Access to Government Data:
Examining and Overcoming Barriers

Matt Ehling, Public Record Media

Good afternoon and thank you for the invitation to be here. My purposes here today are threefold: to give you some background on how to access public records; to provide information on how to overcome challenges to that access; and (frankly) to prosthelytize a bit about the value of these records to your research endeavors.

Four years ago, I started an organization called Public Record Media that focuses on obtaining public records in the service of two separate objectives. The first of those objectives is to obtain and publish government documents as a public affairs resource. The second objective is to deeply engage in the record-seeking process, in order become a mechanism to encourage compliance with public records laws. We engage in litigation work as necessary, and seek to create case law that is conducive to transparency, in order to help keep public record laws viable.

As such, I am here today as an advocate for public data access, with the intention of offering tools to help support your individual enterprises. Public records laws cross-pollinate with many areas of study, and provide useful avenues for obtaining raw data for a variety of analytical purposes.

Background

First, some background about public records laws themselves. At base,

public records laws provide access to government data - not only data created and compiled by government entities, but also the vast repository of data created by private enterprises that the government maintains for its various regulatory functions.

Historically, public records laws are rooted squarely in the realm of government accountability. Prior to the mid-1960s, there were few mechanisms (save for legal action) that could provide the public with access to internal government records. In 1966, the Freedom of Information Act (the FOIA) was passed at a federal level. That law provided statutory requirements that governed access to government data, and gave the public a much easier-to-use tool to obtain government records.

The FOIA was mimicked by numerous state-level laws - many of which were fueled by political reactions to the scandals of the Watergate era. The general impetus behind the adoptions of these laws was the idea that the public itself needed to be a part of the governmental oversight process.

Common to most of these Freedom of Information (or FOI) laws is the presumption that all government data is public, unless specifically exempt from release by law. Each FOI law also contains certain exemptions that have been written in to protect specific types of data. Some of those exemptions are broadly drawn - like those in the federal FOIA. Other exemptions - like those in the Minnesota Government Data Practices Act - are much more specific, and involve a finer level of detail.

Who uses public records?

Certainly, the public utilizes these records for a variety of purposes, as does the press. Academic researchers also rate high among users. A lesser-known user base is represented by elected officials, who rely on these laws to obtain records for oversight purposes, the same way that users outside of the government do.

A large number of FOI requesters – particularly at the federal level - are commercial requesters. Even with the trade secret exemptions that are written into many FOI laws, commercial requesters are constantly filing requests, trying to divine information for their own business purposes, and in many cases are attempting to see what their competitors are up to. This activity has related implications that we'll discus later.

How to use public records laws

The basic process for using public records laws is fairly simple. It is the back-end work that is often more complicated, and has become more challenging over time.

The beginning of the process starts with writing a letter or drafting an e-mail to the agency you're seeking data from. It is important to note that most FOI laws were drafted to provide access to existing government documents, rather than to force agencies to provide answers to specific queries. Requests should describe the kinds of records you are seeking, or else the data that those records would tend to include.

Depending on the structure of the FOI law that you are using, there are

greater or lesser degrees of specificity that you need to be aware of. In Wisconsin, for instance, Attorney General guidelines provide a fair amount of leeway for agencies to accept and process improperly labeled requests. For instance, requests submitted to state agencies that seek data under the federal FOIA law are treated instead as if they were submitted under the Wisconsin Open Records law. Other states are more rigorous about where to send requests, as well as the requirements for properly addressing those requests.

As a practical matter, one should include a reasonable degree of specificity in the initial request itself. This is helpful for a variety of reasons, but in some states there is case law that directly addresses this point, and constrains the actions of requesters. Wisconsin has case law that essentially states that "overly broad" records requests can be rejected outright if a requester does not work to narrow the scope of the data that is sought.

As I've mentioned, follow-up is the most important - and sometimes most troublesome - piece of the record request process. You should be aware of the statutory requirements for agencies to respond to you, and evaluate your opportunities once the statutory time frame has passed. Under the federal FOIA, that timeline is 20 working days, followed by a 10-day extension period if the agency notifies you of some unexpected delay. In reality, very few federal agencies routinely adhere to this timeline, leading to other considerations that we will discuss.

One should also understand that copy fees are frequently a reality of the request process, as they can impact your ability to obtain large data sets.

Some laws like the federal FOIA have fee waiver provisions that certain users - such as members of the press - can attempt to avail themselves of. Some state laws do not feature such provisions. Understanding this at the beginning of the process can help to shape the scale of the requests that you ultimately file.

