The Social Construction of Risk in Digital Preservation

Rebecca D. Frank

Note: This paper was published in the Journal of the Association for Information Science and Technology. Please cite the published version.

DOI: 10.1002/asi.24247

ABSTRACT

Digital information is fragile, yet access to digital information over time is a critical underpinning of core values and functions in our society, from open government to research and scholarship. Digital preservation research has focused on identifying technical, economic, and organizational sources of risk and has relied on an assumption that individuals will behave in rational and predictable ways in response to the same information. This article asserts that viewing digital preservation as a process that takes place in complex social contexts is just as important as thinking about digital preservation in terms of technological or economic issues. This is particularly important for understanding how individuals involved in digital preservation construct their understanding of risk because social factors influence how people construct their understanding of, and behave in response to, risk information. The author proposes an eight-factor model for the social construction of risk, which includes: communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability. The article demonstrates how these factors influence individuals as they construct their understanding of risk in the context of digital preservation and how this in turn affects digital preservation decisions.

The Social Construction of Risk in Digital Preservation

Rebecca D. Frank, PhD
University of Michigan School of Information, 4322 North Quad, 105 S. State Street, Ann Arbor, MI 48109-1285. E-mail: frankrd@umich.edu

Digital information is fragile, yet access to digital information over time is a critical underpinning of core values and functions in our society, from open government to research and scholarship. Digital preservation research has focused on identifying technical, economic, and organizational sources of risk and has relied on an assumption that individuals will behave in rational and predictable ways in response to the same information. This article asserts that viewing digital preservation as a process that takes place in complex social contexts is just as important as thinking about digital preservation in terms of technological or economic issues. This is particularly important for understanding how individuals involved in digital preservation construct their understanding of risk because social factors influence how people construct their understanding of, and behave in response to, risk information. The author proposes an eight-factor model for the social construction of risk, which includes: communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability. The article demonstrates how these factors influence individuals as they construct their understanding of risk in the context of digital preservation and how this in turn affects digital preservation decisions.

Introduction

Access to digital information is a critical underpinning of core values and functions in our society, from open government, to individual rights, to research and scholarship. The creation of this digital content often represents a substantial investment of time and resources. For example, every year the National Science Foundation (NSF) spends billions of dollars on research. In 2017 the NSF had a budget of ~$7.5 billion and supported the work of 359,000 people (The National Science Foundation, 2018). Since 2011 the NSF has required that all proposals include data management plans including information about plans to deposit data with a repository in order to ensure that they will be disseminated and preserved (National Science Foundation, 2011). Despite these efforts to ensure the longevity of this valuable digital information, it remains fragile:

> Gone is the promise of preserving knowledge forever. We are replacing books, maps, and audiovisual recordings with computer code that is less stable than human memory itself. Code is rapidly overwritten or rendered obsolete by new code. Digital data are completely dependent on machines to render them accessible to human perception. In turn, those machines are completely dependent on uninterrupted supplies of energy to run the server farms that store and serve digital data. (Smith Rumsey, 2016, p. 8)

Digital preservation is about ensuring the viability, sustainability, and accessibility of that digital information over time (Berman, 2008). In order to accomplish this, information researchers and professionals have taken an approach to digital preservation that focuses on identifying and assessing risks in order to create and implement risk mitigation strategies and systems that will ensure the viability, sustainability, and accessibility of digital information over time (for instance, Barateiro, Antunes, Freitas, & Borbinha, 2010; Berman, 2008). Indeed, risk management has been considered a conceptual foundation for digital preservation for more than 20 years (Conway, 1996).

Approaches that consider digital preservation as risk management depend upon the ability of people and organizations to accurately and effectively assess risk. While some of the risks associated with digital preservation activities, such as media deterioration and file format obsolescence (for instance, Ohshima, 2010), storage failures (for instance, Vermaaten, Lavoie, & Caplan, 2012), and disasters, attacks, and economic failures (for instance, Barateiro et al., 2010), are known and understood, we know that even when risks are known people are generally poor at judging how to act in response to those risks (Kahneman, 2013). This poor judgment is based in part on the fact that risk is socially constructed and different actors have differing perceptions of risk.

In this article I assert that risk in digital preservation is a socially constructed phenomenon and propose a model for the

Received September 27, 2017; revised February 23, 2019; accepted April 14, 2019

 DOI: 10.1002/asi.24247

social construction of risk in digital preservation that builds on existing research to argue that digital preservation is a process in which social and technical elements interact within organizations and institutions to shape the perceptions of individuals and groups who carry out the work of preserving digital content (for instance, Conway, 2010; Hughes, 2012; MacKenzie, 2012). I argue that sources of risk in digital preservation cannot be considered as merely technical, economic, or organizational. Rather, digital preservation is also a social process in which risks are interpreted by individuals who exist and work within particular cultural contexts (Burgess, 2015). Their subsequent actions are influenced by social factors that shape their perception. In other words, people construct their understanding of risk based on a number of social factors, and individuals may behave differently in response to the same information depending on how they construct their understanding of risk.

A Model for the Social Construction of Risk in Digital Preservation

In the section below I present a model for the social construction of risk in digital preservation. The section begins with a discussion of risk, which is a foundational concept for both digital preservation and this model. Following that, I describe each of the eight factors that comprise the model.

Risk

This model is based on an understanding of risk as a concept that is constructed through social processes and situated within particular social contexts (Burgess, 2015). Risks, from this perspective, "are created and selected by human actors" (Renn, 2008, p. 11). The concept of risk can therefore have different meanings for different people (Slovic, 1987), and the ways in which those people construct their understanding of risk are influenced by social factors (for instance, Dake, 1992; Renn, 2008; Wilkinson, 2001). While I agree with researchers such as Conway (1996) that risk management is foundational for digital preservation, I argue here that risk should be understood as a socially constructed phenomenon. Approaches that consider risk primarily as a calculable, discoverable value (for instance, International Organization for Standardization, 2009; International Organization for Standardization Technical Committee, 2018) assume that people will respond to information in the same way, and are not sufficient to account for the ways in which social factors and circumstances influence how people construct their understanding of risk in digital preservation.

