AA06: Trusting Digital Archiving Services

Literature Review

August 21, 2016, v4.1 - Kristina McGuirk

Trust, Motivation, and Digital Archiving Services

As institutions consider solutions to the problem of storing *and* preserving their digital content, the concept of digital preservation as a service is emerging. Digital Preservation as a Service (DPaaS) combines the established elements of reliable storage—a trustworthy digital repository—with a continued preservation process that includes metadata management, security access, integrity monitoring, routine backups, and file migration and/or emulation tactics to combat obsolescence (LOC, 2010, p. 93). It is a scalable, local or cloud-based third-party service that can be provided at different levels to meet an institution's records schedules, storage needs, security demands, access requirements, and degree of preservation desired. DPaaS provides long-term digital stewardship of files by offering "access to the digital objects independent of the hardware and software that originally created them" in order to "relieve the records owners of the onus of engineering and provisioning the preservation infrastructure" (Nguyen and Lake, 2011, p. 557).

Our study, InterPARES Trust AA06: Trusting Digital Archiving Services, looks at the relationship between the records creating agency, records creators, and digital preservation service provider to ascertain the willingness of public sector agencies to use and trust the service offerings of potential third party DPaaS providers, and determine what factors might encourage

or inhibit the agencies' level of willingness. Because DPaaS is still an emerging concept, this topic will be explored through a literature review and subsequent interviews.

Literature specifically on the topic of trusting digital preservation services is scarce—see Donaldson and Conway (2015), Franks (2015) and Oliver, Chawner, and Liu (2011) for the most relevant writings on the subject—so this review will also look at related areas for an informed idea of how trust, use, and DPaaS relate. Digital repositories provide a relevant and associated topic for us to draw research from because they are a precursor and key element of digital preservation services. After covering the development of digital preservation, available services, and current studies of DPaaS, this paper explores literature studying the use of digital repositories; motivations or disincentives for adopting these services; and characteristics of trust and factors that influence trust in these services. It then draws conclusions about where our study should focus its investigation moving forward.

Development of Digital Preservation and Services

Although digital files and storage have been a concern for decades, digital preservation became a recognized issue in the early 2000s. The early focus of digital preservation looked at "specific technical strategies for digital files," followed by processes for preservation (like the production of the OAIS model and the research of the first InterPARES project), and, subsequently, standards and certifications for trustworthy digital repositories (Dale & Gore, 2010, p. 14).

In 2000, the United States Congress funded research on the preservation of digital cultural heritage materials through the Library of Congress (LOC), resulting in the National Digital Information Infrastructure Preservation Program (NDIIPP). This was the early stages of preservation awareness, and this group was tasked with looking to the future of digital

preservation in the U.S., which included discovering the scope of digital preservation concerns, identifying interested parties, and raising awareness of the issue (LOC, 2002a, p. 14). It was in 2002 that the Online Computer Library Center (OCLC) and Research Libraries Group (RLG) recommended research into the development of certification processes for digital repositories (Beagrie et al., 2002).

DPaaS itself has been slow to develop, but it began to gain interest at the same time that digital preservation became a consideration. In 2003, on behalf of the OCLC, Brian Lavoie wrote:

> In general, digital preservation has yet to become a routine component of managing a digital asset's life cycle. The fact that digital preservation has not yet emerged as a common "aftermarket service" for digital resources seems incongruous with the status of digital information as a durable good. (p. 22)

As late as 2013, Dollar and Ashley were also writing on the upcoming emergence of "third party repository solutions, and preservation services, including cloud-based offerings" (p. 320) and these cloud-based repositories were just becoming a viable option for some institutions, such as governments, in 2015 (Franks, 2015).

There are many digital archiving services on the market, but few offer full-service digital storage, access, management and preservation.[1] Most services aim to assist with only individual aspects of digital preservation, such as ingest, access, or storage.[2] Others offer more

---

[1] In 2009, Brown, Katuu, Sebina, & Seles noted that there was not a software-based repository on the market that offered the full service of digital preservation tasks (p. 38).

[2] Examples of this include Europe's PREFORMA (PREservation FORMATs for culture information/e-archives) which assists with compliance of file formats and conformity tests before deposit into a repository (Home, n.d.); the Hub and Spoke Tool Suite (HandS) developed through research with the NDIIPP and focused on interoperability and management of content between multiple repositories (Cruse, 2009, p. 307); and products such as ContentDM

sophisticated tasks, such as Portico, a dark archive for electronic scholarly material that claims to store and migrate content (FAQ, n.d.). Another option is a single source that offers multiple service types: DuraSpace, for instance, includes DSpace (an institutional repository), DSpaceDirect (a hosted repository), Fedora (a framework for building an institutional repository), and DuraCloud (a management and preservation system for cloud content) (About, n.d.). In addition, many services, especially open-source products like Archivematica, are being engineered to facilitate collaboration with other digital preservation products to better meet the full spectrum of needs through different providers.

