Protecting Sensitive Email: Archival Views on Challenges and Opportunities

Katie Shilton, Amy Wickner, Douglas W. Oard
University of Maryland, College Park (USA)

Jimmy Lin
University of Waterloo (Canada)

Email is a critical institutional and personal record, but including email in archival collections can raise privacy concerns. Semi-structured interviews with archivists describe challenges such as interleaving of personal and institutional records, and donors' complex definitions of sensitive information. Limited current solutions suggest potential technical interventions, such as identifying and filtering commonly sensitive information types, and analyzing the context and content of messages to find anomalous records. We discuss how these findings contribute to privacy-sensitive search tools for email collections.

Introduction:

Providing access to email in archives and special collections presents significant sociotechnical challenges. Defining sensitive information for email users in different roles and contexts, and building access tools based on those definitions, is a complex problem. This work-in-progress paper collects expert knowledge about privacy concerns from archivists who have processed email collections to guide follow-up studies and system design.

Background

Sensitive or private information is a social, contextually-defined phenomenon. Theoretical and empirical work has shown that individuals' privacy concerns are largely shaped by social norms within particular information contexts (Martin & Shilton, 2016; Nissenbaum, 2009). Contextual norms dictate what information it is acceptable to collect, who can have access to it, whether it should be kept confidential, and how it can be shared and reused. These norms take into account roles (people or organizations who are the senders, recipients, and subjects of information); information types (content being transmitted); transmission principles (constraints on the flow of information); and information purpose or use (Nissenbaum, 2009). Key to contextual definitions of privacy is how the components work together within a particular context: who receives the information, what type of information, how is it used, and for what purpose.

Understanding privacy as context-dependent presents several challenges for protecting email archives. Email use crosses social contexts: A person may email family members, their boss, and their doctor from a single account. However, understanding privacy as a function of roles, information types, transmission principles and information purposes enables us to outline variables to test empirically and operationalize in system design. To understand which variables matter most to email privacy, we conducted interviews with subject experts: archivists who have processed email collections.

Method

To select interview subjects, we contacted members of the Mellon Foundation and Digital Preservation Coalition Task Force on Technical Approaches for Email Archives, as well as archivists who had presented on email collections at meetings of the Society for American Archivists (SAA) or had written case studies on email archiving. We searched digital preservation-related blogs, Twitter, and several search engines for combinations of terms like

email archive, preservation, and curation. We also asked interview subjects for the names of colleagues to interview. This resulted in 10 interviews of between 40 and 75 minutes via phone and Skype.

Our questions focused on concerns about sensitivity or secrecy shared by donors, concerns discovered by archivists, and current solutions for addressing those concerns. Two authors coded interview transcripts using an open coding process to analyze the interviews for emergent themes. We each coded a matching subset of the interviews, and then met to discuss divergent codes. After agreeing upon a coding scheme and definitions for each code, we recoded the entire set of interviews.

Findings

To guide future studies and tool development, we report one category of findings: conceptual categories for sensitive information encountered by archivists, either raised by donors or discovered during processing.

Role: Archivists report that donors frequently want to protect emails from particular correspondents (often family members), or alternately, to protect their archive from access by particular roles. For example, when asked about donors' concerns about access, one university archivist immediately replied:

> Newspapers. Public media. Around here, if I'm talking to a distinguished alum, or I'm talking to a faculty member, almost always, if they're concerned about something, it's, "I don't want it on the front page of [the local paper]," or, "I don't want it on the front page of [the student newspaper]." That is their single biggest concern, is the media distorting what their intention was.

However, neither role-based category is straightforward. As one archivist explained:

> So a lot of them are concerned about their family members being present. There's a donor … he initially was like, "You don't need anything with my family, so if you screen anything out, that's fine." But then … he actually talked with his adult children a lot about his work, and they kind of gave him feedback, so that's gonna be a much stickier wicket than we had initially anticipated.

Information type: Archivists also indicated types of particularly sensitive information. For example, personally identifiable information (PII) such as social security numbers, banking information, and health information were all mentioned. University archivists mentioned student records, and several archivists discussed legally privileged information and information relating to pending litigation. Archivists also raised concerns about trade and strategy secrets, internal business security information, business contracts, and nondisclosure agreements.

Contextual violations: Archivists also discussed concerns about information that, if revealed, might risk a donor's reputation. Reputational risks don't fall into a single category of Nissenbaum's framework, but instead emphasize the ways that elements of the framework work together: Information meant for one context becomes embarrassing if disclosed in a second context. Reputational risk types included memberships and beliefs ("his grandfather or great-grandfather…was a member of the Klan and he was scandalized about that") and evidence of stigmatized activity (such as drug use). But reputational risk also incorporated less obviously controversial issues that could be embarrassing to donors: using inappropriate language in work emails, gossiping about another person, making "unfiltered" or – as an archivist put it – "very very frank" remarks, or expressing emotional content in professional situations, for example.

Donors also worried about revealing their involvement in controversies or fights with others. As one archivist relayed:

> Usually, [sensitivity] is almost entirely going to be something that happened in their career that was contentious. Some controversy that they were part of, some event where they were at loggerheads with another person … and they would prefer not to have that made public.

To further complicate reputational risk, donors worried about not only their own reputations, but also those of their correspondents. Sometimes donors wished to protect the identities of their contacts:

> So for example, we have the papers of a very prominent religious speaker and she gets a lot of letters from people about spiritual crises they're going through. And in some cases that involve… heavy things like abortions, she has asked that the identifying information, the name of the person who sent her that letter be anonymized.

In other cases, donors wished to protect the content of their interactions, for example, emails from family members.

Strategies: We asked archivists to discuss current strategies for protecting sensitive information in email collections. Email archiving tools provide technical means of redacting some categories of personal information. Search tools can find PII such as social security numbers and phone numbers. Some repositories place access restrictions on some or all records. Role-based access restrictions were described as attractive to donors, but problematic for archivists to enforce:

> Donors often want to limit access because feel they might be targeted in some way. Part of what they want to be able to do is restrict access to folks who might use it against them. We would not limit access to some individuals and not others. Any restrictions we allow are that you have to get permission from the donor.

The most widely used current solution is time. Embargoes on access to some or all records were the most frequently discussed solution in our interviews. All of our interview subjects suggested a need for more targeted tools to help archivists and donors find and protect sensitive information in email collections.

Design Implications

The categories of concern explored here, including roles, information types, and more contextual forms of reputational risk, can guide techniques to protect sensitive information. Beyond today's tools that delineate and then search for sensitive *topics*, we might consider searching for unusual *contexts*. If many instances of sensitive information are in fact information taken out of its original context, we should investigate ways to sense and protect out-of-context information. Finding and protecting, for example, personal emails in a work account, emails sent to an unusual person, or emails using unusually course language might help to mitigate donors' concerns. But because researchers might value anomalous instances that are *not* sensitive, a system must also learn to distinguish between anomalous communications. We will also use the categories of concern described by archivists to guide surveys for email users to discovers roles and information types most likely to be sensitive to specific users.

Limitations

Interviews only elicited areas of concern frequently experienced by archivists and donors. The interviews did not elicit emergent types of sensitivity. For example, inferences about a person's habits or routines based on non-sensitive emails might be privacy-invasive. Future work will rely on surveys, text analysis, and machine learning techniques to further elucidate definitions of sensitive information and protect sensitive content.

Acknowledgement

This work was supported in part by NSF grant 1618695. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

Martin, K. E., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society, 32*(3), 200–216.

Nissenbaum, H. (2009). *Privacy in context: technology, policy, and the integrity of social life.* Stanford, CA: Stanford Law Books.