A classical definition of risk from the Royal Society includes elements that are common across the literature from a variety of disciplines: an adverse event or hazard, and the likelihood of that event (Royal Society (Great Britain) & Study Group on Risk, 1983). While this report describes risk as the probability of some adverse event, other definitions include the magnitude of consequences of an adverse event: "[r]*isk* is the combination of the likelihood of an event and the consequences of that event" (Leveson, Dulac, Marais, & Carroll, 2009, p. 230). Taking this definition one step further, additional research has established the importance of causation "[d]efinitions of particular risks include at least three conceptual elements: an *object* deemed to 'pose' the risk, a putative *harm*, and a *linkage* alleging some form of causation between the object and the harm" (Hilgartner, 1992, p. 40).

Similarly, ISO 31000, a standard for Risk Management, describes risk as the effect of uncertainty on objectives, and specifies that risk typically includes a source, an event, and the consequences and likelihood of that event (International Organization for Standardization Technical Committee, 2018). This standard describes risk management as "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities" (International Organization for Standardization Technical Committee, 2018, p. 2). While the view of risk presented here does specify a relationship between risk and uncertainty, it assumes that people will behave predictably in response to the same information.

As these examples demonstrate, risk is generally described as some combination of probability and magnitude of consequence relating to a hazard or adverse event (for instance, Gardoni & Murphy, 2013; Kaplan & Garrick, 1981; Rowe, 1977). The assumption here is that both probability and magnitude can be reduced to measurable, calculable quantities (for instance, Fischhoff, 1983). These definitions of risk rely upon the concept of a rational actor, and fail to take into account the idea that social factors might influence the way that individuals perceive and construct their understanding of risk:

> The classical risk approach assumes that it is possible to define and assess risks. The assumption that risks can be objectified and calculated has met with a lot of criticism. Notions like complexity and uncertainty to characterize the risk situation have played a central role in clarifying the limits of the classical risk approach. (van Est, Walhout, & Brom, 2012, p. 1075).

In contrast to this classical definition of risk, scholars across a variety of disciplines have found that "risks are created and selected by human actors" (Renn, 2008, p. 11). And, given the fact that risks are fundamentally human creations, Renn (2008) defines risk perception as "the outcome of processing, assimilation and evaluation of personal experiences or information about risk by individuals or groups in society" (p. 64). In this view, "the concept 'risk' means different things to different people" (Slovic, 1987, p. 283).

Some interpretations of social construction acknowledge objective conditions, and link perception to those conditions. In other words, a constructivist view of risk in digital preservation is not inconsistent with a classical definition of risk, but rather shows that this classical view represents an incomplete picture of risk, as it does not account for the ways in which people construct their own understanding or perception of risk in response to the information that comprises that classical definition (for instance, object, hazard, likelihood, and consequences). Theories of risk perception, in contrast, hold that people construct

DOI: 10.1002/asi

differing understandings of the probability and adverse consequences of events, that these differing understandings are the result of social, organizational, and/or political factors, and that they shape the ways in which people behave in response to risk information (Lachlan, Burke, Spence, & Griffin, 2009; Nelkin, 1989; Nickel & Vaesen, 2012; van Est et al., 2012; Wildavsky & Dake, 1990).

Digital preservation as an academic discipline has engaged with the concept of risk as a knowable, quantifiable figure that technical systems must be designed to overcome (for instance, Barateiro et al., 2010). This approach to digital preservation relies on positivistic perspectives and is heavily influenced by computer science (for instance, Barateiro, Antunes, & Borbinha, 2011). Digital preservation scholarship addressing the concept of risk consists mainly of identifying and classifying types of vulnerabilities or threats, and individual case studies describing actions taken by a particular repository (for instance, Vermaaten et al., 2012). The literature in this area, which consists largely of self-produced case studies about specific organizations, treats risk as an objective value and does not engage meaningfully with the notion that perceptions of risk, rather than the risk itself, drive decision-making and action with regard to digital preservation (Ross & McHugh, 2006). These positivistic attitudes about risk in digital preservation form the basis for an underlying assumption among many digital preservation researchers and practitioners: that the stakeholders involved in digital preservation processes have the same perceptions of risk and therefore interpret risk information in the same way.

The model below represents an analytical framework of risk that is based on a definition of risk as a socially constructed phenomenon and draws on eight social factors that influence how people and groups construct their understandings of risk: communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability. Each of these factors is examined in greater detail below (Figure 1).

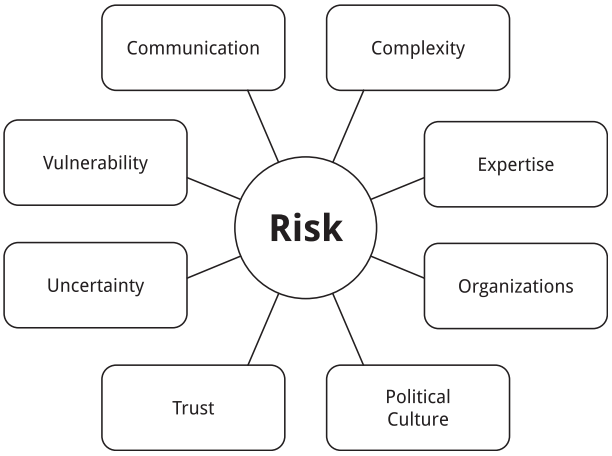

FIG. 1. Model for the social construction of risk in digital preservation.