DPaaS is intended to be a full-solution service. Two prominent DPaaS products noted by Franks (2015) are Preservica and ArchivesDirect. Preservica can be hosted in the cloud or on site, and it includes a system to ingest, store, and actively preserve files as well as a platform to view them—in addition to preservation services. ArchivesDirect, another component of the DuraSpace brand, boasts similar all-encompassing accession, storage, retrieval, and preservation by combining its DuraCloud service with Archivematica for a full-service, single packaged offering (Franks, 2015, part IV).

Exploration of digital preservation services only recently began in earnest. This is in part due to the trend of providing varying levels of cloud-based services for archives, but also a result of the recognition that digital storage does equate to long-term preservation or guaranteed integrity. For example, Nguyen and Lake (2011) proposed a preservation-as-service concept as "Long-Term Digital Preservation as a Service (LDPaaS)."

Current research on DPaaS includes a major initiative by the National Library of New Zealand and Archives New Zealand to pursue a nationwide digital preservation solution. The

---

that offer interfaces for depositing files into repositories and can also include platforms for viewing those items (Brown et al., 2009, p. 38).

DPaaS project is "designed to provide evidence of the demand and need for a national approach to digital preservation" and ultimately model what digital preservation can look like at the national level (Knight, 2015). Smaller pilot projects across New Zealand are contributing to a better understanding of the institutional and user needs for DPaaS ("Digital Preservation as a Service," 2016). This is perhaps the most widely referenced DPaaS project to date.[3]

InterPARES Trust started researching cloud-based services in 2013—Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) (Franks, 2015, part II). DPaaS has since come on scene and is currently being explored in various capacities through InterPARES Trust. Other InterPARES Trust studies include AA03, which is studying "dark" or offline repositories and includes a component looking at whether DPaaS providers would be willing to offer dark archives services; and AS03 is looking at trust and certifications for large archives and long-term preservation of digital material. NA12, Preservation as a Service for Trust (PaaST) is an initiative of InterPARES Trust that directly addresses the challenges of digital preservation in the Cloud. It sets out functional and data requirements that can be included in contracts for preservation with Cloud service providers (the potential benefits of using these requirements are not limited to the Cloud.) This study, AA06, is the first to focus on the trust aspect of pursuing DPaaS.

Studies of digital repository use

As digital repositories have become more prevalent, use of these repositories is being studied, particularly in academic and scientific settings where digital records are often proprietary and produced in large quantities. Characteristically, these repositories are underutilized (Chan, 2004; Davis & Connolly, 2007; Foster & Gibbons, 2005). During

[3] A Google search for "digital preservation as a service" will link to many New Zealand agency sites as well as references to the project on other websites.

interviews for their study on digital repository use, Gillian Oliver found that "where digital repositories had been developed, the transfer of digital records into archival custody had not been as great as expected" (Oliver et al., 2011, p. 313). The reasons why repositories are not being used, even when they are solidly established at an institution, provide tangible concerns related to trust and digital services.

One such study by Hedstrom and Niu (2008) looked at records creators in the social sciences. Although they were required to deposit their research into an archives, the timeliness of that deposit was influenced by the user's views on the repository. Factors that negatively impacted the transfer items to the archives included a "desire to publish more papers from the data before releasing them to a public archive (44%), followed by concerns over confidentiality (35%), loss of control over the data (31%), loss of exclusive use of the data (28%), and the costs of preparing the data for release (20%)" (Hedstrom & Niu, 2008, p. 4).

In 2004, Chan explored the emerging trend of university-based open access repositories, and in the process identified a lack of confidence in the institution's commitment to the repository, apprehensions about copyright, and "cultural inertia" leading to slow adoption processes as negative influences on the use of repositories (p. 293). Foster and Gibbons (2005) further explored the topic by researching faculty deposits into institutional repositories at Rochester University, ultimately identifying a disparity between faculty expectations/perceptions of the repository and the reality of the repository's function and benefits.[4] Davis and Connolly (2007) identified similar reasons that faculty did not deposit into the DSpace repository at

[4] Faculty looked for services that assisted with the creation of works—rather than handled finished works—and seemed to feel that the repository was not for their own individual benefit but for the institution.

Cornell, adding redundancy, a steep learning curve, quality and reputation of the repository to the list, as well as the fear of plagiarism and theft of research data.

Motivation

This section explores what encourages or inhibits the adoption and use of digital repositories and preservation services. Broadly, these motivating factors influence two categories: institutional level decisions to pursue digital preservation, and the records-creating individuals that are responsible for turning over their records to the repository for preservation.