Compliance

Understanding strategies for compliance is a large part of understanding how to effectively use public record laws today. Not every FOI request will produce records within the time mandated by law. And not every document that is produced will contain all the information that is requested - and legally sanctioned - for release.

In regard to timeframe, FOI laws often provide several mechanisms that can be used to encourage agency compliance after the statutory timeframe for a response has elapsed.

In regard to redactions or the withholding of records, the compliance picture is much more complicated. To a certain degree, this complexity is understandable, given the breadth of material governed by FOI laws, and the need to make individualized determinations about the application of legal exemptions to that body of material. However, the application of record exemptions can also provide avenues for abuse, as the process can be used to hide public information, or to delay its release through costly legal fights.

It is also important to understand that there are many legally permissible exemptions to public record laws, and withholding actions need to be

reviewed within that context. One must first be able to discern legitimate grounds for withholding from those that are impermissible, and then evaluate the situation for the appropriate follow-up strategies.

The compliance "tool kit"

Strategies to address compliance issues involve this basic set of tools:

1. Request follow-up (or request "care taking"). This involves regular follow-up with agency personnel, and is best suited to pursuing incomplete requests;

2. Administrative remedies. These remedies can be used to address both failures to respond, as well as redactions. Both the FOIA and many state laws allow you to prompt an agency to review its own decisions. Other times, an outside entity will handle this kind of work;

3. Litigation. Court review is "baked" into most FOI statutes as the final compliance tool. If an agency is not compliant, you can go to a judge to obtain an order to force that compliance.

I will discuss all of these options in more detail. Before that, let me provide more background about why compliance has become a bigger issue for public records laws in recent years.

Problems with compliance

As we'll discuss, problems with compliance have been on the rise for some time. From my perspective, the main drivers of this trend can be largely

grouped into the following categories:

1. Functional limitations;

2. The growth of security claims;

3. Resistance from commercial entities;

4. Active agency resistance.

Functional limitations

At the "base" of the hierarchy of compliance problems is a nest of functional issues that stems from the fact that more government data exists today than ever before. Record requests have also on the rise, and in some cases there has not been a commensurate increase in the resources needed to address the increase in volume. Thus, within some agencies, workload and resource issues have created functional bottlenecks. We can look at recent federal statistics for an illustration.

According to the U.S. Justice Department - which tabulates FOIA statistics across the federal government - "federal agencies processed more than 631,000 FOIA requests in fiscal 2011 - 5 percent more than the year before. However, the number of backlogged requests shot up from less than 70,000 to more than 83,000."

The DOJ attributes this backlog to what it calls "a significant increase in the number of FOIA requests sent to agencies in 2011" - an 8 percent increase

for that year. During that same year, the federal government dedicated "9 percent more full-time staff to FOIA processing and spent almost $20 million more on FOIA-related activities", but backlogged requests "nonetheless grew by 20 percent." As these recent statistics indicate, the overall processing of FOIA requests does appear to be on the rise, but it remains to be seen if it will catch up with agency backlogs.

State experiences vary widely, of course. I'll speak to Minnesota's briefly. Minnesota law clearly states that government data must be arranged and maintained in such a way so as to facilitate easy public access. While this statutory requirement is something that should be taken into consideration as databases and information systems are developed, it has not always been the case. The result is that data at some agencies – particularly within municipalities - is compartmentalized and scattered, and requests are delayed.

How do these functional issues play out in reality? Let's look at an example:

Public Record Media requested radiation-monitoring data from the state of Minnesota on two separate occasions over the last three years. The Department of Health is responsible for radiation monitoring within the state, and has conducted environmental monitoring of radiation levels since the 1950s. In 2011, we asked for any radiation monitoring reports that might be pertinent to a 2009 tritium leak at one of Minnesota's nuclear power plants. The state responded with those documents, and also sent additional monitoring reports extending back to 2004.

We received that data very quickly, largely due to the fact that the pertinent data had already been compiled into reports that the department produced as part of its regular work output. Thus, it was easy for the agency to find and release it.

We've subsequently gone back to the Department of Health, and have asked for all of the pre-2004 monitoring data. That request has taken much longer for the state to fulfill. First, we learned that pre-2004 data was not routinely compiled into final reports, and that staff would have to go back through old filing systems to find the underlying data. Such work must be undertaken by the small number of people within the department who are familiar with the data, and they - of course - are pursuing their other duties at the same time. So that already provides for a certain amount of delay.