Communication

The way that risk information is communicated influences the manner in which an individual constructs his or her understanding of risk (Bostrom, 2014; Chung, 2011; Kasperson & Kasperson, 1996; Konheim, 1988; Lachlan et al., 2009; Renn, 1991; Renn, Burns, Kasperson, Kasperson, & Slovic, 1992). Theories of risk amplification and attenuation argue that communication provides a lens through which individuals receive risk information, and that perceptions of risk vary depending on a number of factors, including the source, method, channel, and means of communication (for instance, Bostrom, 2014; Kasperson & Kasperson, 1996). Indeed, "social interactions may either amplify or attenuate the signals to society about the risk" (Kasperson & Kasperson, 1996, p. 96). Information about risk can be communicated in different ways and those different means of communication, in turn, influence information processing and interpretation.

The amplification (or attenuation) of risk information can take place in a myriad of ways, and can involve many different types of actors and organizations, including media, government, political actors, scientists, or other experts (Arvai, 2007; Kasperson & Kasperson, 1996; Lachlan et al., 2009). Different individuals, if given the same risk information from the same source, will not necessarily perceive risks in the same way, and so it is important to consider both the audience and the mode of communication any time risk information is communicated (Arvai, 2007).

Understanding how communication can influence perceptions of risk is important for digital preservation, a sociotechnical process in which individuals within digital repositories work together to assess and mitigate risk. Furthermore, "[r]isk analysis, then, requires an approach that is capable of illuminating risk in its full complexity, is sensitive to the social settings in which risk occurs, and also recognizes that social interactions may either amplify or attenuate the signals to society about risk" (Kasperson & Kasperson, 1996, p. 96). Risk analysis and/or mitigation processes can have unintended consequences on risk perception that arise not from the information itself but rather from the social factors surrounding the risk, the assessment process, and the ways in which all of those things are communicated. Risk perception can be amplified or attenuated as a result of the ways that technical information about risk is communicated.

To summarize, the transmission of risk information from an information source to a receiver influences the way in which that information is received, and "messages have a meaning for the receiver only within a sociocultural context" (Kasperson et al., 1988, p. 180). In the context of digital preservation, for example, risk information can be communicated to and/or from digital repository staff and administrators; other repository stakeholders such as users, content creators, and designated community members; and external parties such as partner organizations. Professional discourse around digital preservation may also influence perceptions of risk for different types of stakeholders depending on their

DOI: 10.1002/asi

connections to the digital preservation community, and the ways in which the communication norms of this community either match or diverge from the communication norms of their own professional communities.

Complexity

The second factor, complexity, has also been found to influence risk perception. Research shows that high levels of complexity in technical and social systems can make it difficult to identify probabilities, consequences, and hazards (Fischhoff, 1983; Perrow, 1999; Rijpma, 1997; van Est et al., 2012). van Est et al., (2012) argue that "the interactions of humans and/or technological subsystems are much more complex than an a priori risk assignment can capture" (p. 1076).

Perrow (1999) and Rijpma (1997) in particular have argued that complexity results in interaction between seemingly independent features within sociotechnical systems, and this complexity may neutralize the benefits of redundancy and impair organizational learning. In other words, complexity introduces problems while also counteracting measures that are meant to offset those problems. This research indicates that perceptions of risk can be influenced by the complexity of sociotechnical systems, which suggests that the differing levels of complexity of digital repositories and in the organizations within which they are situated may lead to varying perceptions of risk for different stakeholders, depending on their level of familiarity with different aspects of the repository. Other types of complexity might be present in processes such as content ingest, curation, and managing relationships with repository stakeholders.

Repository staff face complexity in managing digital preservation processes, which include complicated technical systems and complex arrangements of people, policies and procedures, and technologies, and also in terms of organizational and economic factors relating to the repository. They may have differing perspectives on these complexities depending on their backgrounds, and their roles within the repository. External actors, such as designated community members, auditors, or funding agencies, may understand risk for a repository differently, depending on the complexity of the repository environment, and the complexity of their own organization. For example, repositories that are positioned within larger organizations such as universities, consortia, or partnerships are likely to have complex governance structures that may heighten or minimize risks relating to organizational governance for repository staff members and/or organizational administrators.

People who are not directly involved in digital preservation activities may also view repositories differently, depending on how complexity is communicated, because documentation efforts by repository staff that attempt to make repository processes comprehensible through simplification may in fact mask the underlying complexity that external parties seek to understand. Indeed, Wilkinson argues that "[a]ny attempt to mask the complexity of the social experience of risk perception in rigid conceptual abstractions may lead us further away, rather than towards a more intimate understanding of the day-to-day reality in which people recognize and negotiate with 'hazards' as 'risks'" (Wilkinson, 2001, p. 11).

In short, high levels of complexity in technical and social systems can make it difficult to identify probabilities, consequences, and hazards (for instance, Fischhoff, 1983; Perrow, 1999; Rijpma, 1997; van Est et al., 2012). The differing levels of complexity of digital repositories, and of the organizations within which they are situated, may lead to varying perceptions of risk for different stakeholders depending on their level of familiarity with different aspects of the repository and/or digital preservation processes.

Expertise

The third factor included in this model is expertise. A great deal of literature about the social construction of risk focuses on the differences between experts and nonexperts (for instance, Douglas & Wildavsky, 1982; Hilgartner, 1992; Kasperson & Kasperson, 1996; Konheim, 1988; Perrow, 1999; Slovic, 1987; Tversky & Kahneman, 1974; Vaughan & Seifert, 1992; Wildavsky & Dake, 1990; Wynne, 1992). It was previously thought that experts had more accurate understandings of risk because they had greater levels of knowledge about the factors that contribute to risk, and that their understanding of risk was more objective and/or rational than that of nonexperts (for instance, Otway, 1992; Starr, 1969; Wynne, 1992).