Institutional

Loss is one of the most impactful factors in motivating an institution toward adopting a digital preservation program. Obsolescence, hardware and software failure, availability of technical knowledge and services, and human error and threats such as hacking can all lead to loss (Askhoj, Sugimoto, & Nagamor, 2011; Fresa, Justrell, & Prandoni, 2015; LOC, 2002a). While loss of records and information is itself a concern, the NDIIPP noted the resulting impact on productivity and income as an institutional driver as well (LOC, 2002a, p. 20). A survey of the NDIIPP partner institutions identified other practical business justifications for digital preservation services as well, such as meeting internal needs by bringing together an institution's widespread digital content, providing structured access to that content, and protecting records—which are an economic investment of their own (LeFurgy, 2009, p. 21). The project also recognized an existing concern over the potential to fail to preserve records of cultural significance (LOC, 2002a, p. 20).

Economic incentives are some of the most commonly discussed institutional motivators. In "The Incentives to Preserve Digital Materials," Lavoie (2003) establishes economic models for preservation services and how those intersect with incentives. He concludes that there is

insufficient economic incentive to pursue digital preservation. The LOC came to the same conclusion, particularly emphasizing the lack of incentives to preserve culturally and historically relevant materials that may not have merit to the records producer (2010). In addition, they highlight that businesses in the U.S. have a strong disincentive to preserve records due to the litigious nature of society (LOC, 2010, p. 109). Surveying U.S. cultural heritage tax incentives like historic building preservation, as well as international incentive models, the LOC notes that some current laws and incentives could be stretched to include digital assets but suggests that new or revamped laws and models would provide better incentive for digital preservation (2010). This lack of economic incentives fails to balance the initially high costs of engaging in digital preservation, further hindering motivation to engage in digital preservation services: "The financial rewards of a robust preservation system for digital assets are generally far from immediate, and the high up-front costs may be difficult to justify in a tight economy" (LOC, 2010, p. 92).

Often stimuli for institutional records management comes from external motivators—the laws, regulations, and policies that already specify or influence records management and retention practices (Hedstrom & Niu, 2008, p. 6). These same extrinsic factors can be used to argue for the adoption of digital preservation services in order to better to meet those legal and regulatory requirements.

While there are many incentives and motivations that appeal to the business sense of institutions, these organizations can foster internal conflicting motivations which prevent them from developing digital preservation strategies. The LOC noted that partners in the NDIIPP project worried that copyright and asset management issues would outweigh conversations on preservation (LOC, 2002a, p. 20). Stakeholders also noted that it was "easier to obtain funding

for digitization for access than for digital preservation itself, [because] the long-term benefits and requirements of preservation seem often to be overshadowed by the immediate benefits of current access initiatives" (LOC, 2002b, p. 133).

Mentioned in the LOC report, as well as the previously discussed studies of academic repository use, concerns about copyright can also hinder motivation. Not only is copyright a confusing grey area for both institutions and records producers, the process of preparing, storing, and preserving files involves making copies of files, and "unless an exception to copyright law applies, copyright law is implicated with each copy" (LOC, 2010, p. 93). While this may not prove to be too large of a hurdle for businesses and proprietary records producers, public institutions like archives and universities, as well as private institutions that hold personal data, must consider the ownership and copyright of their amalgamated files.

Institutions also may be unmotivated to pursue digital preservation due to the vast resources required. At a time when many institutions, especially in the public sector, are functioning with smaller budgets and fewer staff, the already limited resources may not be available to be put toward digital preservation. In addition to the expense of a preservation service, the cost of human resources (both time and money) is also high due to the intensive process for preparing files for digital deposit and preservation (Askhoj et al., 2011; Beagrie et al., 2002; Skinner & Halbert, 2009). This process is further explained below in the section on individual motivators.

The "Report on Digital Preservation and Cloud Services" created for the Minnesota State Historical Society highlights the extensive amount of information—including terminology and an understanding of OAIS—needed in order to properly research and identify a service provider (Instrumental, Inc., 2013). Not all institutions may have the resources to afford such a thorough

search for services as produced by this third party evaluator, nor do they have as comprehensive of an understanding of their needs. This complex understanding of the institution well as the resources available—or, simply, an institution's ability to even identify an external, third party qualified to assess these available resources—may negatively impact an institution's motivation for pursuing digital preservation services.

