

PRACTICE TIPS

Requests for Electronic Information: The Top Ten Pitfalls

By Hilary Ruley, Chief Solicitor, Baltimore City

I know all too well that different states have different public information laws because I reviewed *all* of them in preparing to speak on the panel titled "Electronic Impact on Open Government" at IMLA's 2013 Annual Conference in San Francisco. I addressed the types of electronic documents, highlighting the multitude of software programs and hardware devices in use and the metadata they create. I concluded that trying to create a standard national policy to address the problems posed by requests for electronic information misses the opportunity for each municipal government to balance the desire for transparency with its available resources. A uniform approach also naively ignores the comparatively nimble legislative and regulatory process at the local government level, which allows for relatively quick solutions tailored to each government's needs.

Yet, what do municipal attorneys do with the existing requests for documents, particularly electronic documents, which clog their in-boxes and pile up in office mail? Although each local government is unique in how it wants to handle the volume and type of requests it receives, there are many similarities in requests for electronic information, no matter the jurisdiction. While there may not be a universal roadmap we all can follow when answering a request for electronic documents, experience reveals common problems we should try to prevent.

Here are the top ten pitfalls municipal attorneys should avoid when counseling a client about a request for electronic information:

10. Not understanding metadata. Metadata is the usually hidden information associated with what you see on your computer screen or mobile device. If I have lost you already, think about a spreadsheet. The government data is what your client types into the cells in the spreadsheet. The numbers for the rows and the letters for the columns are information created by the software program and visible on the screen. Metadata is the information tied to the spreadsheet that you cannot see automatically on the screen: author, file creation date, last edited and last saved dates.

9. Not redacting (or, if you are in some jurisdictions, reviewing) metadata. In most jurisdictions, public information laws are silent on how to treat metadata captured by a request for information. Consider redacting the metadata if it is financially and technologically feasible by purchasing a software program that erases the metadata from the electronic document. If this is too cumbersome, and your jurisdiction allows, release the information in a PDF or TIFF file or as a hard-copy document. If you are in a jurisdiction (*e.g.*, Arizona, Washington, Maryland, Montana, Connecticut, New York) where metadata has been addressed in statutes or by the courts, review the metadata in your documents to decide if you want to redact some of it.

8. Not understanding your jurisdiction's laws about information concerning public business contained on private devices. There is no national consensus on when e-mails (or other electronic information) concerning government business contained on private devices must be produced in response to a request for documents. In a recent Illinois case, the appellate court ruled that if a councilmember was sending or receiving a message about public business from a personal device while engaged in a council meeting with a quorum present, then the message was subject to the records law. *See City of Champaign v. Madigan*, 992 N.E. 2d 629 (Ill. App. Ct. 2013). If you are practicing outside of Illinois, does a similar rule apply to your clients? If so, you need to advise your clients to allow their personal devices to be searched for relevant electronic information. In any case, counsel your clients to keep separate work, campaign and personal e-mail/Facebook accounts. This makes the process of searching for responsive information easier regardless of the applicable law. It also prevents personal information from being captured when work devices or work e-mail accounts are searched.

7. Not discussing who owns proprietary information in software. Make clear in each contract to purchase or license software (or hardware that runs with unique software) which party owns the information keyed or uploaded into the software. Many contracts will be clear that the vendor owns the software code because it is proprietary and commercially valuable. But the contracts also need to address what happens to the information placed in the software system by the government or the vendor. You do not want your client to be unable to provide information it created because it cannot run a particular report or otherwise extract that information from the software it purchased. In a Connecticut case, a court held that it was illegal to purchase a software program that did not allow the government to make its information available to a requestor as readily as it had done prior to the purchase. *See Office of Health Care Access v. Freedom of Info. Comm.*, 2005 Conn. Super. LEXIS 962, *4 (Conn. Super. Ct. 2005)(unreported). The court required the government to pay to have the software reprogrammed so that the information sought was easily retrieved.

Continued on page 38

Practice Tips *Cont'd from page 21*

Id. at *30.