However, as researchers have developed a deeper understanding of the ways that experts and nonexperts differ in constructing understandings of risk, research has come to support the idea that risk assessment and management efforts should include both perspectives:

> [p]erhaps the most important message from this research is that there is wisdom as well as error in public attitudes and perceptions. Lay people sometimes lack certain information about hazards. However, their basic conceptualization of risk is much richer than that of the experts and reflects legitimate concerns that are typically omitted from expert risk assessments. (Slovic, 1987, p. 285)

Research has found that the distinction between experts and lay people, or nonexperts, is misguided, and that individuals with different experiences and types of knowledge bring different types of expertise to bear on assessments of risk (Pidgeon, 1998). Rather than a clear division between experts and nonexperts, a digital repository consists of people with varying levels of expertise in different aspects of the repository. Broadly speaking, repositories typically consist of people with administrative expertise, digital preservation expertise, and information technology (IT) expertise, and each of these types of people are involved in the work of preserving digital content. Each of these types of people has deep, focused knowledge in some areas of repository management but may be considered a novice with regard to others. This knowledge, paired with a lack of similar expertise in other areas of repository management, has the potential to influence perceptions of

DOI: 10.1002/asi

risk by opening their eyes to some types of risk and closing them to others.

With regard to digital preservation, these varying levels of expertise may influence attitudes about risk differently, depending on how involved each person is in particular aspects of preservation and repository management, and on how much they rely on and trust the expertise of others, or the perspectives of those who lack the familiarity of experts.

In summary, "experts are often in a privileged position in terms of information, even if their values and decision processes are not always employed optimally. On the other hand, while non-experts may not possess as much relevant factual information, they may be in a position to augment expert risk analyses with additional useful information" (Pidgeon, 1998, p. 12). In order to understand how risk is constructed in digital preservation, it is important to consider the role of expertise both in terms of the information and experience that different people and groups possess, as well as how they perceive the expertise of others.

Organizations

The fourth factor in the model is organizations. Organizations are "both centres for processing and handling risks and potential producers and exporters of risk" (Hutter & Power, 2005, p. 1). Hutter and Power (2005) argue that risk analysis and risk management are both activities that take place within organizations, and that these activities rely on social constructions of risk knowledge that are framed within the structure of the organization. Alternately, rather than constructing a shared perception of risk for all members, individuals within an organization may perceive risk differently depending on their roles (Hutter, 2005).

Most formal risk assessment and management takes place within organizations; "[i]f selection of risk is a matter of social organization, the management of risk is an organizational problem" (Douglas & Wildavsky, 1982, p. 198). The ways that the organization and/or its members might share, or have differing perceptions of, risk can influence the outcome of the risk assessment or management activities (Hutter, 2005; for instance, Hutter & Power, 2005; Renn, 2008; Vaughan, 1996, 2005). Similarly, outcomes can be affected by whether the individuals conducting the assessment are a part of the organization or if they are outsiders, as this will also influence their likelihood of sharing the risk perception of the organization being assessed (Vaughan, 1996).

For digital preservation, each repository is a separate organization that may shape perceptions of risk for its members in different ways. In some cases repositories themselves consist of separate organizations, which have joined together for a common purpose. External actors such as designated community members also belong to organizations that may shape their perceptions of risk in ways that differ from the repository staff members. It is possible that individuals or groups will have varying perceptions of risk based on their positions within their own organizations, in a manner similar to the influence of expertise as described above. Position within an organization is, in some cases, related to expertise because people are likely to be situated within groups based on their expertise (for instance, IT, digital preservation, and so on). However, lines of communication within organizations do not always follow these functional lines. Organizations with matrix reporting structures, for example, may influence perceptions of risk in different ways than more traditional or siloed organizations.

Organizations, in short, can both create and manage risk. People construct their understanding of risk in ways that are shaped by their positions in, and/or relationships with, organizations. Complexity, communication, and expertise are all closely related to the organizational context in which the work of digital preservation takes place, and can shape the ways in which people perceive and construct their understanding of risk.

Political Culture

Political culture and national context influence how risks are defined (Beck, 1992; Jasanoff, 1986; Parthasarathy, 2007). Dake (1991) argues that "mental models of risk are not solely matters of individual cognition, but also correspond to *worldviews* entailing deeply held beliefs and values regarding society, its functioning, and its potential fate" (p. 62). This argument is based on the assumption that individuals exist within social, cultural, and political spheres, that they perceive risks within those contexts, and that their perceptions of risks are influenced by those contexts (Dake, 1991). Indeed, Parthasarathy (2007) argues that political culture shapes practices and artifacts in ways that vary across political boundaries, and that the differences among political cultures can explain some of the challenges to transnational technology transfer.

Perceptions of risk are constructed and shaped not only by the political culture within which individuals exist, but also by their place or role within that culture (Beck, 1992). For Beck (1992, 1999), relative power within political culture influences perceptions of risk in that individuals, organizations, or groups with greater power are able to reduce their exposure to risk. Much like theories of vulnerability described below, risk perception depends in part on whether an individual has control over their own level of exposure to risk.

In addition to the fact that political culture shapes perceptions of risk, Jasanoff (1998) contends that, "[t]heories of risk perception are inherently political because they carry within them implicit understandings about how to organize and implement policies for managing risk … people's attitudes toward risk partly reflect their feelings of power, or lack thereof, in relation to the sources of risk" (p. 93). Individuals perceive risks within their own cultural and political context, and it is within this same context that decisions about how to respond to those risks are formulated and implemented.