Digital preservation services do offer some financial and functional benefits that could act as motivators, especially when compared to institutionally administered digital preservation programs. Third-party providers often allow levels of preservation services and networks of providers that result in economies of scale, creating more fiscally achievable options to better match institutional needs (LeFurgy, 2009). In addition to being more expensive, Fresa, Justrell, and Prandoni (2015) write that standalone or in-house preservation systems fall victim to "a lack of interoperability and fragmentation of resources into 'digital silos'" which is a less sustainable long-term model (p. 196). Not only is the infrastructure weak, sustainability of resources is also harder to ensure with locally administered repositories. Alongside costs of structuring and maintaining a digital repository, considerable skills and technical knowledge—and trained personnel—are needed to administer an effective institutional preservation program, and these requirements are hard to sustain without large commitments of resources (Brown et al., 2009; Fresa et al, 2015).

Individual

Like institutions, time and effort play a large role in influencing individual motivators. Hedstrom and Niu (2008) conducted significant research into motivations for digital preservation, focusing on creators of archival material. They studied motivations of creators to produce "archive-ready" data packets, or records that are in a state that meets digital repository

and preservation criteria. Their research showed that even when an institution has explicit and even minimal requirements for preparation of data, "data producers may be unwilling to invest the time and effort necessary to meet submission guidelines" (p. 1).

The requirements for submission into a repository are both many and diverse, depending on institutional guidelines for creation as well as repository and preservation requirements. Most work for the records creators and creating agencies falls in the pre-ingest period. Pre-ingest functions can include tagging metadata and unique identifiers, scanning for viruses, generating backup copies, creating Submission Information Packages (SIPs), and checking conformance for compliance with the service's systems (Askhojet al., 2011; Beagrie et al., 2002; Brown et al., 2009; Skinner & Halbert, 2009). Following ingest, a creator should also check records to make sure they maintained functionality, content, format, and metadata (Brown et al., 2009, p. 45). These "resource intensive" tasks can discourage individuals from depositing files in a timely manner and ultimately delay preservation processes (Askhoj et al., 2011, p. 178).

To combat this unwillingness, Hedstrom and Niu (2008) present potential incentives motivating creators to participate in digital preservation, including recordkeeping practices as part of performance appraisals and giving monetary rewards and public praise for participation. They also suggest integrating the preparation for deposit of archival materials into the research and/or records creation processes—in order to better facilitate the transfer of files—but they are careful to note that it would require tools and training early in the project planning or work flow. In addition, their research identified concepts that positively motivated participants, including an awareness that deposits could benefit others, mandatory deposits for potential future funding, deposit as a prerequisite to publishing, and monetary compensation for deposits.

A lack of institutional support for digital preservation also negatively influences individual motivation. Technical solutions may be in place, but without established organizational requirements, procedures, and processes, the individual may not receive the support, training, or efficient process they need to help them feel confident and motivated to use the services (Halas, Porekar, Klobučar, & Blažič, 2008). An attention to change management when transitioning a new system, and guidance in identifying what content needs to be deposited and preserved, could boost individual use (Skinner & Halbert, 2009).

Trust

This section explores literature on trust, starting with the characteristics of trust and moving to specific influences on trust in relation to digital services. Trust, like motivation, is influenced at both institutional and individual levels, and there is much overlap between the two.

Characteristics of Trust

A study of continued user trust in public e-services concluded that trust is a transferable concept: a user's trust of e-services is influenced by their trust in the technology conducting the service and the public administration associated with the service (Belanche, Casaló, Flavián & Schepers, 2014). The UK Data Archive (a repository for social science and humanities data) also identifies trust as a "transitive" trait, suggesting a record producer's trust in the institution should transfer to trust in the repository selected to preserve the records (Trust in Data Archives, n.d.).

Another characteristic of trust is that it is socially and situationally influenced. A historical study by InterPARES Trust (NA11) looking at "how perceptions of privacy, risk, and organizational/culture factors influenced (dis)trust in cloud service providers," identified social and community context and personal disposition, as well as familiarity with technology, online interfaces, and service providers as influencers on trust (Leverich, Nalliah, & Suderman, 2015, p.

2). Through NDIIPP, the LOC also noted social capital's impact on enhancing trust, including the benefit of a "trusted intermediary" (like LOC) connecting institutions with services (LOC, 2010, p. 114).

Hill and Donaldson (2015) connect the transitive and social traits, identifying two types of trust: behavioral trust, which exists when a product has proven to the user that it does what it says it will, and trust built on reputation or promise, called social trust. The experience-based behavioral trust is "more important to their perceptions of trustworthiness," but Siegrist and Cvetkovich also highlight instances where social trust is an easy second if there are no individual experiences on which to base behavioral trust (Donaldson, 2013, part 2.2.1; as cited in Hill & Donaldson, 2015).