Then, other events have intervened. In January we had an extreme cold snap in Minnesota, and the pipes in some of the department's public health labs burst, complicating work throughout the building. So now it has been five months since the initial request was filed, and the Department has not yet produced documents.

From a follow-up standpoint, we have checked-in on this request on a regular basis, but there is only so much that we are able to do. Because of our understanding of what the department is going through, we realize that the administrative remedies that we could avail ourselves of are not going to be particularly helpful.

In a case like this one, you could certainly sue the agency and get a court

order to produce the records you are seeking. While that would put your work at the top of the list, we don't feel that the litigation tool is best utilized in situations like these. To the extent that you can, you want to have good relations with agency data management personnel since – conceivably - you'll be going back to them with more requests in the future. That said, there are other instances where litigation is the preferred tool. We'll talk more about that shortly.

Security claims

The phenomenon of agencies raising security claims to deny access to data is another trend that has impacted FOI compliance in recent years.

At the federal level, this started occurring almost immediately after 9/11. In October of 2001, the Ashcroft Justice Department issued a directive to federal agencies in regard to their compliance with the FOIA. The Attorney General's position was essentially this: if an agency had a colorable basis for denying a request due to security-related (or other) concerns, then the agency was encouraged to avail itself of that option, with the assurance that the Justice Department would fully defend its decision. This was a reversal of previous DOJ guidance on FOIA response, which urged agencies to default on the side of disclosure, if at all possible.

The Ashcroft memo was read within federal agencies as a clear mandate to proceed cautiously with FOIA responses, and it impacted the release of public information for almost a decade after 9/11. A 2009 analysis of Bush-era FOIA requests by the Sunshine in Government Initiative found that while the federal government fully granted roughly 56% of the requests it

received in 1998, it only fully granted about 28% of its requests a decade later.

In 2009, the Ashcroft memo was effectively reversed by a presidential directive signed by President Obama on the day that he took office. At the time, there was much made of this action in the transparency community and the press. But functionally, has the directive had its desired impact? The record is mixed.

As noted previously, recent DOJ statistics have cited an increase in total FOIA responses during the Obama administration, even though the percentage of backlogged FOIA requests has increased. At the same time, the use of exemptions – including security exemptions – appears to be on the rise. According to federal statistics available at foia.gov, 2012 DOJ exemptions totaled over 30,000, as compared to roughly 20,000 in 2008. Within those totals, security and law enforcement-related exemptions were invoked over 14,000 times in 2012, as opposed to 10,000 times in 2008.

Independent studies show similar results. The Center for Responsibility and Ethics in Washington recently produced a study that noted that the use of FOIA exemptions had risen 33 percent over the course of the Obama administration. Likewise, an Associated Press investigation noted that FOIA exemptions were up 22 percent in 2012 compared to the prior year. The AP specifically noted that the CIA invoked national security exemptions 49 percent more frequently than the year before.

It should be recalled here that exemptions are legally allowable reasons to

withhold data from release under the FOIA – but only to the extent that an exemption is based upon a set of facts (or another legal authority) that actually supports the exemption. There are some statutory reasons for the increase in security-related withholding under FOIA. For instance, the passage of the Critical Infrastructure Information Act of 2002 allowed private sector infrastructure data submitted to the Department of Homeland Security to be withheld under FOIA Exemption 3. I would – incidentally - argue that there is a reasonable policy basis for such withholding. However, security claims have also been used to withhold data without a statutory basis, causing rising compliance problems.

SBU information

We have seen such compliance issues arise, for instance, from the tangle of internal security designations that federal agencies have instituted in recent years. Since 9/11, agencies have expanded the use of what is called "sensitive but unclassified" - or SBU – information.

As previously described, the executive branch classifies certain data as "national security information" that is then explicitly exempt from FOIA by statute. However, the growing category of "SBU" data is not classified by executive order, and does not necessarily create a basis to trigger one of the other statutory FOIA exemptions. This internal labeling process has caused a number of problems with FOIA compliance.

For instance, the National Security Archive did a 2006 study of multiple federal agencies to learn how they were using SBU classifications, and to discover how those classifications were impacting FOIA compliance. Their

findings indicated that many agencies lacked specific guidelines about how internally-marked "SBU" data was to be treated in the face of FOIA requests. They also found that multiple agencies were denying requests on the basis of an SBU classification alone, even though SBU designation did not constitute an allowable basis for withholding under the FOIA.