To summarize, research about risk and political culture has shown that individuals perceive risks within their own cultural and political context, and it is within this same

DOI: 10.1002/asi

context that decisions about how to respond to those risks are formulated and implemented (for instance, Dake, 1991; Jasanoff, 1986, 1998; Parthasarathy, 2007). Additionally, attitudes about risk reflect feelings of power, or lack of power, in relation to potential sources of risk (Jasanoff, 1998). In the case of digital preservation, repository managers may be influenced in their perceptions of risk by political events such as the defunding of heritage organizations on a national scale (for instance, CBC News, 2012). Individuals involved in repository audit processes may have different understandings of risk, depending on their positions and feelings of power within their own organizations and on their feelings of power between their organizations. For example, repository staff may view threats as more risky if they feel that they lack the power or authority to enact risk mitigation strategies.

Trust

Trust, the sixth factor included in this model, influences how people construct their understanding of risk. Wynne, for example, argued that "public experiences of risks, risk communications, or any other scientific information is never, and can never be, a purely intellectual process, about reception of knowledge *per se*" (1992, p. 281). Rather, "the trustworthiness and credibility of the social institutions concerned are basic to people's definitions of risks" (1992, p. 300). Information about risks cannot be separated from its context, but rather is informed by the norms around knowledge production within communities.

Similarly, Wildavsky and Dake (1990) found that "the great struggles over the perceived dangers of technology in our time are essentially about trust and distrust of societal institutions, that is, about cultural conflict" and that "risk perceptions and preferences are predictable given individual differences in cultural biases" (1990, pp. 56, 57). Nelkin argued that not only does trust affect perceptions of risk, but that trust (or mistrust) can be a guiding factor in how risk is defined: "[d]efining risk can become a way of explaining the failure of existing political or social relationships, of voicing mistrust, of delegating blame" (Nelkin, 1989, p. 98). Findings from Wynne (1992), Wildavsky and Dake (1990), and Nelkin (1989) indicate that relationships exist between individuals and institutions, and among people with different types of expertise, and that trust is an important factor in these relationships. Lack of trust both influences and can be influenced by risk perception, and can impact efforts to assess and manage risk.

In the domain of digital preservation, discussions about trust have focused on online environments (for instance, Berman, 2008; Colati & Colati, 2009; Corritore, Kracher, & Wiedenbeck, 2003; De Santis, Scannapieco, & Catarci, 2003; Dryden, 2011; Kelton, Fleischmann, & Wallace, 2008; MacNeil, 2000; Mutula, 2011; Yakel, Faniel, Kriesberg, & Yoon, 2013; Yoon, 2014, 2016), and also on the development of criteria for the evaluation of digital repositories (for instance, Becker & Rauber, 2011; Day, 2008; RLG-NARA Digital Repository Certification Task Force, 2007). This scholarship relies upon the idea that "[t]rust is instrumental for the preservation of digital media" (Hart & Liu, 2003, p. 95). Given that trust is necessary for the preservation of digital information, and that this preservation frequently takes place in digital repositories, we must consider how trust is conceptualized for digital repositories. Jantz and Giarlo (2007) note that digital repositories are unique among the various types of digital organizations (such as for-profit businesses conducting e-commerce), and as such "for the digital repository, trust involves scholarship, authenticity, reliability, and persistence over time and has little relationship to immediate financial rewards" (2007, p. 197).

This line of inquiry—scholarship about digital preservation and trust—leads to the concept of the trustworthy digital repository (TDR). While there are several different standards for TDRs (for instance, ISO 16363, CoreTrustSeal, nestor, and so on), common elements of these standards include a commitment to providing reliable long-term access to digital information, the ability to assess and mitigate risks, and the desirability that repositories demonstrate that they are able to do so (for instance, Consultative Committee for Space Data Systems, 2012; Dale & Gore, 2010; Dillo & De Leeuw, 2018; Keitel, 2012; McHugh, Ross, Innocenti, Ruusalepp, & Hoffman, 2008).

In sum, information about risk cannot be separated from the context in which it exists. Trust (or mistrust) is an important factor in the relationships between individuals and institutions, and can be a guiding influence in how risk is defined (Nelkin, 1989; Wynne, 1992). The work of preserving digital information frequently takes place in organizations such as digital repositories, and trust among the individuals, groups, and/or institutions involved in the work of preserving digital content can shape how people construct their understanding and perceptions of risk. For example, risk assessment and management activities such as those required for TDR certification depend upon stakeholders in those activities having trust in others.

Uncertainty

Seventh, uncertainty has been identified as a factor that influences how individuals perceive and understand risks (for instance, Starr, 2003; Tversky & Kahneman, 1974; van Est et al., 2012). Scholars have characterized risk calculations that take place under conditions of both speculation and ignorance as representing uncertainty about either the probability or magnitude of the consequences of an event (Starr, 2003; van Est et al., 2012). Tversky and Kahneman argued that people rely on heuristic principles when making decisions under conditions of uncertainty, and that these heuristics can lead to "severe and systematic errors" (1974, p. 1124).

More recently, scholars have argued that the dichotomy between probability and magnitude is flawed and that it is more productive to talk about risks themselves as uncertain rather than uncertainty in particular elements of risk: "current risk assessment is mostly future-oriented. The basis for

DOI: 10.1002/asi

risk assessment, therefore, has shifted from probability, based on experience in the past, to possibility, based on expectations about the future" (van Est et al., 2012, p. 1077). In this view, probability and magnitude cannot really be separated when considering uncertainty for risk. Rather, these elements combine to make risks themselves uncertain.

The research described above indicates that perceptions of risk can be influenced by the existence and/or recognition of uncertainty. Uncertainty affects different types of people in different ways, as levels of expertise or knowledge about particular events, systems, or risks can influence the degree of uncertainty that a given person perceives. Uncertainty may influence digital preservation activities because people involved in the work of preserving digital content are likely to face uncertainty in a variety of areas such as organizational stability and funding.

