

3-17-2021

Managing privacy: A survey of practices in digital archives and libraries

Virginia Dressler
Kent State University, vdressle@kent.edu

Kelley Rowan
Florida International University, krowan@fiu.edu

Rebecca Bakker
Florida International University, rbakker@fiu.edu

Follow this and additional works at: <https://digitalcommons.fiu.edu/glworks>



Part of the [Library and Information Science Commons](#)

Recommended Citation

Dressler, V., Rowan, K., Bakker, R. Managing privacy: A survey of practices in digital archives and libraries. *Journal of Digital Media Management* Volume 9 / Number 2 / WINTER 2021, pp. 177-190(14)

This work is brought to you for free and open access by the FIU Libraries at FIU Digital Commons. It has been accepted for inclusion in Works of the FIU Libraries by an authorized administrator of FIU Digital Commons. For more information, please contact dcc@fiu.edu.

Managing privacy: A survey of practices in digital archives and libraries

Received (in revised form): 17th September, 2020



Virginia Dressler

Digital Projects Librarian, Kent State University, USA

Virginia Dressler is the Digital Projects Librarian at Kent State University. Her specialty areas include the management of digital projects and the migration of analogue collections to open digital collections. She holds an MLIS from Kent State University and an MA in art gallery and museum studies from the University of Leeds.

Kent State University Library, 1125 Risman Dr., Kent, OH 44242, USA
Tel: +1 330 672 1465; E-mail: vdressle@kent.edu



Kelley Rowan

Digital Archives Librarian, Florida International University, USA

Kelley Rowan is the Digital Archives Librarian in the Digital Collections Center at Florida International University where she is responsible for publishing electronic theses and dissertations. She also manages various projects related to the dPanther digital repository and serves as a dPanther liaison within the university and with community partners. She specialises in the science of survey creation, offering workshops through the university's Digital Scholar Studio, and is the Editor-in-Chief of Athenaeum: Scholarly Works of the FIU Libraries Faculty and Staff collection.

Digital Collections Center, Florida International University, Green Library 818, 11200 SW 8th Street, Miami, FL 33199, USA
Tel: +1 305 348 1079; E-mail: krowan@fiu.edu



Rebecca Bakker

Digital Collections Librarian, Florida International University, USA

Rebecca Bakker is the Digital Collections Librarian in the Digital Collections Center at Florida International University. In addition to overseeing the retrospective mass digitisation of the university's theses and dissertations, she provides workshops on digitisation skills, metadata and content management. Rebecca specialises in digital humanities topics such as creating oral histories and digital exhibits. She also serves as a liaison for community and university partners working with the university's digital and institutional repositories. She holds an MLIS from Florida State University.

Digital Collections Center, Florida International University, Green Library 818, 11200 SW 8th Street, Miami, FL 33199, USA
Tel: +1 305 348 1079; E-mail: rbakker@fiu.edu

Abstract Building on past research regarding privacy and digital librarianship, this study surveyed managers of digital libraries across the USA to gauge prevalent attitudes regarding individual privacy versus access to information. In the wake of controversy surrounding the European Union's 2014 ruling regarding the 'right to be forgotten', the authors sought to develop a better understanding of how digital library managers in the USA handle privacy concerns, such as takedown requests, especially in light of the strong protections for first amendment rights in the USA. This research explores whether the

majority of archives and digital libraries have developed privacy policies and what they consider to be the key elements of a robust privacy policy. The study also explores the shifting attitudes around privacy and access, both of digital library managers and of their institutions, in an effort to determine how these relate to the handling of such requests. Finally, the research examines how often information professionals receive takedown requests from their communities, with the hope of tracking this trend over time. This paper provides an overview of the current landscape involving privacy policies and takedown requests, and highlights some of the fundamental issues facing information professionals so that they may have the necessary resources to develop and implement privacy policies at their institutions.

KEYWORDS: digital archives, digital libraries, privacy, practitioners, ethics, information professionals

INTRODUCTION

Privacy has been under increased scrutiny in the past few years, particularly how it relates to digital tracking, the capture of consumer information and practices relating to user data in social media. Privacy as a concept, however, is a looming and often evasive idea. For digital librarians, privacy issues are often rather conspicuous, and at other times hidden in plain sight. This paper investigates the strain between access and privacy in digital collections, and explores how practitioners relate to privacy in their decision-making regarding takedown requests and how this is reflected in the development of privacy policies at their institution.

Digital librarians and archivists, whether at universities, colleges or special libraries, are the custodians of the historical record, and interested in preserving and making such documents discoverable so that scholars and community users can maintain accurate narratives. While librarians are trained in copyright and sensitive to the careful handling of private documents, instances arise where individuals ask that content relating to them be taken down from a digital repository. Dulong de Rosnay and Guadamuz¹ found that the most common reason for takedown requests from Google came from both the victims and perpetrators of sex crimes and for those

who had committed financial crimes. In the university setting, research indicates that students who are unhappy with their research or who have plagiarised often ask for their work to be removed or embargoed from their institutional repositories. In some instances, students from closed societies who fear retribution have asked not to have their names associated with their work.² In these cases, how takedowns are handled can literally mean life or death for the individual, while the other reasons fall strictly into the realm of privacy concerns over social stigmas and personal preferences. In 2017, Dressler and Kristof³ surveyed Association of Research Libraries (ARL) member institutions on how practitioners handled takedown requests. This survey was used as a basis for the present research.