When security exemptions are mis-applied in this way, a requester is in a significantly different position from one who is simply trying to deal with agency over-work. Contesting exemptions almost always involves extensive legal research, and seeking recourse through administrative or court remedies.

Commercial data

Another area where there has been push-back against compliance with public records laws has been in the arena of commercial data held by the government. This has occurred at both federal and state levels, and the trend has produced both victories and losses for public records access.

In the "win" category, we find the “FCC v. AT&T” case of 2011. In that case, AT&T made a novel argument to try to protect from disclosure some of its data held by the Federal Communications Commission. The issue ultimately reached the U.S. Supreme Court.

For background, corporate records maintained by the federal government have routinely been made available under FOIA so long as they can't be protected by another exemption, such as the trade secret exemption.

In this case, the FCC had investigated AT&T for the over-billing of a federal program, and obtained corporate records related to its enforcement action. Subsequent to this, Comp-Tel - a trade group representing several of AT&Ts competitors - filed a FOIA request to obtain those FCC records. AT&T challenged the disclosure, and claimed that one of the FOIA's statutory exemptions – Exemption 7(c) - applied to the documents in question, and thus prohibited their release. "7(c)" is a law enforcement records exemption, and documents can be withheld under that exemption if they can "reasonably be expected to constitute an unwarranted invasion of personal privacy."

AT&T asserted that 7(c)'s "personal privacy" protection extended to corporations as well as individuals, and they sought to block release on those grounds. The result of a successful court challenge would have been to close a vast body of regulatory and enforcement records that had long been public, due to precedent interpreting Exemption 7(c) as covering individuals only. Ultimately, the Supreme Court sided with the FCC, and disallowed the use of 7(c) as an exemption that could apply to corporate records.

Elsewhere, public access to business data held by the government was recently restricted in Minnesota as the result of a state Supreme Court decision. This decision involved access to the records of private companies that had been contracted to perform government functions. The background here was that the Timberjay newspaper had been investigating potential cost over-runs in the construction of area schools that were being built by private companies under contract with the school district. The project's general contractor was Johnson Controls of Milwaukee, Wisconsin, and it was using a variety of sub-contractors to help complete the job. The Timberjay sought

out Johnson's subcontracts - initially from the school district itself – under Minnesota's data practices law. The district said that it did not have the records, and so the Timberjay requested them from Johnson Controls. In such a circumstance, Minnesota law allows you to request data directly from a private entity under public contract, and the Timberjay made such a request. Johnson Controls then denied access to the data.

The Timberjay pursued the records through various levels of administrative and court review, until the issue arrived at the Minnesota Court of Appeals. That court found for the Timberjay, and ordered the data to be disclosed. Afterwards, the Minnesota Supreme Court took up the case, and sided with Johnson Controls, changing what had been long-standing assumptions about access to contractor data. The Court sided with Johnson on a fairly narrow basis, however, and said that private contractors performing government functions were only obligated to disclose data if their contracts contained an express "notice" provision. Without the notice provision, there was no disclosure obligation.

Because of the court's ruling, the Minnesota legislature is poised to re-visit the issue this year. However, dicta in the Court's opinion has also opened another front in this matter, which will likely focus on narrowing the definition of what sort of government-contracted work constitutes a "government function," and is thus available to the public.

Active resistance

Active agency resistance is a category that deserves its own discussion. This kind of resistance involves actions that do not stem from agency over-work,

but rather from a desire to prevent the release of data despite the legal obligation to do so. This can flow from a variety of factors, including agency culture and various political pressures.

A concrete example of this was highlighted in the press recently, when a Washington DC-based television reporter received documents from a FOIA request related to last year's shooting at the Washington Navy Yard. Notably, part of the documentation that he received included internal agency correspondence about how to slow down and impede his own request.

Such "active resistance" does occur, and responding to it most often requires the use of administrative or litigation remedies. Let's look at some examples:

DHS "political vetting"

One situation that we were peripherally involved in related to the Department of Homeland Security, and its practice of subjecting FOIA requests to "political vetting." This was an issue first uncovered by the Associated Press in late 2010. In this DHS "vetting" procedure, political appointees inserted themselves into the FOIA response process to run political interference as FOIA requests were coming through. They examined the content of FOIA requests, and tracked who was making them by organization and party affiliation before approving release. This additional scrutiny – termed "Front Office Review" - resulted in significant delays in agency FOIA response.