Vulnerability

Finally, risk perception may also be influenced by factors that heighten vulnerability or risk exposure, such as gender or socioeconomic status. Research in this area argues that lived experience, including exposure or vulnerability to risk, can influence risk perception (Konheim, 1988; Olofsson et al., 2014). In an article seeking to expand risk perception research in the area of gender differences, Hitchcock (2001) makes the point that people who benefit less from high-risk technology, and who lack control over their own exposure to those technologies, live in a more dangerous or risky world than people who benefit from these technologies or who are able to limit their own exposure to them. Another study that focused on gender, race, and risk perception with regard to environmental risks concluded that, "perhaps women and nonwhite men see the world as more dangerous because they benefit less from many of its technologies and institutions, and because they have less power and control" (Flynn, Slovic, & Mertz, 1994, p. 1107).

Those researchers argue that groups of people who lack privilege may face greater exposure to risks, and that this exposure may be thought of as independent of will or choice. When viewed alongside Starr's (1969) findings that "the public is willing to accept 'voluntary' risks roughly 1,000 times greater than 'involuntary' risks," this suggests that risk perception will fluctuate as privilege and the ability to control one's risk exposure varies (p. 1237). Individuals who lack the ability to control their environment, and who do not benefit from the sources of risk, may perceive greater risk in any given situation than individuals who occupy positions of relatively greater privilege. In other words, choice matters, and the ability to choose one's risk exposure influences how much risk a person is willing to accept in any given situation.

Understanding how vulnerability can influence risk perception is important for digital preservation because individuals involved in preserving digital content have varying levels of control over the decisions made for their organizations, and therefore experience vulnerability to external factors (based on location, financial resources, and so on) differently. For example, decisions about the geographic location of primary and backup storage sites are made for many different reasons, some practical and some political. Repository staff may have different perceptions of risk depending on their own involvement in the selection of sites. Similarly, staff members of repositories that lack economic security (for instance, heavy reliance on "soft money") may also have different perceptions of risk than repositories with more financial stability. Perceptions of risk may vary between repository staff and external actors, as awareness of vulnerability (external actors) and exposure to risk (repository staff) do not influence perceptions of risk to the same degree (Starr, 1969).

To summarize, research has shown that lived experience, including exposure or vulnerability to risk, can influence risk perception (for instance, Konheim, 1988; Olofsson et al., 2014). This view of risk perception corresponds to the section about organizations above, which argues that vulnerability and privilege can affect risk perception—because different roles within an organization have varying amounts of perceived and real power, control, vulnerability, and exposure to risk. People and groups who experience greater vulnerability are likely to perceive greater risk than those in positions of relative power and/or privilege. Those involved in the work of preserving digital content may perceive greater risk to the content because of their knowledge about vulnerabilities, or because of their own personal or professional vulnerability within their organization.

The elements described above represent eight social factors that have the potential to influence how notions of risk are constructed in digital preservation: communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability. In the following section I will discuss this model in the context of TDR certification in order to provide an example that illustrates how social factors influence perceptions of risk in a digital preservation context. This example also highlights the fact that the factors in this model are interconnected, and have the potential to increase or lessen perceptions of risk where they intersect.

Discussion

In this article I have described a new framework to critically examine risk in digital preservation as a socially constructed phenomenon. This approach, which is informed by the large body of research on the social construction of risk and risk perception, considers the potential influence of social factors on the actors who carry out digital preservation activities. This model builds upon previous research about risk in digital preservation (for instance, Barateiro et al., 2010; Conway, 1996; Vermaaten et al., 2012), and invites scholars to move beyond a classical view of risk to consider not only the probability and likelihood of a threat or hazard (for instance, International Organization for Standardization, 2009; International Organization for Standardization Technical Committee, 2018), but also to acknowledge that social factors influence how people construct their understanding of risk in digital preservation.

DOI: 10.1002/asi

Research about digital preservation has tended to treat risk as a discoverable and calculable figure. However, risk is a foundational concept of digital preservation and a view of risk that does not consider the ways that social factors have been shown to influence how people perceive and understand risk will be incomplete. What is needed is a shift in understanding toward an approach that considers the social context in which digital preservation activities take place, in order to understand not just the likelihood and consequences of a hazard, but also how people perceive and behave in response to risk information.

In order to illustrate how each of the factors contributes to the model above (communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability), it is useful to consider the example of TDR certification. Repository certification is fundamentally about risk assessment. Repositories achieve certification as trustworthy by demonstrating their ability to identify and mitigate risks, and one type of certification in particular is based on the ISO 16363: Trustworthy Repositories Audit and Certification: Criteria Checklist (Consultative Committee for Space Data Systems, 2012).

An organization that has certified repositories as trustworthy using the criteria described in ISO 16363 is the Center for Research Libraries (CRL) (for instance, Center for Research Libraries, 2010, 2011, 2012, 2013, 2018, 2015). ISO 16363 explains that a TDR "will understand threats to and risks within its systems" (Consultative Committee for Space Data Systems, 2012, p. 19). It also discusses financial risks, infrastructure risks, and security risks, and calls for repositories to identify preservation risks and provide strategies for dealing with them (Consultative Committee for Space Data Systems, 2012). The standard treats risks as concrete and identifiable and addressable, suggesting an alignment with the classical definition of risk as a quantifiable value based on the probability and consequences of a negative event.