The right to erasure versus freedom of expression

The Right to be Forgotten (RTBF), or Right to Erasure law, was created in 2014 after a Spanish court ruled against Google, requiring the company to remove links to personal information if asked by European Union (EU) residents.

To assess whether removal requests meet the criteria for removal, Google developed a policy that measures whether the content in question is inaccurate, inadequate, irrelevant

(or no longer relevant) and/or excessive. Currently, Google removes about 42 per cent of the requests made.⁴ When Google delinks information, it is also required to notify the controllers of that information concerning the need and reason for said delinking. According to the RTBF law, reasons for delinking information include the removal of sensitive information, such as involvement in a sex crime (whether as victim or perpetrator); absence of public interest; where the information involves minors; and information pertaining to a crime where the sentence has already been served.

Article 17 of the EU General Data Protection Regulation — The Right to Erasure — illuminates the difference in cultural values between the EU and USA with respect to how privacy is considered. While the EU prioritises the protection of personal data, within the USA, the RTBF stands in direct conflict with the freedom of expression enshrined in the US Constitution's First Amendment, as well as in Article 17 of the United Nations' Declaration of Human Rights. To this end, it has been highly criticised as verging on censorship.

In early 2020, the UK appointed Ofcom as internet regulator, inciting further backlash both in the EU and in the USA,⁵ as the role of the regulator will be, for all intents and purposes, to censor and restrict access to information on the internet. The EU, however, views this not as censorship, but as a means to control the spread of hate speech and terrorist recruitment.

The existing RTBF legislation can be differentiated from censorship. First and foremost, in theory, the right to erasure does not endanger the preservation record or history, as information is delisted rather than removed. The intention of the RTBF is to allow people to be able to live full and meaningful lives without, for example, being forever stigmatised by past events that have been remediated, as in the case of spent prison sentences, or being forever primarily

identified as a victim of rape, when searched for on the internet.

In the book 'Delete',⁶ Mayer-Schönberger discusses different ideas around the virtue of the idea of purposeful deletion in the digital age, providing some ways to think about programmable 'forgetfulness' within the perfect memory of the internet. The author stresses the importance and role of forgetfulness throughout human history, and has recommended a way to address this concept in a digital world with the idea of expiration dates on information. This idea also echoes the sentiments of the RTBF, allowing some room for natural erasure, expungement of information and ultimately, privacy.

Interestingly, the USA once considered itself at the forefront of proactive privacy policies. This was evidenced with the Privacy Act 1974, which pertained to federal data collection at the beginning of the computing age. At that time, it was rightly assumed that computing power would increase exponentially and be a real threat to privacy. In the article 'Computers and personal privacy', Ware defined privacy as:

- (1) the social expectation that the individual will have some say in how information about him is used, to whom it is communicated, and how it influences him.
- (2) It is the social expectation that the individual will have some protection against unwarranted harm because of the functioning of some record-keeping system and will be treated fairly by such systems.
- (3) It is the social expectation that the individual has protection against unwelcome, unfair, or intrusive collection of information.⁷

Writing in 1977, Ware argued that were an individual ever to experience unfair treatment or actual harm related to information gathering and dissemination, then privacy policies would have failed. At the time, Ware felt the USA to be 'ahead of the game for a change'. Ware

was certainly correct about the growth of information and the threat it could pose to privacy, and it is apparent from the present research that librarians and archivists are concerned about privacy and are attempting to reconcile these disparate concerns both institutionally and personally. As the debate continues between freedom of expression, including access to information, and the right to some semblance of privacy, it is important to understand how the librarians and archivists who manage, collect, preserve and disseminate information are managing these competing points of view among their institutions, communities and the individuals whom the information concerns.

LITERATURE REVIEW

For the literature review, articles and books that focused on privacy and digital archives were examined, many of which discussed the complex ethical issues that were present in many scenarios where privacy conflicted with access. Some articles addressed issues around digital collections representing sensitive populations, such as Native Americans and colonial territories.^{8,9} Another author cited a need for increased care around privacy and responsibility of ethical access from practitioners.¹⁰ In addition, new workflows from UC Berkeley that address privacy during the pre-digitisation phase were examined.

Agostinho¹¹ discusses the complexities of ownership and access in a post-colonial digital archive, digitised and managed by the Danish National Archives. The author grapples with access to digital archives of colonial records from the Caribbean islands St. John, St. Thomas and St. Croix (previously known as the Danish West Indies and under Danish colonial rule until 1917), particularly in cases where a subject was photographed without permission. Issues of ownership, custody, provenance and access add layers of complexity into the digital archive, and the author notes a 'striking divide' between

open access and the right to information and encourages work towards a post-colonial ethics of care in scenarios such as this one.