DHS e-mails obtained by the Associated Press indicate that career FOIA

staff were frustrated by this approach. Chief Privacy Officer Mary Ellen Callahan e-mailed her boss to note that the level of scrutiny was "crazy," and that "someone should FOIA this whole damn process."

When this practice came to light, we submitted a request to DHS to see if one of our own FOIA requests had been caught up in the process. In 2010, we had sought internal Coast Guard records related to the Deepwater Horizon oil spill. We had not heard anything back from the Coast Guard for several months, and so we sent a FOIA request to DHS (the Coast Guard's parent agency) to see if they had intervened in our 2010 request.

We received six documents back from DHS, including one page of e-mail correspondence in which two e-mail routing names had been redacted under Exemption 6, allegedly for reasons of "personal privacy." Although the e-mail noted that no responsive documents had been found by DHS, it also stated that our request had been flagged for "front office review." Given the subject of our inquiry and the "front office" notation in the message, the identities of the personnel who sent and reviewed that e-mail were particularly pertinent.

We believed that DHS lacked a legal basis to withhold the e-mail routing information, and so we filed an administrative appeal to contest the redaction. We prevailed in that appeal, and an administrative law judge remanded our request back to DHS for reconsideration. However, DHS has not subsequently responded to us about revisiting the redactions, even after follow-up correspondence. At present, we are evaluating our options to obtain that information.

PRM v. DOJ

Perhaps the most interesting request that we've been involved with is one where we ended up suing the Department of Justice in relation to drone records. In that case, we sought to obtain DOJ Office of Legal Counsel opinions on the subject of killing US citizens with drones. Our request was in three categories. The first was in regard to legal opinions related to the killing of Anwar al-Awlaki - an American citizen who was an al-Qeada member killed by a targeted drone strike in Yemen. We were curious to see what those memos looked like to establish how broadly drawn the memos might be, and how they might apply to other US citizens.

The second was for any other legal opinions related to the killing of US citizens outside the US with drones. The third was for any memos about the killing of any person inside the US with drones.

Our assumption had been that because of the use of drones by - for example - the border patrol, someone may have drawn up legal opinions about the potential to use lethal force through same. We were curious to see if such things existed.

DOJ's response to our request was interesting. Regarding Category 1 - the al-Awlaki memos - OLC said:

"We can neither confirm nor deny that we have memos responsive to Item 1." This is a commonly-used and court-recognized response called the "Glomar" response, invoked by agencies asserting a "national security"

exemption under FOIA Exemption 1. Essentially what it means is, by the very nature of revealing whether documents exist, national security is compromised. There are mechanisms for *in camera* review of such claims, but that is a subject for another day.

Regarding Categories 2 and 3, DOJ had this to say: "We have documents responsive to the remaining items in your request, but we are denying them on the basis of FOIA Exemptions 1, 3, and 5."

In other words, DOJ appeared to be indicating that it possessed legal memoranda relating to the use of lethal force by drones. We believe that legal opinions - particularly final legal opinions, which the FOIA specifically states have to be disclosed - are important public documents, because they form the basis for government actions. They should be available for public inspection, since they give insights into how the government construes its powers, and acts accordingly.

Given this response, we filed an administrative appeal with DOJ, narrowing our request, and contesting the withholding of, specifically, the "Category 3" opinions – ie., the use of force by drones within our borders.

Again, the Administrative Appeal is an internal process whereby the parties have an opportunity to revisit or clarify the agency's response outside of formal litigation.

More than four months passed with no DOJ response to our appeal. At four months, the statutory response time for an administrative appeal had well

since passed. I then called DOJ, and was told that the appeal had been lost internally. This had occurred despite the fact that I had a courier obtain a signature from a DOJ mailroom worker upon delivery of our appeal, and despite the fact that I had called DOJ to confirm receipt of the appeal four months earlier. I was then told that DOJ would print out the appeal from our web site, and submit it to the appeals staff. We then waited, and several weeks passed once again without any decision from DOJ.

With our administrative remedies "exhausted" under the statute, PRM undertook the decision to file suit in US District Court, seeking to produce the "Category 3" records for public review. We believed that we had a solid legal basis to obtain those records, and that they should be public.