- A CRL-administered TDR audit is a process that involves *communication* among and across repository staff members and auditors. Perceptions of risk among people involved in the audit process may vary depending on the way in which risk information is communicated, and the relationship between the source and recipient of the message.
- In an audit process, repository staff face *complexity* in terms of the technical work of digital preservation, and also in terms of organizational and economic factors relating to the repository. Auditors may assess each repository differently depending on the complexity of the repository environment, the complexity of their own organization, and/or the complexity of the audit process itself.
- Participation in the process is required from a variety of people who have different types of *expertise.* Trust in the expertise and knowledge of others is necessary in order to complete the documentation required.
- Each repository is a separate *organization* that may shape perceptions of risk for its members in different ways. Auditors also belong to organizations that may shape their perceptions of risk in ways that differ from the repositories that they are assessing. It is also possible that individuals or groups within organizations will have varying perceptions of risk based on their position in the organization.
- *Political culture* is relevant to TDR certification in part because of strong ties between political culture and policymaking. Also, all of the repositories certified by CRL are located in North America, and it is possible that perceptions of risk within the audit process will vary across international boundaries.
- Certification following ISO 16363 is all about demonstrating that repositories can be *trusted.* The goal of the certification checklist is for repository staff to demonstrate their ability to manage risk in a number of areas. As with expertise, the management of digital repositories depends upon different stakeholders within the organization having trust in others. The push for transparency in the audit process is meant to foster trust among repository staff and with external stakeholders such as auditors.
- *Uncertainty* may influence the TDR audit process because the repository staff members who take part in the process are likely to have varying levels of expertise and knowledge about the repository. Additionally, auditors are likely to have varying levels of knowledge about the repository and may experience uncertainty based on their own knowledge and expertise about activities relating to digital preservation.
- Perceptions of risk may vary among repository staff depending on their awareness of the *vulnerabilities* that a repository faces. Perceptions of risk may also vary between repository staff and auditors, as repository staff experience varying degrees of risk exposure, and auditors face varying levels of awareness of the vulnerabilities that repositories and their staff members face.

As the example of TDR certification above demonstrates, the eight elements that comprise this framework for the social construction of risk have the potential to influence perceptions of risk within a repository audit.

Academic research in digital preservation has engaged with the concept of risk as a knowable, quantifiable figure that technical systems must be designed to overcome (Barateiro et al., 2010). This approach to digital preservation relies on a positivistic methodological orientation and a technical perspective heavily influenced by computer science (Barateiro et al., 2011) and previous conceptualizations of risk by professional organizations such as the Institute of Risk Management (Institute of Risk Management, Association of Insurance and Risk Managers, & Public Risk Management Association, 2002).

Scholars, including Lavoie and Dempsey (2004) have laid out many ways to investigate digital preservation, including focusing on digital preservation as a technical, economic, organizational, or social challenge (Lavoie, 2008; Lavoie & Dempsey, 2004). Many in the digital preservation community have focused on technical challenges (for instance, Jantz & Giarlo, 2007). Digital preservation research focusing on technical aspects of preservation has examined file formats (for instance, Lawrence, Kehoe, Rieger, Walters, & Kenney, 2000; Ohshima, 2010), system architecture (for instance, Barateiro, Antunes, & Borbinha, 2012), IT governance (for instance, Becker, Antunes, Barateiro, Vieira, & Borbinha, 2011), the reliability of storage

DOI: 10.1002/asi

media (for instance, Baker et al., 2006), mechanisms for managing distributed backup systems (for instance, Maniatis, Roussopoulos, Giuli, Rosenthal, & Baker, 2005), and the development of technical standards (for instance, Dobratz & Schoger, 2007; Harmsen, 2008).

This article posits that risk in digital preservation should be considered a social challenge, and builds upon previous research to present a framework for the social construction of risk in digital preservation. I argue that digital preservation risks are not merely technical, economic, or organizational. Rather, I have shown how ensuring the longevity of digital information is also a social process in which risks are interpreted by individuals. Their subsequent actions are influenced by social factors that shape the ways in which they perceive and understand risk. This approach will provide insights about the ways that people behave in response to information about risks and the complex social contexts in which they operate.

While the examples provided above focus on digital preservation activities taking place in organizations such as repositories, this framework can be applied in any setting where the long-term preservation of digital content takes place. Indeed, individuals across a variety of organizations are engaged in work that contributes to digital preservation, and as the example of TDR certification in this section demonstrated, it is not only the risk perception of repository staff members that matters for digital preservation but also the perception of repository stakeholders and other external groups/individuals who are in some way involved in the work of digital preservation.

Conclusion

It is time for the digital preservation community to engage with the concept of risk in a way that accounts for the complex social contexts within which digital preservation takes place. In this article I have presented a model for the social construction of risk in digital preservation, which consists of eight factors: communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability. Taken individually, each of these factors can influence how individuals and groups construct their understanding of risk. When considered together, they can amplify and/or attenuate perceptions of risk.

The concept of risk is foundational to the field of digital preservation. With our increasing reliance on digital information, and the central role that it plays in research, education, government, and commerce, it is important to understand how the people and groups who carry out the work of digital preservation construct their understandings of risk. Risk identification is an important first step, but understanding how and why people respond to that information is necessary for the long-term preservation of digital information.