In a similar vein, Caswell and Cifor¹² call for radical empathy in archives, shifting from a rights-based model towards a feminist ethics of care. The authors give an example of a case involving a volunteer archivist for the South Asian American digital archive. While working through documents pertaining to an Indian immigrant — documents that had been donated by a descendent — the volunteer discovered a suicide note. The archive had included permission to put the note into the digital archive, although the note included a desire from the writer that no one else besides the family should read it. Despite the fact the archive had permission to digitise, the practitioners valued the wish of the content creator and the note was ultimately not included in the digital collection. The act indicated that decisions around privacy were made during the digitisation process as a means to honour the original wish of the content creator.

Schofield and Urban's¹³ research in the matter of takedown requests at academic libraries found that the most common reason for a takedown request is privacy rather than copyright. Respondents in that survey indicated that they were more confident about handling requests for removal that did not involve copyright, as they could rely on 'longstanding informal practices'. It is likely that this confidence is in part due to the lack of legal ramifications for mishandling privacy takedown requests, unlike with copyright.

Shelley Black¹⁴ examines the conflict between the professional codes for archivists (such as from the International Council on Archives and the Society of American Archivists) with respect to protecting privacy and providing access, in the context of takedown requests. Black specifically mentions large-scale digitisation projects, which often unintentionally include private information. The author reflects on the right

to be forgotten as privacy self-management, although Black also notes the need for stronger data privacy laws in the USA.

Ashley Vavra¹⁵ rightly notes that the balance between privacy and access within archives did not originate with RTBF, and has long been part of the professional practice of archivists and librarians. She refers to some of the guiding principles within the American Library Association's Library Bill of Rights, the Core Values Statement of the Society of American Archivists, and the International Federation of Library's ethical code, which stress the ideals of accountability, access to information and fighting censorship. Vavra cautions archivists to remain vigilant about legislation that restricts access to digital information 'for the sake of the public's fair and equal access to information and for the press and public's freedom of expression'.

Most recently, Berkeley Library (University of California) published responsible access workflows centred on copyright, contracts, privacy and ethics. The four workflows connect and provide a framework for practitioners to think about the more elusive and complex digitisation issues. Additionally, the library has published an accompanying community engagement policy, which outlines a process for users who wish to 'make requests to restrict, limit, update, or remove access to digital content'.¹⁶ The new workflows and policy are important steps in the work to acknowledge the complicated landscape of digital initiatives, and also point to a change in practice, making more thorough, thoughtful selections before content is put online. The workflows are also broad and may be adapted for use in other institutions and provide an invaluable tool for practitioners to think about these issues and apply in daily practice.

METHODOLOGY

A survey of digital librarians and digital archivists was conducted between May and June 2020. The survey was administered

through the Kent State University Qualtrics survey tool to assess how practitioners relate to privacy in practice. Invitations to the survey were sent to a variety of listservs, such as Digital Library Forum (DLF) Announce, Ohio Digitization Interest Group, etc. Respondents could opt for a US\$10 Amazon gift card after completing the survey. The survey was reviewed and approved by both Kent State and Florida International University's Institutional Review Boards (IRB #20-198 and IRB #20-0109, respectively). Participant information was anonymised, with all identifying data scrubbed prior to being analysed. The survey included 15 questions, which are detailed in the appendix.

DISCUSSION

Out of 59 participants who began the survey, 46 participants (78 per cent) completed it. The respondents were made up of digital library professionals. They varied in their years of experience, with 36.36 per cent being relatively new professionals, with between zero to five years of working with digital collections in an academic library, followed by 27.7 per cent working 6–10 years, 20.45 per cent working 11–15 years, and 15.91 per cent working over 16 years with academic digital libraries. Most respondents (52.83 per cent) had received one to three takedown petitions in the preceding year. Not surprisingly, larger institutions that served more patrons, as seen in Figure 1, received more takedown requests compared with smaller institutions.

When asked if their institution had a policy in place that addressed privacy and/or takedown requests of content in their digital libraries, 33 people (46 per cent) said they did, with 5 people (7 per cent) indicating they had a draft policy in the works. Twenty-one people (30 per cent) stated that they did not have a policy, and 12 people (17 per cent) were unsure. Eighteen provided PDFs or the URLs of their policies.

