FEAR AND LOATHING (of Archives) IN A POST-FOIA WORLD
International Council on Archives, Annual Meeting
Brussels, Belgium, November 24, 2013

Archives and archivists are facing an existential threat like nothing we've ever seen before. We've always assumed that what we've been doing for generations–boxing up and collecting official institutional records to make them available to researchers–would work in today's digital world, once we figure out the right way to deal with what is essentially the electronic equivalent of yesterday's file cabinets.

And why not? The digital world we live in today is like the air we breathe–so ubiquitous that we barely give a thought to using work e-mail to shoot off a note to our spouse, or networking with far-flung colleagues as if they were sitting in our office. And that, of course, is what makes the digital footprint we all leave so valuable to researchers in the future, and why archives are so eager to find a way to harvest it.

But what if this shiny, new networked age has a dark side, and what if that dark side suddenly threatens to literally turn off the lights for archives? It's already happening, and it's been insidious in the way it's snuck up upon us.

Not surprisingly, the events causing the threat originally had little to do with archives. From my perspective as an archivist at a major research university, it all started with efforts to debunk climate change research. Back in 2009, unknown hackers broke into the computer servers of England's University of East Anglia, a leading center for climate-change research. It was just weeks before a major climate-change summit in Copenhagen and was an obvious attempt to discredit the research and the researchers themselves by exposing what the climate-change deniers claimed was proof of data manipulation and suppression of critics.

Subsequent investigations in the UK determined that these charges were false, but the fallout did not end there. One of the scientists whose e-mails were scooped up came from the U.S. Originally, he was at the University of Virginia, a state institution, thus making him a state

employee. As the so-called “climategate” issue raged in the media, a conservative advocacy group dedicated to exposing what they called “false science,” decided to file a FOIA request in Virginia for all this scientist’s e-mails. They claimed they were entitled to know if state funds were used to “defraud the public about climate change.” The scientist was cleared of all charges of manipulating data, but the case is still rattling around state courts because there is a question whether unpublished academic research is covered by FOIA. But this scientist’s case doesn’t end here. By 2009, when the hacking occurred, he had moved to Pennsylvania State University. Because of the ongoing controversy in Virginia, Penn State also felt obliged to investigate the scientist for data manipulation. Again, he was cleared. All of this was heavily covered not only in the mainstream media, but especially in news outlets like the *Chronicle of Higher Education* that are aimed specifically at university faculty.

Then came the U.S.’s off-year elections in 2010. Several previously Democratic states suddenly found their governorships and entire state legislatures turned over to Republicans, most of them from the ideological far right. In Wisconsin, a state known for over a century for its progressive politics and union affiliations, the new Republican governor and legislature quickly worked to pass legislation in 2011 banning collective bargaining for most public employees. Tens of thousands of citizens protested daily outside the state capitol.

One of the most prominent critics of the anti-labor move was a nationally famous historian at the state university of Wisconsin. Among other actions, he published a strong op-ed piece in *The New York Times* against the new legislation. As a direct result, he found himself the subject of a wide-ranging FOIA request from a staff member of the Wisconsin Republican party. They were sure he had used his university e-mail account to engage in political activity, which would be a crime for a state employee. As it turns out, the man knew enough to have scrupulously kept all his political advocacy on his own private accounts, but that wasn’t enough

to stop the FOIA request. His account, of course, also had the occasional private e-mails to family and to and from colleagues around the world about his and their research in progress. Luckily, the university’s legal counsel constructed a very savvy response to the FOIA request relying in part on the notion of academic freedom–the lawyers restricted the e-mail search to only those items containing the governor’s name, the word “union,” and the like, but they refused to turn over anything of a private nature or anything deemed “intellectual communications among scholars.” This was the first high profile attempt to use FOIA to try to discredit an academic for partisan political reasons.

The mischief, however, didn’t stop there. In neighboring Michigan, a libertarian think tank followed Wisconsin’s lead and filed FOIA requests on the labor studies departments of three state universities, looking for anything with the words “collective bargaining disputes” and even the name of a left-leaning news commentator.

In the midst of all this, and not thinking this had anything to do with us at the University of Illinois, the Archives’s records management team began work on a test project to capture all of the e-mail of the president, vice-presidents, and chancellors. The plan was that once we worked out the logistics with the senior administrators, we would extend the program to deans, directors, and to some faculty in a progressively more selective fashion. As with any major digital effort, we planned to take many months before we would actually capture the e-mail. And so, this past spring, with the imprimatur of the university president, we sent out what we considered an innocuous memo announcing our pilot program.

