level, metadata may be such information as original file name, modified date, accessed date, created date, file size, file extension and original file path. Additional metadata may exist based on the specific application and version of the software used. For example, for Microsoft Word, there may be metadata for comments, date created, primary author, last saved by, revision number, source, last saved date, last print date, pages, words, characters (without spaces), characters (with spaces), lines, paragraphs, total editing minutes and company. If you are dealing with picture files, there is something called exchangeable image file format (EXIF) metadata which has the source camera make and model, date, time, geolocation if recorded and a lot of metadata that may be noise (irrelevant data). As you can see, with any request for metadata it's important that metadata being sought is properly defined or there can be a lot of extraneous information.

Q: Where is metadata found?

A: This is a bit of a loaded question. If metadata is embedded within a file, it can be extracted with processing. However, if you are seeking metadata at a file system level, metadata is extracted differently based on the operating system. For example, if you are seeking a creation date within a file, that would tell you when a document was created versus if you obtain the creation date at a file system level, the creation date is typically when the file was first placed on a hard drive.

For email, metadata is embedded within the email message. For security logs in the cyber security realm, the data is typically in a database. For a wearable device (like a Fitbit or smart watch), it could be on the device or stored centrally in a database in the cloud.

If you compare metadata to a human being, there may be data stored about you externally (e.g., Social Security number, birth date, home address). There may also be metadata that is part of your system that consists of blood type, DNA, blood pressure or cholesterol level. Documents follow a very similar pattern, where there may be metadata stored externally and embedded. Rather than getting caught up with the word "metadata," it's important to preserve what you can and ensure that the requesting party defines what they are seeking when metadata is requested, as each system can vary in what metadata is maintained.

Q: Does an employer or employee need to take any steps to preserve metadata?

A: For discovery purposes in litigation, it's critical that metadata is preserved based on how documents are held in the ordinary course of business. This involves forensic preservation that ensures no data is altered along with proper chain of custody procedures and processing documentation. Many employers and employees are tempted to cut corners and do such things as forward relevant emails to their attorneys. However, this does not properly preserve the email for evidentiary purposes.

Q: If a public agency is legally obligated to produce metadata that is located in an employee's personal electronic device or account, how would it go about doing so?

A: It depends. At Digital Mountain, we have a separate form that custodians sign providing authorization to collect their digital evidence. For metadata extraction, what information is processed depends on the type of device that is subject to discovery. For desktops or laptops, a forensic preservation would need to take place, so metadata is not altered. In the processing phase, relevant metadata is extracted so it can be displayed alongside the actual document view. For devices such as smartphones, the device is forensically preserved, reports are typically parsed

out from SQLite databases and then filtering is performed for relevant information. For cloud-based accounts, we obtain the user's authorization to access personal accounts prior to preserving. Metadata varies across different cloud-based applications. It's important to know what metadata is relevant and what's considered noise. Bring your own device policies have created a lot of complexity in our industry. It's always best to have written policies upfront that address how business documents or communication on personal devices or cloud accounts may be treated for investigations, Public Record Act requests, litigation or other purposes.