Although these characteristics are powerful, it's important to note the liquid nature of trust is not boundless. Not only is the collective perception of trust subject to positive and negative influences—trust and distrust are both influential—it also has limits. Oliver, Chawner, and Liu (2011), detailed below, highlight how differing work environments and mediums can restrict trust's transferability.

In archives and records management literature, attributes of trust have been a frequent area of study. In their literature review on "trustworthiness in archival research," Donaldson and Conway (2015) invoke some foundations of archival theory, including Duranti and MacNeil's pillars of trustworthiness (reliability, authenticity, and genuineness) and Hedstrom and Lee's study on trust as an element inherent to archival documents rather than a construct or perception of the user (a concept strongly related to the study of diplomatics). They also argue that in 2009 Duranti "reinforce[d] the central role of the archivist as the mediator of trust" (Donaldson, 2015, p. 2430). This argument is in line with our research, which suggests that a trusted intermediary—

be it a third party provider or well-known organization or a qualified individual employee—can positively influence trust in digital services (LOC, 2010; Oliver et al., 2011)

Donaldson and Conway (2015) note the lack of research on *how* users relate trust with digital objects obtained from digital repository or preservation service (p. 2429). To address this, and further expand some of the aforementioned traditional trust theory into the digital realm, they studied digital repository users' conceptualizations of trust related to retrieved documents. Concepts of accuracy, validity, authenticity, and even legibility were championed, while stability and objectivity were revealed as less important (Donaldson & Conway, 2015). Although the legibility issue referred to digital copies of materials, this is an area particularly relevant to DPaaS research, where readability hinges on trust that preservation processes will make sure content is migrated and updated, and as well as accessible.

Trust and digital services

Writing specifically on cultural heritage institutions' relationship to digital repositories, Beagrie et al. (2002) identify a minimum of three levels of trust: how communities trust the institutions, how those institutions trust third-party service providers, and how users trust documents[5] retrieved from the repository (p. 9). Our study largely considers the second relationship, the trust of DPaaS, but as the literature reveals, this level of trust is also influenced by the perception of the institution and service provider as well as user experiences.

The relationship between trust and digital repositories started to gain attention in the 1990s. As groups such as the NDIIPP began to explore the possibilities of repositories and preservation, they also recognized the need to be able to identify reliable and trustworthy repositories and services. The RLG suggested a certification process for digital archives "to

[5] For further research on the relationship between user, repository, and digital objects, see Donaldson (2011; 2013), Donaldson and Conway (2015); and Donaldson & Fear (2011).

create an overall climate of trust about the prospects of preserving digital information" (Beagrie et al., 2002, p. 1). This interest in trust lead to the development of various audits, checklists, guidelines and standards for certifying digital repositories and services.[6]

In addition to repository certification, Donaldson (2011) suggests that document-level sanctions would increase trust in digital objects themselves, which illustrates Beagrie's third level of trust. Donaldson argues that, when it comes to the objects retrieved from a repository, there are two ways to communicate trust: through preservation metadata that highlights authenticity and reliability or by visual qualifications, like an item-level seal of approval (p. 20). Interestingly, despite the many suggestions for certifications, Donaldson notes that "little research has been conducted to understand the extent to which third-party audit and certification affect users' perceptions of trustworthiness" (2011, p. 21).

While it is obvious that great strides have been made in terms of trusting digital repositories thanks to certifications and third assessments, trust in digital preservation services is just beginning to be explored as services become available. Much like the progression of trusted digital repositories, it is expected that an institutional guarantee can positively influence trust in digital preservation services (Hart & Liu, 2003), but there are other elements that impact trust as well.

---

[6] For instance, Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) toolkit lets institutions asses their own repositories, while the Data Seal of Approval (2008) and Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist (2007) act as a formal identification of digital repositories that meet long-term, trustworthy digital stewardship guidelines. International standards have also been established to encourage trust in digital repositories. ISO 16363:2012 is a standard for assessing the trustworthiness of digital repositories, while ISO 16919:2014 delineates guidelines for those organizations utilizing standards like ISO 16363:2012 to assess and certify a repository.

Perhaps the biggest barrier to trust is the lack of familiarity with DPaaS. For institutions—especially those that preserve cultural heritage—it's hard to trust an unproven product. Beagrie et al. (2002) explains:

> Service providers gain the trust of cultural institutions through a combination of proven reliability, fulfillment of contractual responsibilities, and demonstrated sensitivity to community issues. These attributes are easily measured, however institutions are reluctant to engage the third-party digital service providers that have not proven their reliability and without demonstrated experience, the service provider cannot prove reliability. To resolve the tension between a repository's appropriately high standards and the attempts to meet the challenge, a combination of repository attributes and other criteria must be identified to foster interaction and begin to lay the foundation for trust between cultural institutions and third-party providers. (p. 9)

LeFurgy echoed the same sentiments in 2009, writing that "the perception of digital preservation as a new, untested, and unfamiliar activity reduces the confidence that funders and others may have" (p. 423). Studies by Conway and St. Jean et al. directly correlated trust and experience, noting that positive experiences between a user and a repository equated to, and in some cases increased, their trust in the repository (as cited in Donaldson, 2013, part 2.2.1). Good experiences with services can go a long way to countering these initial holdups. Through the social nature of trust, "early adopters can encourage others to explore similar services" (Franks, 2015, part II).