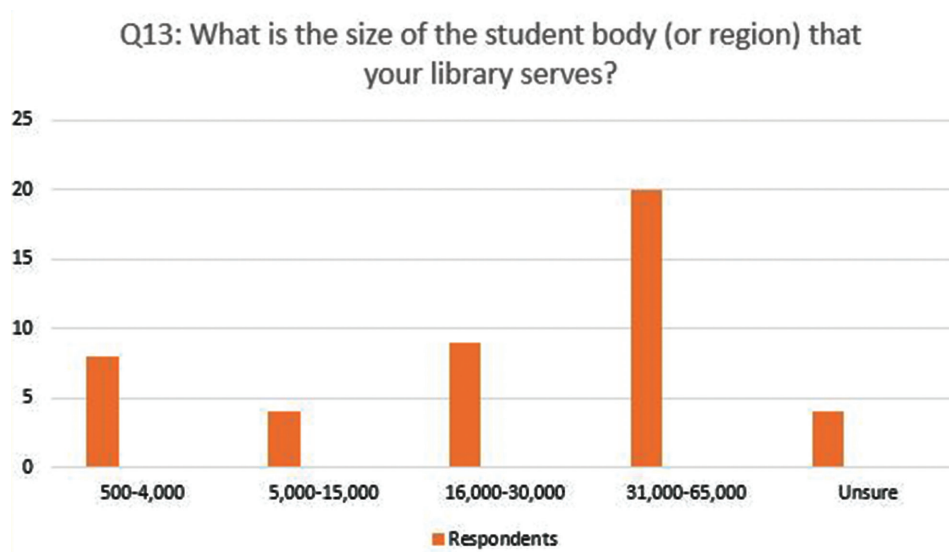


Figure 1: Size of the student body (or region) served by the library

(Two survey participants were from the same institution so only 17 policies are reviewed below.)

Survey participants were asked the most common reasons requests to take down information were approved at their institution. Copyright concerns were most prevalent, and this was listed as the top takedown reason for 30 per cent of respondents. Following copyright, security issues and privacy concerns tied as secondary concerns for 22.4 per cent. However, 4 per cent indicated they would take down content for 'any reason offered', and another 4.8 per cent stated that they did not allow takedowns requested by the community. In a fill-in section where survey participants could include reasons not mentioned, 12.8 per cent listed their particular concerns, including 'sensitive content, eg traditional knowledge' and 'library director concerns'. Two responses suggested that takedown enquiries at their institutions were handled on a case-by-case basis, for example: 'if a former student, for example, is quoted saying something truly, blatantly offensive to the point of doing serious damage to their reputation, we will honor the request'.

Of particular interest was the response to the question that asked participants to state how they felt privacy concerns were weighed against access to content at their respective institutions. As seen in Figure 2, 45 per cent believed that their organisations valued privacy and access equally. This was followed by 20 per cent believing that access was valued slightly more importantly than privacy, and 14 per cent believing access was almost always more important than privacy. In contrast, 7.4 per cent believed privacy was slightly more important than access, and almost 13 per cent believed that privacy concerns were almost always more important than access.

Figure 3 conveys whether access or privacy was more important for respondents in varying stages of privacy policy development. Of those who responded that access was either slightly or almost always more important than privacy at their institution, seven did not have policies in place, eight did, and one stated their policy was being developed. For those that believed access and privacy to be equally important, 17 had policies, four did not, and three were in the works. Six respondents described

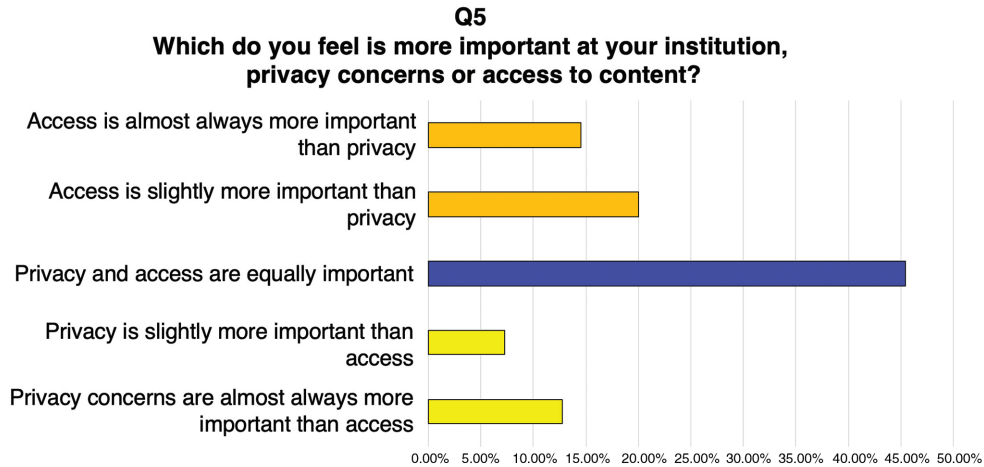


Figure 2: Perceptions of the importance of privacy and access from digital librarians about their institution

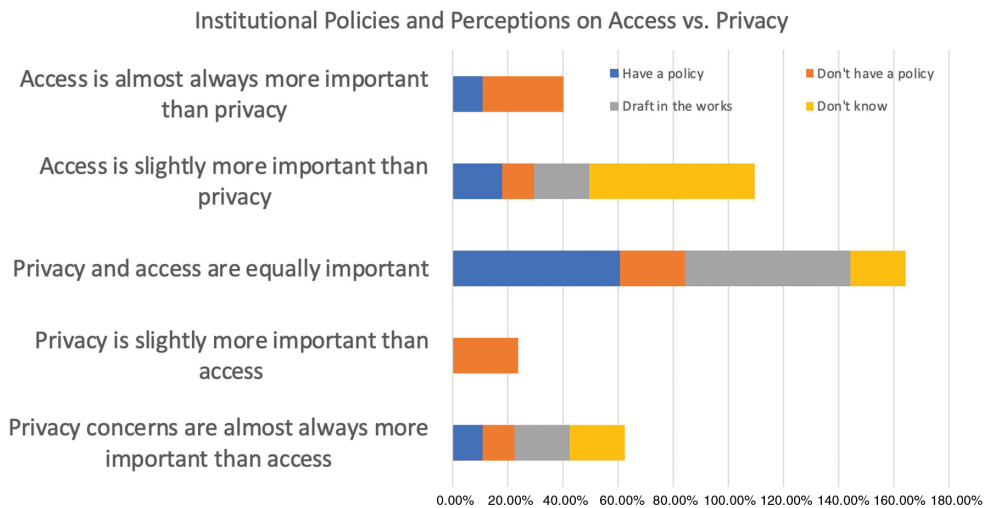


Figure 3: Graph comparing the presence of institutional policies and perceptions on access vs privacy