Administrators naturally had some concerns, but we did not expect the rather substantial blowback from some key faculty leaders. They worried about ownership of intellectual property, about privacy, and about the increased vulnerability to FOIA once it could be known that there were archival stashes of faculty e-mail. Apparently, our faculty had become overly sensitized to

the issue of electronic privacy because of what had happened to their colleagues in England, Virginia, Wisconsin, and Michigan. We, of course, immediately started crafting an even more deliberative strategy to deal with these fears, but before we could release it, Edward Snowden became a household name. Now the fear and loathing we had encountered with our first memo became full-blown paranoia on the part of some of our faculty, and it became glaringly apparent that we were becoming their way of pushing back against outside forces they could not control. They might not be able to do anything about FOIA or hackers or the NSA, but they could certainly push back against us.

Now, if you think this is merely a matter of me becoming a bit paranoid myself, just two weeks ago, I was told by an outgoing administrator, whose records fall within our legal mandate, that he had been regularly purging his e-mails to, as he put it, “avoid storing anything confidential in a fashion where it could be easily hacked into or accidently forwarded.” What this kind of behavior means for the future of archives is obvious: it undermines our ability to secure cultural heritage and it makes accountability impossible for the public we all serve.

CONCLUSION

What we are faced with is an unfortunate mix of advanced technologies and widespread social angst, both of which are outside the usual sphere of archives and records management. Hacking, of course, is a criminal offense, but FOIA requests are not, even if used for political purposes. That’s because the law is neutral regarding access to records–whoever wants the information has the right to request it. As archivists, how can we argue with that?

There can be no one solution to this multi-faceted problem, but probably the most important first step is to address the fear and paranoia that is starting to infect the people from whom archives must secure records whether for accountability or preservation of heritage. To this end, every archives should immediately make clear as publicly as possible all the safeguards

it has in place to protect not just privacy, but especially a person’s current research work, including data, unpublished works, and informal professional communications. It is concern for the vulnerability of these types of records that appears to create the most fear among records creators. Such safeguards must include everything from computer security measures to multi-year restrictions on access.

Given the networked world we live in, however, just dealing with individuals or even focusing on our own institutions will not suffice to dissuade records creators from deleting everything, as one tech administrator at my institution has been doing. That’s because, as the climate-change incident showed, if one individual’s e-mails or research data are breached, then the e-mails or data of dozens, maybe hundreds of others, who corresponded with him or her, also have been breached. That’s the dark side of living in a networked world. Therefore, we need to approach the hearts of those research networks most important to our constituencies to impress upon them the importance of involving professional archival management in their output. In the case of “climategate,” for instance, the heart of the network would have been the University of East Anglia’s Climate Research Unit. I’m not saying archival management could have stopped the hackers, but it’s entirely possible that not so many years worth of e-mails and data would still have been on that unprotected current server–they would already have been under archival management elsewhere. And if we can convince the centers of a few such networks of the value of archiving their data, the confidence in archives may spread to other network’s members, wherever they happen to be.

Perhaps most important in stemming the fear we are beginning to see among academics will be for archives to work closely with their institutions’ legal counsels to forge robust policies for dealing with fishing-expedition FOIA requests like the ones in Wisconsin and Michigan. The University of Wisconsin’s strong defense specifically excluding anything of a private nature

or anything deemed "intellectual communications among scholars" is a model for universities to follow. Thus, archivists must make sure their institutions have this kind of strong policy in place and promote it widely to our constituencies. As for protection against hacking, well, even the Pentagon has been hacked. Every one of us, from teenage gamers to heads of state, is vulnerable–there is no way to stop a determined hacker. This is life in the digital age. Going back to clay tablets simply will not happen.

At the global level, either through the ICA or through the ICA in dialogue with international scholarly and scientific societies, we need to become strong advocates for the preservation of these digital records for historical purposes. We need to publicize how critically important it is to preserve digital records of scholars and scientists, lest this intellectual backbone of our society be lost to future generations.

ICA should consider developing a policy statement declaring that it is a fundamental human right for living individuals to control the release of information about themselves or their creative works.[1] ICA should also consider promoting a more sophisticated advocacy of archives beyond just open government. The public does have the need for both privacy from government prying and for freedom of information. Its our job to create an environment that does not undermine the essential role of archives in securing the culture and intellectual record of society. That, I think we would all agree, is an equally important human right and well worth defending.

---

[1]Ann Wells Branscomb, *Who Owns Information: From Privacy to Public Access*, (New York, Basic Books, 1994) 180-81 argued that resolution of issues of securing privacy and protection against appropriation of personal information by going beyond conventional notions of public records and instead focus on giving all individuals property rights in all personal information. She developed this idea from: Arthur R. Miller "Personal Privacy in the Computer Age," *Michigan Law Review* 67 (April, 1969) and Alan Westin, *Privacy and Freedom*, (New York: Atheneum, 1967). Westin argued that this 'right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due processes guarantees that our law of property has been so skillful in devising." (P. 324-25).