The source of the service provider also affects trust. Literature suggests a bias on the part of the user or institution, who seem to prefer intermediaries with a connection to their work. For example, the MetaArchive Cooperative developed a digital preservation network "in cultural memory alliances rather than corporations external to the cultural memory sphere" because

participants believed that preservation, as a core responsibility of cultural heritage institutions, should not be given to outside providers (Skinner & Halbert, 2009, p. 384). Similarly, studying scientific data and preservation relationships, Akmon, Zimmerman, Daniels, and Hedstrom (2011) noted that "archivists favored preserving the data in discipline-specific data repositories based in government scientific agencies or large laboratories," instead of finding preservation services that did not understand the content preservation and access needs of scientists (p. 332). Governmental and non-profit institutions, as well as networked partnerships also seem to have the potential to garner more trust (Hart & Liu, 2003, p. 96). In addition to its professional nature, scale is another important factor when evaluating the intermediary—there are fears that a smaller provider could go bankrupt sooner than a preservation system hosted by a larger institution (Hart & Liu, 2003, p. 96).

Distrust may also inherently exist in the current structure and presentation of digital preservation services. The "Report on Digital Preservation and Cloud Services" (2013) produced by a third-party information technology company for the Minnesota Historical Society provides an interesting case study into the needs and wants of a public archives. Included in the report are the society's desires for cloud-service preservation such as ownership reliability, integrity and accessibility of files, preservation and protection against obsolescence, disaster recovery, and security. However, many shortcomings are identified when discussing how service providers meet these needs. These limitations likely influence the ability to trust in digital preservation services. Because this report and the identified concerns are so relevant to this study, they are worth noting in their original language here:

> "Since no cloud vendors provide any data integrity guarantees, a requirement is that there be checksums generated …. These locally maintained checksums must be

periodically validated at least until MHS is confident that the cloud data integrity is assured." (p. 8)

"Though the cloud provider might state that file checksums are validated regularly, it is MHS that has the legal responsibility for the data stored with the cloud provider." (p. 20)

"One area of concern is the retention and portability policies of the cloud vendors. Some cloud vendors make it difficult, time consuming and expensive to move data from their cloud service to that of another vendor. There is also the issue of ensuring that all copies of the data have been removed once an agreement with a vendor has been terminated." (p. 8)

"Some of the vendors provide an availability (uptime) guarantee… [others] do not provide any availability guarantees, but often make marketing availability claims that they will not provide in a contract." (p.8)

"The cloud vendors have extensive documentation on security features… However, there is limited or no information on how data breaches are handled." (p. 9)

"Preservation is provided… by background integrity checks, which look for missing files and file corruption, and it is also claimed that it includes a set of tools to migrate files from obsolete formats as technology changes, but this will be difficult to accomplish if the file names and data are encrypted." (p. 9)

"Technology obsolescence is an issue that can affect both content and the metadata associated with the content; archiving systems need to provide mechanisms to monitor and transform content as needed to protect against obsolescence. ... However, this may not be feasible with the challenges of encrypted file names and data." (p. 9)

This real-world example demonstrates the search for service providers and highlights the ways trust is being counteracted in the disconnect between expectations and reality of current services' offerings.

Individual experiences also shape a user's ability to trust digital preservation. People who regularly work with digital information may not trust digital preservation for many reasons, including the inaccessibility of material, the intangible nature of digital preservation (opposed to keeping physical records), the fluidity and ease of altering digital documents, and privacy and security concerns about using a repository (Hart & Liu, 2003).

In 2011, as New Zealand began to develop a national digital archives, Oliver, Chawner, and Liu conducted a focused survey "to investigate how ICT [information and communication technology] professionals view archivists and records managers and to try to determine whether recordkeepers were perceived as having any relevance to the management of digital information" (p. 312). The team wanted to identify what would positively influence trust in a third-party digital repository.