having no policies in place and indicated that their institutions were more likely to value privacy as slightly or almost always more important, compared with only three respondents with policies and one with a draft who felt the same way.

As shown in Figure 4, when asked about their specific support of the right to be forgotten legislation, most survey participants indicated that they supported it either somewhat (35.56 per cent) or extremely (17.78 per cent). Only 11 per cent stated they were not supportive of RTBF, with 17.78 per cent being less supportive, and

another 17.78 per cent being neutral. This personal support of legislation restricting access to content contrasts somewhat with the institutional value given to access over privacy (Question 5).

Survey questions 9–11 were open-ended questions. Question 9 posed a scenario about a desire to remove a personal name from a digitised student newspaper, due to the requestor's belief that their privacy was being violated. Forty-six responses were recorded and coded. Seventeen (37 per cent) indicated that they would be inclined to keep the text as it was and not make any

Q12
How supportive are you, personally, of the right to be forgotten?

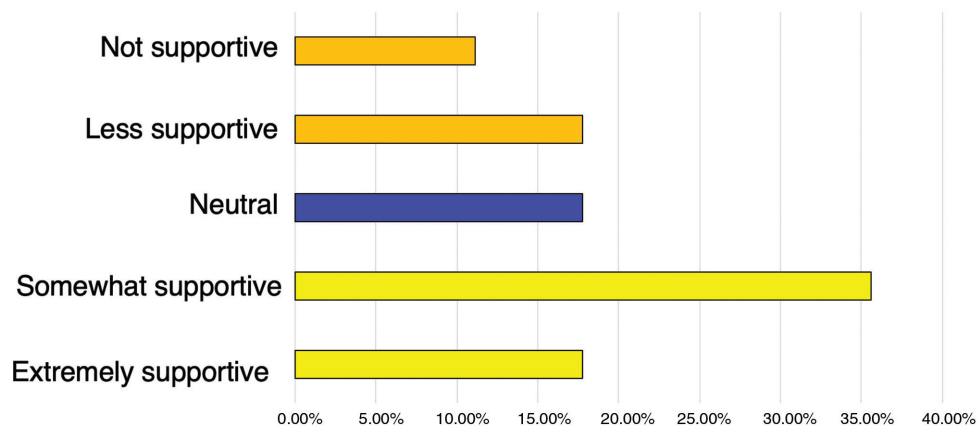


Figure 4: Respondents' support for the right to be forgotten

changes. Around 30 per cent of survey responses indicated they would likely refer to another party for advice (general counsel (5), internal working group/colleague (5), supervisor/library leadership (3), copyright librarian (1)). In the open-text answers, nine respondents commented that the newspaper is a published entity, and information was presumed to be vetted and checked before publication. Many of these responses also discussed the availability of the information in a different format (original print, newspaper digital archive), and thought it would be problematic to remove information from one source while it was still available elsewhere.

Six (13 per cent) said they were open to the idea of redacting the information, and an additional five participants (11 per cent) posed the idea of removing the information in the underlying recognised text, known as optical character recognition (OCR), while keeping the viewable page image intact. Five respondents (11 per cent) indicated there were internal policies or practices that would be referred to in situations such as this one.

A few people commented that takedowns represented a matter for the original content creator or copyright holder. In the words

of one respondent: 'Our takedown request process is limited to the copyright holder, so I could pass the buck and tell her she has to take it up with the copyright holder'. Nine participants (20 per cent) said they would ask for more information from the person asking, and many indicated they would use the opportunity to talk about the implications of removal and the purpose of the digital archive with the requestor.

The survey highlighted the conflicting ways that information practitioners view and handle these kinds of enquiries, often with one side leaning towards retaining the historical record and the other wanting to please the patron. One respondent stated, 'The digital library is not in the business of censoring free press', while another respondent shared that they would 'Take it down, no questions asked', and another stated 'When patrons have a good reason to take down their names or anything related to one's privacy or other rights. We would do all we could to take that down'. One participant said they would cite privacy laws: 'We would respond by citing laws indicating what constitutes a violation of privacy, and explaining how this does not meet that threshold'. Finally, one respondent was unsure.