We filed suit in May 2012. We served our complaint, the government filed its answer, and then things got a little curious. Two months into this process, our attorney received a phone call from DOJ, and then a letter, that essentially reversed DOJ's earlier position about the existence of the records. The government's new position was: when they said they had responsive items to Categories 2 and 3, they really meant only Category 2, and that the earlier reference to "items" just meant Item 2 "broadly construed." And since our appeal (to which they never responded) and lawsuit was for Category 3, the issue was now moot.

Our first reaction was, of course, surprise. Our second reaction was to ask why - if that was their position - they didn't say so in the many months that had elapsed before we filed suit.

Other than the novel grammar of DOJ's letters, we were not in possession of any evidence to contradict their new claim. Our preparation to that point had been to litigate FOIA exemptions, not to challenge a “no records” declaration or the propriety of a records search.

Given this fact, our position - which we expressed to DOJ - was this: For purposes of this lawsuit, we will take you at your word and settle on two conditions: 1) You further explain yourselves, and 2) You reimburse us for the costs we’ve incurred as a result of your delays and obtuse statements.

To fast forward a bit in the interest of time, the court’s resolution of the case ultimately produced exactly the result we proposed in August of 2012, i.e, a sworn declaration about DOJ's statements, and the receipt of a good portion of our fees and costs. It just took nearly another year of litigation, and 10 or so collective filings between the parties, to do it.

First, we obtained from DOJ a sworn declaration outlining their search process. In the declaration, they stated that they searched twice but were not able to find anything responsive. Importantly, the declaration stated that they knew they had no "Category 3" records at the time of their initial letter, in which they said that they held “records responsive to the remaining items in our request.” Based on this declaration, the parties jointly dismissed the underlying suit, PRM moved for fees, and we were eventually awarded those fees.

While we prevailed, there are several important takeaways. First, and perhaps most importantly, this set of circumstances should not have occurred

in the first place. Agencies need to be accurate with their representations to the public, and not use the FOIA process as a vehicle for oblique statements and actions. Second, transparency has to be the goal in a case like this. We believe that our successful litigation delivers an important reminder to agencies that they need to be forthright with their FOIA responses to requesters. This, of course, is why we do this work.

Dealing with compliance

Returning to the issue of compliance, let's review what your compliance options entail:

1. First, you can "care-take" your request, checking with agencies and staying on top of the response time. Again, in many cases of agency non-response, this can be an effective strategy.

2. Secondly, you have administrative remedies available, in which you can appeal higher up within the agency, or sometimes to an outside party. One very useful service that has been created within the last few years is the Office of Government Information Services (OGIS), which is housed within the National Archives. OGIS has been tasked specifically with mediating disputes between requesters and agencies. OGIS does not categorize itself as being on the side of the requester, but rather as a neutral mediator. However, the net effect of its work has been to break data logjams and otherwise assist requesters in obtaining records. We've used them once, and will be using them again, as they were able to obtain a response for us after a three-year agency delay. They are a great resource to connect yourself with at the federal level.

3. Finally, there is the litigation remedy. In this process, a lawyer is most often required, although some people have successfully sued *pro se*. Steven Aftergood of the Federation of American Scientists took on a *pro se* FOIA suit a few years ago and prevailed. For the most part, however, requesters should employ an attorney to take on this sort of work. Our counsel JT Haines represents our interests during FOI litigation, which we have become increasingly involved in.

It should be noted here that litigation entails risks – the most pointed of which is that you might create case law that negatively affects other requesters. In cases of what is called "constructive denial" - where an agency simply won't respond to you - the danger of making bad case law is low, since the issues are simple and have been previously litigated. Litigation over withholding is much more difficult - and possibly riskier - depending on the existing case law landscape.

Our advice would be to use this tool in a strategic way, and to be careful in how you employ it. If you're going to be treading into an area of FOI law that is at all unsettled, make sure that you have not only competent legal counsel, but counsel that has a FOI resource base to draw upon, so that you don't inadvertently damage the prospects of other requesters that come after you.

Summary

The remedies I've mentioned are, of course, individual responses to systemic issues. At the individual level, an informed and active user-base is necessary

to keep FOI laws functional, and agencies compliant.

At the macro level, legislative attention is ever required to address deficiencies that evolve within the FOI system. Keeping FOI laws updated is a critical part of preventing a return to where we were in the mid-1960s – pre-FOIA – when litigation was often the only way to resolve record access issues, and the public was largely shut out of the process.

In both instance, engagement by the scientific community can be a part of the necessary solutions. Thank you.