Their research shows that an individual's trust in digital repositories happens in two ways: trust in the archivist/records manager who administers the repository, and trust in the repository and its documents. These levels of trust are influenced by individual and occupational experiences. The survey revealed that relationships play a key role in trust within work environments. While records producers and records managers may have a strong relationship with archives and repositories, digital repositories and services require working with a new cohort, ITC personnel, and the two do not have an established mutual trust (Oliver et al., 2011, p. 312). ITC personnel, who work more regularly with digital records and systems, were generally less confident in an archives' or repository's ability to preserve, and it was noted that "although

archivists were fully trusted in the management of paper records, this level of trust did not carry through automatically to digital records" (Oliver et al, 2011, p. 312).

Other aspects that were identified as positively influencing trust in a repository or service include staffs of knowledgeable IT and records management specialists and certification. Respondents also suggested the ability to ask other users of the service about their experiences and "legal parameters on access and ability to move to another provider if performance was unsatisfactory" (Oliver et. al, 2011, p. 319). The most prominent and frequently cited concern for those surveyed was the necessity of being able to retrieve and access records stored within the repository. Demonstrating this capability will go far in increasing trust.

Conclusion

Digital preservation services are too unknown to inherently encourage trust in their processes, products, or providers. Working relationships, too, will need to develop before DPaaS can be fully trusted by records creators. As digital repositories have shown, even an established service has a number of factors preventing users from using and trusting it.

The wants and needs of the public sectors targeted by our study will likely be similar to those explored in this review. Instead of further researching perceptions of trust in a preservation service or document retrieved through preservation services (parallel studies of the research presented here related to digital repositories), we propose researching the motivations of institutional decision makers—the management, records managers, and archivists that make the decision to purchase and use DPaaS—in order to better understand what can push DPaaS across the threshold from consideration to commitment.

References

About. (n.d.). *DuraSpace.* Retrieved from http://duraspace.org/about

Akmon, D., Zimmerman, A., Daniels, M., & Hedstrom, M. (2011). The application of archival concepts to a data-intensive environment: working with scientists to understand data management and preservation needs. *Archival Science*, *11*(3-4), 329-348.

Askhoj, J., Sugimoto, S., & Nagamor, M. (2011). Preserving Records in the Cloud. *Records Management Journal, 21*(3): 175-187. doi: 10.1108/09565691111186858.

Beagrie, N., Bellinger, M., Dale, R., Doerr, M., Hedstrom, M., Jones, M., . . . Woodyard, D. (2002). Trusted Digital Repositories: Attributes and Responsibilities. *Research Libraries Group & Online Computer Library Center, Report.* Retrieved from http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

Belanche, D., Casaló, L. V., Flavián, C., & Schepers, J. (2014). Trust transfer in the continued usage of public e-services. *Information & Management*, *51*(6), 627-640.

Brown, A., Katuu, S., Sebina, P. and Seles, A. (2009). "Module 4: Preserving Electronic Records", London: International Records Management Trust. Retrieved from http://www.irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Module%204.pdf

Chan, L. (2004). Supporting and Enhancing Scholarship in the Digital Age: The Role of Open-Access Institutional Repositories. *Canadian Journal of Communication, 29*(3): 277-300. Retrieved from http://cjc-online.ca/index.php/journal/article/viewArticle/1455

Cruse, P., and Sandore, B. (2009). Introduction: The Library of Congress National Digital Information Infrastructure and Preservation Program. *Library Trends*, *57*(3), 301-314. Doi: 10.1353/lib.0.0055

Dale, R. L., & Gore, E. B. (2010). Process Models and the Development of Trustworthy Digital Repositories. *Information Standards Quarterly*, *22*(2), 14-19.

Davis, P. M., & Connolly, M. J. L. (2007). Institutional repositories: evaluating the reasons for non-use of Cornell University's installation of DSpace. *D-lib Magazine*, *13*(3). Retrieved from http://www.dlib.org/dlib/march07/davis/03davis.html

Digital Preservation as a Service. (2016). National Library of New Zealand. Retrieved from https://diaarchivesndha.cwp.govt.nz/current-initiatives/dpaas/

Dollar, C. M., & Ashley, L. J. (2013). Long Term Digital Preservation. In Smallwood, R. F. (Ed.), *Managing electronic records: Methods, best practices, and technologies* (p. 285 - 315): Somerset, N.J.: John Wiley & Sons.

Donaldson, D. R. (2011). Users' Trust in Trusted Digital Repository Content, *8th International Conference on the Preservation of Digital Objects* (iPres'2011), Singapore, November 2011, 20-23.

Donaldson, D. R. (2013). Measuring Perceptions of Trustworthiness: A Research Project, *10th International Conference on the Preservation of Digital Objects* (iPres'2013), Lisbon, Portugal, September, 2013, 88-94.

Donaldson, D. R., and Conway, P. (2015). User Conceptions of Trustworthiness for Digital Archival Documents, *Journal of the Association for Information Science and Technology*, 66(12), pp. 2427-2444.