There were 43 responses to Question 10, which posed a slightly different takedown request scenario than the preceding question, in that it presupposed that a correction had been made to a print publication, and that the digital archives was not the institution that published the title. Ten (23 per cent) respondents indicated they would be inclined to leave the original content as it was, contingent on the correction being included in the digital archive. Here, the rationale was that if the original article was discoverable, the correction would be too. Eighteen participants (42 per cent) indicated doing some kind of work to point to the correction (cross-index (10), update record, scope or notes (6), add correction (2)). Four respondents (9 per cent) indicated that they would remove the name from the original. Another three (7 per cent) said they would work with the publisher or copyright holder to resolve the issue. One respondent said they would check with general counsel. Two (5 per cent) were unsure what they would do in this scenario.

One library professional reflected on the potential time and labour burdens of such a request: 'If my repository has many digitised newspapers, I cannot imagine having the staff time to link older articles with newer ones that offer clarifying information. I could only ensure, to the best of our ability, that all items are findable, so that a researcher who finds the first article will also find the second, and so have fuller context'.

In Question 11, survey participants were asked to share real-life experiences of takedown requests and how they were handled. Twenty-six responded, although 13 (50 per cent) commented that they had no personal experience of dealing with a takedown petition. One respondent noted, 'We host items only with the consent of the creators. Consent is only meaningful if it can be revoked!'. Four (15 per cent) shared similar requests to have a name removed from digitised yearbooks, and in three of the scenarios, the name was removed (one

removal was under directive from general counsel). One commented that the reason for removal was compelling enough to remove the name, while another viewed it as a courtesy.

One person shared they had worked with the content creator on a takedown request: 'One individual requested his name and an article about him be removed from[sic] a digitised organizational newsletter we have in our collection. The organization approved the removal and the article and OCR text was removed'. Another respondent (#98) reflected:

We've never had a takedown request from any of our digital content. I think there are a few reasons for this. First, we're a historical society so we tend to prioritize older content over newer. Second, we do think about privacy, but it's early in the process. It's part of selection. We have so much content (and in this case I'm thinking of our non-newspapers) that if we think there's anything problematic then it's significantly less likely to be chosen for digitization. When we've digitized things about people (often archival collections), it's usually with family permission (because the actual people involved are dead).

This response indicated that privacy is considered as part of the selection process, and perhaps has minimised the potential for takedown requests at their institution. Another individual commented, 'We have had similar requests from a student writer who felt that what she published in the student newspaper while she was at the institution did not reflect her current views on the topic. In this case, we did not feel the reason given was compelling enough to alter the historical record, and we left the paper as is'.

A few respondents shared scenarios of times when information was removed as a courtesy to the requestor (in some cases, alumni were the ones asking). For example (respondent #23):

A request was made by a patron who found his name, picture, and information about a fellowship he was awarded in high school in a printed journal for a small community organisation. He requested it be removed on grounds of invasion of privacy. We assessed the information and found it was factual and newsworthy, and did not violate privacy laws. The assessment involved a number of people including a scholarly communications officer/lawyer, University Librarian, and collection staff (head and archivist). It was decided as a courtesy to remove only his name from the underlying text, but retain the page image as it was.

This response was interesting in that they noted the factual nature of the information, but also empathised with the requestor enough to comply with the entreaty.

Survey participants described additional situations they had encountered where removing items from the digital record were contemplated. One described a scenario of names being removed from photographs depicting minors in a religious setting. Another respondent described a time where allegations were made towards a content creator that led to moving images into a dark archive, although they noted the allegations were never proven one way or the other. Another cited a scenario where a colleague had asked for their name to be removed from an online publication with fear of safety, which was granted.

Privacy policies

There were 17 policies provided by the survey respondents, either by linking to a public website with the policy or uploading the document directly into the survey tool. The better policies included several elements, such as clearly defining the collection, describing use and retention of private information throughout the various library systems represented by survey takers, explaining the types of information

collected and whether the information was shared with any other parties, as well as ways to opt out or request that their information not be collected. One library with a more comprehensive and detailed policy outlined a process for patrons to opt in to have their information collected. The more extensive and comprehensive policies also included references to external vendors and hosting services which have their own privacy practices and policies that library patrons may not be aware of. Many of the documents labelled as takedown policies included a method to contact the library in order to initiate a takedown request, and some included characteristics of a takedown that may be approved for removal (presence of personally identifiable information, legal concerns (protected under Health Insurance Portability and Accountability Act 1996 or Family Educational Rights and Privacy Act 1974), significant risk to privacy and information that would prove (documented) that keeping information up may be a personal threat to one's wellbeing).

Two policies contained the same sentence to address errors in a historical item: 'Given our commitment to preserving the authenticity and integrity of the scholarly and historical record, we are unable to correct errors or inaccuracies present in original items'. Likewise, in another policy: 'The Libraries are opposed to censorship in all forms and strive to collect, digitize, and preserve diverse perspectives in support of education, intellectual freedom, and open dialog on the record of human history'. Statements such as these speak not only to the tension between open access and privacy, but also the complexities of working with primary sources.

One respondent noted that the policy at their institution is 'not available online in order to reduce visibility of takedown request policy', while another stated 'I don't believe we have a policy statement, but we make an e-mail address available for requests'.