6. Not discussing document retention. Many states have laws that require the government to keep certain documents forever or for a certain period of time. Now that governments use many software programs and sometimes store data in a cloud or on a server, it is imperative that the client think about retaining that information. Even if there is no state law on retention of e-mails, text messages or drafts of word processing documents, the municipal government should consider a policy to address the retention of this information. Many state courts have looked unfavorably upon governments that have been unable to produce a record in response to a request for information because the information originally stored electronically has not been retained. As a rule of thumb, consider keeping electronic information at least as long as you would keep similar paper information.

5. Not asking the requestor to narrow the scope of the request. In most states there is a mechanism for narrowing the scope of broad requests, either under the law itself or in practice. This can be done for electronic requests by asking the requestor to narrow the timeframe for documents sought, or the number of senders or recipients. A key-word search can be used to pull only responsive documents or e-mails.

4. Searching only e-mails. If your request seeks all "electronic documents" remember that most states have very broad definitions of a "public record." Those broad definitions likely encompass more than just e-mail. There are texts, pins, IMs, tweets, Facebook pages, etc. Do not forget word processing files, spreadsheets and electronic calendars. Tell your client to search all of these when there is a request for electronic documents.

3. Not searching everyone's documents. While we may all sit in front of a computer doing our own typing, having long since abandoned paralegals and perhaps even secretaries and receptionists, our clients likely still work in hierarchical offices. Remember this when you receive a request asking for all documents from a municipal agency. The complete universe of information may not be solely in the files of those *you* regularly contact. The secretaries, subordinates, and manual laborers who fill out the client's workforce may all have documents relevant to a request.

2. Not encouraging your municipality to manage its public relations. Less information is requested by citizens and the press if abundant information is already available on-line. Consider counseling your client about a website where forms, documents, and schedules of government hearings and meetings are readily available. In a controversial situation, encourage your client to make the media its friend and release all the relevant documents that legally can be released and take that opportunity to shape the story. Give the documents context and highlight when there has been careful deliberation about the choices made. Silence breeds distrust and overuse of public information requests.

And the number one pitfall to avoid . . .

1. Not understanding your client's IT structure. Do not be ignorant about how your client creates and stores its electronic information. Each government, and perhaps even each agency within your government, has its own e-mail server and may store documents on the internet or a shared drive. The most important thing to know is whether there is a central agency that has access to all of your client's e-mails or electronic files. Not only will this educate you about where your client's documents are located, but it may matter if your state requires a request to be addressed to the custodian of the documents sought. Is the custodian of the records sought the agency or the government's central information technology office?

Rule 1.1 of the American Bar Association's Model Rules of Professional Conduct mandates, in Comment 8, that a lawyer "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Avoiding these pitfalls is a good first step. ML

Code Enforcement *Cont'd from page 15*

have some good debate on whether to enforce or not to enforce is the regulation prohibiting the keeping of farm animals within City limits. With more and more communities seeing an increase in the desire for backyard chickens, goats and similar type of animals, more citizens may advocate for not enforcing this restriction. At the same time, citizens will still voice concern over noise, smell and other impacts they may have on neighbors and the surrounding neighborhood.

One of my most memorable cases involved animal regulation. When I first began working for my municipality, I prosecuted violations in circuit court. My cases were set for one afternoon a week. Each of those afternoons, I would bring my binder to court. My binder usually consisted of approximately 120-150 cases, several of which were scheduled for trial. I would always prepare for the trials. But, most often, I would not look at the cases set for initial appearance ahead of time. One afternoon, as the judge and I worked our way through the cases, he opened a file and I turned in my binder to the next case. As I saw the charge, I looked at the judge. He was looking back at me with an expression that said all that needed to be said. I quickly dismissed the case and moved on. The charge was for "cat running-at-large." Needless to say, that was one animal regulation that fell by the wayside a long time ago. ML

Amicus Corner *Cont'd from page 37*

precursor to its more familiar statutory second cousin–RLUIPA, the Religious Land Use and Institutionalized Persons Act. RFRA had been enacted by Congress to confirm religious protections; when the Supreme Court ruled that RFRA could not apply to the states due to 11th Amendment constraints, Congress passed RLUIPA to ensure that state and local activity was also covered. To anyone involved in municipal land use and zoning, the protections afforded religious organizations under RLUIPA are very consequential. It bars state and local governments from enforcing land use regulations that impose a "substantial burden" on "the religious exercise of a person" unless