Donaldson, D. R., and Fear, K. (2011). Provenance, End-User Trust, and Reuse: An Empirical Investigation, Proceedings of *3rd Workshop on the Theory and Practice of Provenance* (TaPP'2011) Heraklion, Crete, Greece, June 2011.

FAQ. (n.d.). *Portico*. Retrieved from http://www.portico.org/digital-preservation/about-

us/about-usfaq

Foster, N. F., & Gibbons, S. (2005). Understanding Faculty to Improve Content Recruitment for Institutional Repositories. *D-Lib Magazine, 11*(1). Retrieved from http://www.dlib.org/dlib/january05/foster/01foster.html

Franks, P. C. (2015). Government use of cloud-based long term digital preservation as a service: An exploratory study. In *2015 Digital Heritage* (Vol. 2). IEEE.

Fresa, A., Justrell, B., & Prandoni, C. (2015). "Digital curation and quality standards for memory institutions: PREFORMA research project." *Archival Science, 15*(2). Retrieved from http://dx.doi.org/10.1007/s10502-015-9242-8

Halas, H., Porekar, J., Klobučar, T., & Blažič, A. J. (2008). "Organizational aspect of trusted legally valid long-term electronic archive solution." *WSEAS Transactions on Information Science and Applications*, *5*(6), 939-948. Retrieved from http://moreq2.eu/attachments/article/330/Organisational%20aspects%20-%20Slovenian%20paper.pdf

Hart, P. E., & Liu, Z. (2003). Trust in the preservation of digital information. *Communications of the ACM*, *46*(6), 93-97.

Hedstrom, M., & Niu, J. (2008). Incentives for data producers to create "archive/ready" data: Implications for archives and records management. In *Proceedings from the Society of American Archivists Research Forum.*

Hill, R., and Donaldson, D. R. (2015). Bridging the Trust Gap: Integrating Models of Behavior and Perception, New Security Paradigms Workshop (NSPW'2015), Twente, The Netherlands, September, 2015.

Home. (n.d.). PREFORMA. Retrieved from http://www.preforma-project.eu/

Instrumental, Inc. (2013). Report on Digital Preservation and Cloud Services. St. Paul, MN.

Retrieved from http://www.mnhs.org/preserve/records/docs_pdfs/Instrumental_MHSReportFinal_Public_v2.pdf

Knight, S. (2015). Digital preservation as a service. National Library of New Zealand. Retrieved from https://natlib.govt.nz/blog/posts/digital-preservation-as-a-service

Lavoie, B. F. (2003). *The incentives to preserve digital materials: Roles, scenarios, and economic decision-making*. OCLC Online Computer Library Center.

LeFurgy, W. G. (2009). NDIIPP partner perspectives on economic sustainability. *Library Trends*, *57*(3), 413-426. doi: 10.1353/lib.0.0044

Leverich, M., Nalliah, K., & Suderman, J. (2015). Historical Study of Cloud-Based Services (final). InterPARES Trust. Retrieved from https://InterPAREStrust.org/trust/about_research/studies

Library of Congress. (2002a). Preserving our digital heritage: Plan for the national digital information infrastructure and preservation program. Retrieved from http://www.digitalpreservation.gov/documents/ndiipp_plan.pdf

Library of Congress. (2002b). Preserving our digital heritage: Plan for the national digital information infrastructure and preservation program: Appendices. Retrieved from http://www.digitalpreservation.gov/multimedia/documents/ndiipp_appendix.pdf

Library of Congress. (2010). Preserving our digital heritage: Plan for the national digital information infrastructure and preservation program: 2010 report. Retrieved from http://www.digitalpreservation.gov/documents/NDIIPP2010Report_Post.pdf

Nguyen, Q. L., & Lake, A. (2011). Content server system architecture for providing differentiated levels of service in a digital preservation cloud. *2011 IEEE International Conference on Cloud Computing (CLOUD)*: 557-564.

Oliver, G., Chawner, B., & Liu, H. P. (2011). Implementing digital archives: issues of trust. *Archival Science*, *11*(3-4), 311-327.

Research Studies. (n.d.). InterPARES Trust. Retrieved from https://InterPAREStrust.org/trust/about_research/studies

Skinner, K. & Halbert, M. (2009). "The MetaArchive Cooperative: A Collaborative Approach to Distributed Digital Preservation." *Library Trends, 57*(3): 371-392. doi: 10.1353/lib.0.0042

Trust in Data Archives: A Social Science Perspective. (n.d.). UK Data Archive. Retrieved from http://www.data-archive.ac.uk/curate/trusted-digital-repositories/trust-in-data-archives