Additionally, some policies also included acknowledgments and citations from other documents and policies, such as Code of Ethics and other related documentation from the American Library Association, Society of American Archivists, HathiTrust, ACRL-SAA (Joint Statement on Access: Guidelines for Access to Original Research Materials), and the ACRL Code of Ethics for Special Collections Librarians.

Ethical concerns on privacy policies

Some ethical issues mentioned in the submitted policies include: inclusion of offensive language, images or content that reflects a different era/time period and accounts for social and religious customs that may prevent access to some materials. There may be inherent conflict for some between the presentation of the historical record as-is, and those who may wish to alter content with the intent of appeasing a patron's desire for privacy, removing a profane word or image, etc. This conflict about sanitising history can be particularly difficult for archivists and other content gatekeepers charged with maintaining faithful analogue and digital collections.

One institution stated that in their digital collections they strive to 'protect the privacy rights of individuals documented in our collection; adhere to cultural and ethical guidelines related to sensitive materials; and respect access or use conditions set by creators or donors of objects and documents'.

Future studies/research

The survey indicated that most respondents were personally in favour of RTBF, which restricts access to information, yet most also believed their institutions valued access over privacy. Further studies could be done to determine if the reasons for this had to do with the perceptions of access to information

on platforms such as Google, compared with digital libraries and repositories. Additional research to track the creation of privacy policies by digital libraries would also be useful to determine if the increase shown continues longitudinally.

CONCLUSION

This survey revealed that digital librarians and archivists are currently encountering privacy issues in their collections and are working actively to develop their policies. Almost half of the respondents already had policies in place and the prevailing attitude was that both access and privacy are of equal importance. While the percentage of institutions with privacy policies was still only 46 per cent, it was an improvement over the 25 per cent of respondents indicating their institutions held privacy policies in Dressler and Kristof's 2017 survey¹⁷ of Association of Research Libraries. This trend towards institutions recognising the need to develop their own policies is not surprising, considering the lack of laws in the USA regarding privacy, in contrast to the EU Right to Erasure. It should also be noted that access has historically been the primary concern among information professionals, as shown in the various professional codes and value statements. With the development of digital repositories, librarians and archivists were initially inundated with a backlog of content needing digitisation, and the work of providing access may have taken precedence over issues concerning privacy, with the exception of copyright. As time goes on, information professionals may be able to more thoughtfully take other privacy concerns into consideration, although this survey revealed that the overarching concern for takedowns continues to be the avoidance of copyright infringements, and the ensuing legal repercussions, despite past research that copyright claims are not as prevalent as other privacy requests.

Survey results from the open-ended questions displayed variety in how practitioners process requests for takedowns and also how they relate these requests to privacy and their professional practice. Some institutions have made decisions around selection in digitisation about privacy, perhaps taking into account pre-digitisation workflows like the new one from UC Berkeley. The responses mirrored the literature review that showed this is an ongoing debate by information professionals, with decisions about privacy and access happening not only after an item has been made available online, but also during the acquisition, curation and digitisation processes.

The study also found that concerns over privacy and access are presented in the regular work of digital librarians, and indicates that they may benefit from having institutional policies and a framework of best practices. There was some conflict on how practitioners felt about privacy as a concept when contrasted to their actions and thoughts around privacy requests in takedown demands. Respondents with privacy policies in place were slightly more likely to report that their institutions valued access over privacy, suggesting that having a privacy policy in place may encourage institutions to be more permissive in regards to access. As practitioners encounter takedown requests, they will need to determine whether privacy or access will be the driving factor in their decisions. While these competing concepts are both important issues, at some point it may not be possible for them to be equal entities in the larger picture of practice. Policies and best practices that have been developed over time can help in some of these scenarios, although as some of the survey answers found, it may come to a case-by-case basis. The trend for institutions to implement privacy policies has increased in the past three years, and yet respondents indicated the need for continuing work around policy creation.

APPENDIX: SURVEY QUESTIONS

1. Do you have a policy (or policies) in place that address privacy and/or takedown requests of content in your digital library or website?
 - Yes
 - No
 - We have a draft in the works
 - I am unsure at this time
2. If available, please provide a link to the policy, or to both policies, in the text box below. You may alternately also upload the text directly if you prefer in the next question.
3. If available, please upload policy, or policies, here.
4. What reasons for takedowns are approved at your institution? Check all that apply.
 - Any reason offered
 - Privacy concerns
 - Security issues
 - Copyright concerns
 - Because a patron doesn't want the content there (they gave no other reason)
 - We don't allow takedowns requested by the community
 - Other (Please explain below)
5. Which do you feel is more important at your institution, privacy concerns or access to content?
 - Privacy concerns are almost always more important than access
 - Privacy concerns are slightly more important than access
 - Privacy and access are equally important
 - Access is more important than privacy
 - Access is almost always more important than privacy
6. Approximately how many issues arise concerning privacy and/or the takedown of content due to privacy concerns at your institution per year?
 - None
 - 1–3
 - 4–7

- 8–11
 - 12–15
 - More than 15
7. What is the current staffing (part-time and full-time) for digital projects in place at your institution?
- None
 - We do not have a department, digital work is done by other departments
 - 1–2
 - 3–4
 - 5–6
 - 7+
8. What role do you have within the digital library?
- Content production
 - Metadata creation
 - Publishing content
 - Digitising
 - Manager/administration
 - Other (Please explain)
9. You receive a request for a name to be removed from a particular item in your digital library, directly from the individual in question. The requester believes that the inclusion of their name in an openly accessible digital library violates their privacy. The name appears in print in your digital regional newspaper collection, within the student newspaper that was published in print at your institution, and later digitised for the digital collection. This content has been run through optical character recognition (OCR) software and has been fully indexed by search engines such as Google. How would you respond?
10. You receive another request to remove a name from another digital object from the digital newspaper collection. In this scenario, you find that there is a later mention of a correction to a story that could aid in the requester's defense. (Misprinted information, subsequent findings that alter the original story, a court case where the person is later found innocent of charges, and so on). This particular newspaper was not published by your institution, but from a local township. How would you respond?
11. Finally, if you have had a real-life scenario that is similar to the ones listed above, could you provide information below illustrating such a scenario? Please describe the request, the subsequent chain of events internally, persons involved in the resolution, and the outcome.
12. In 2006 the EU adopted a human rights policy entitled 'The Right to be Forgotten'. This allows individuals to request that access to any or all content about them be removed from the internet. It is distinct from the right to privacy in that the right to be forgotten includes removing public information from websites (eg criminal record, photos, news articles, etc) whereas the right to privacy protects private information (eg medical records, student records, library usage, etc). How supportive are you, personally, of 'the right to be forgotten'?
- Extremely supportive
 - Somewhat supportive
 - Neutral
 - Less supportive
 - Not supportive
13. What is the size of the student body (or region) that your library serves?
- 500–4,000 students/residents
 - 5,000–15,000 students/residents
 - 16,000–30,000 students/residents
 - 31,000–65,000 students/residents
 - Unsure
14. How many years have you worked with digital collections in an academic library?
- 0–5
 - 6–10
 - 11–15
 - 16+

15. When were you born?

- 1925–1945
- 1946–1964
- 1965–1976
- 1977–1995
- 1996–2001
- 2002 or younger
- Prefer not to say

References

1. Dulong de Rosnay, M. and Guadamuz, A. (2017) 'Memory hole or right to delist? Implications of the right to be forgotten for web archiving', Social Science Research Network scholarly paper, available at: <https://papers.ssrn.com/abstract=3107565> (accessed 6th June, 2020).
2. Rowan, K. and Bakker, R. (2019) 'The dark side of digitized content: stalking, consent, and subpoenas', DLF Forum, available at: <https://digitalcommons.fiu.edu/glworks/82> (accessed 15th July, 2020).
3. Dressler, V. and Kristof, C. (2018) 'The right to be forgotten and implications on digital collections: A survey of ARL member institutions on practice and policy', *College & Research Libraries*, Vol. 79, No. 7, pp. 972–990.
4. Google. (2020) 'Requests to delist content under European privacy law', Transparency Report, available at: <https://transparencyreport.google.com/eu-privacy/overview?hl=en> (accessed 6th June, 2020).
5. Herbert Smith Freehills. (2020) 'UK Green-Lights Ofcom as the first internet regulator ... But the devil is in the detail', available at: <https://hsfnotes.com/tmt/2020/02/13/uk-green-lights-ofcom-as-the-first-internet-regulator-but-the-devil-is-in-the-detail/#page=1> (accessed 30th September, 2020).
6. Mayer-Schönberger, V. (2009) 'Delete', 2nd edn, Princeton University Press, Princeton, NJ.
7. Ware, W. (1977) 'Computers and personal privacy', *American Philosophical Society*, Vol. 121, No. 5, pp. 355–359.
8. Agostinho, D. (2019) 'Archival encounters: Rethinking access and care in digital colonial archives', *Archival Science*, Vol. 19, No. 2, pp. 141–165.
9. Mathiesen, K. (2012) 'A defense of Native Americans' rights over their traditional cultural expressions', *The American Archivist*, Vol. 75, No. 2, pp. 456–481.
10. Black, S. (2020) 'The implications of digital collection takedown requests on archival appraisal', *Archival Science*, Vol. 20, pp. 91–101.
11. *Ibid.*, ref. 8 above.
12. Caswell, M. and Cifor, M. (2016) 'From human rights to feminist ethics: Radical empathy in the archives', *Archivaria*, Vol. 81, No. 1, pp. 23–43.
13. Schofield, B. and Urban, J. (2016) 'Takedown and today's academic digital library', available at: <https://osf.io/preprints/socarxiv/3rhfe/> (accessed 16th July, 2020).
14. *Ibid.*, ref. 10 above.
15. Vavra, A. (2018) 'The right to be forgotten: an archival perspective', *American Archivist*, Vol. 81, No. 1, pp. 100–111.
16. University of California (Berkeley Library). (2020) 'UC Berkeley Library makes it easier to digitize collections responsibly with novel workflows and bold policy', press release, May, available at: <https://news.lib.berkeley.edu/responsible-access> (accessed 15th July, 2020).
17. *Ibid.*, ref. 3 above.