References

Arvai, J.L. (2007). Rethinking of risk communication: Lessons from the decision sciences. Tree Genetics & Genomes, 3(2), 173–185. https://doi.org/10.1007/s11295-006-0068-7

Baker, M., Shah, M., Rosenthal, D.S.H., Roussopoulos, M., Maniatis, P., Giuli, T., & Bungale, P. (2006). A fresh look at the reliability of long-term digital storage. In Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems 2006 (pp. 221–234). New York: ACM. https://doi.org/10.1145/1217935.1217957

Barateiro, J., Antunes, G., & Borbinha, J. (2011). Long-term security of digital information: Assessment through risk management and enterprise architecture. In 2011 IEEE EUROCON - International Conference on Computer as a Tool (EUROCON) (pp. 1–4). https://doi.org/10.1109/EUROCON.2011.5929270

Barateiro, J., Antunes, G., & Borbinha, J. (2012). Manage risks through the enterprise architecture. In 2012 45th Hawaii International Conference on System Science (HICSS) (pp. 3297–3306). https://doi.org/10.1109/HICSS.2012.419

Barateiro, J., Antunes, G., Freitas, F., & Borbinha, J. (2010). Designing digital preservation solutions: A risk management-based approach. International Journal of Digital Curation, 5(1), 4–17. https://doi.org/10.2218/ijdc.v5i1.140

Beck, U. (1992). Risk Society: Towards a New Modernity. London, Newbury Park: Sage Publications.

Beck, U. (1999). World Risk Society. Malden, MA: Polity Press.

Becker, C., Antunes, G., Barateiro, J., Vieira, R., & Borbinha, J. (2011). Control objectives for DP: Digital preservation as an integrated part of IT governance. Proceedings of the American Society for Information Science and Technology, 48(1), 1–10. https://doi.org/10.1002/meet.2011.14504801124

Becker, C., & Rauber, A. (2011). Decision criteria in digital preservation: What to measure and how. Journal of the American Society for Information Science and Technology, 62(6), 1009–1028. https://doi.org/10.1002/asi.21527

Berman, F. (2008). Got data?: A guide to data preservation in the information age. Communications of the ACM - Surviving the Data Deluge, 51 (12), 50–56. https://doi.org/10.1145/1409360.1409376

Bostrom, A. (2014). Progress in risk communication since the 1989 NRC report: Response to 'four questions for risk communication' by Roger Kasperson. Journal of Risk Research, 17(10), 1259–1264. https://doi.org/10.1080/13669877.2014.923032

Burgess, A. (2015). Social construction of risk. In H. Cho, T. Reimer, & K. McComas (Eds.), The Sage Handbook of Risk Communication (pp. 56–68). Thousand Oaks, CA: SAGE Publications.

CBC News. (2012). Federal Libraries, Archives Shutting Down [News]. Retrieved from http://www.cbc.ca/news/canada/ottawa/federal-libraries-archives-shutting-down-1.1139085. [19 June 2016].

Center for Research Libraries. (2010). CRL Certification Report on Portico Audit Findings. Retrieved from Center for Research Libraries website: https://www.crl.edu/sites/default/files/reports/CRL%20Report%20on%20Portico%20Audit%202010.pdf

Center for Research Libraries. (2011). CRL Certification Report on the HathiTrust Digital Repository. Retrieved from Center for Research Libraries website: https://www.crl.edu/sites/default/files/reports/CRL%20HathiTrust%202011.pdf

Center for Research Libraries. (2012). CRL Certification Report on Chronopolis Audit Findings. Retrieved from Center for Research Libraries website: https://www.crl.edu/sites/default/files/reports/Chron_Report_2012_final_0.pdf

Center for Research Libraries. (2013). CRL Certification Report on Scholars Portal Audit Findings. Retrieved from Center for Research Libraries website: http://www.crl.edu/sites/default/files/attachments/pages/ScholarsPortal_Report_2013_f.pdf

Center for Research Libraries. (2018). 2018 Updated Certification Report on CLOCKSS. Retrieved from Center for Research Libraries website: https://www.crl.edu/sites/default/files/reports/CLOCKSS_Report_2018_0.pdf

Center for Research Libraries. (2015). CRL Certification Report on the Canadiana.org Digital Repository. Retrieved from Center for Research Libraries website: https://www.crl.edu/sites/default/files/reports/CANADIANA_AUDIT%20REPORT_2015.pdf

Chung, I.J. (2011). Social amplification of risk in the Internet environment. Risk Analysis, 31(12), 1883–1896. https://doi.org/10.1111/j.1539-6924.2011.01623.x

Colati, J.B., & Colati, G.C. (2009). A place for safekeeping: Ensuring responsibility, trust, and goodness in the Alliance Digital Repository. Library & Archival Security, 22(2), 141–155. https://doi.org/10.1080/01960070902904118

Consultative Committee for Space Data Systems. (2012). Space Data and Information Transfer Systems — Audit and Certification of Trustworthy Digital Repositories (Standard No. ISO 16363:2012 (CCSDS 652-R-1)). Washington, DC: Consultative Committee for Space Data Systems Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510

Conway, P. (1996). Preservation in the Digital World. Washington, DC: Commission on Preservation and Access.

Conway, P. (2010). Preservation in the age of Google: Digitization, digital preservation, and dilemmas. The Library Quarterly: Information, Community, Policy, 80(1), 61–79. https://doi.org/10.1086/648463

Corritore, C.L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. International Journal of Human-Computer Studies, 58(6), 737–758. https://doi.org/10.1016/S1071-5819(03)00041-7

Dake, K. (1991). Orienting dispositions in the perception of risk: An analysis of contemporary worldviews and cultural biases. Journal of Cross-Cultural Psychology, 22(1), 61–82. https://doi.org/10.1177/0022022191221006

Dake, K. (1992). Myths of nature: Culture and the social construction of risk. Journal of Social Issues, 48(4), 21–37. https://doi.org/10.1111/j.1540-4560.1992.tb01943.x

Dale, R., & Gore, E. (2010). Process models and the development of trustworthy digital repositories. Information Standards Quarterly, 22(2), 14. https://doi.org/10.3789/isqv22n2.2010.02

Day, M. (2008). Toward distributed infrastructures for digital preservation: The roles of collaboration and trust. International Journal of Digital Curation, 3(1), 15–28. https://doi.org/10.2218/ijdc.v3i1.39

De Santis, L., Scannapieco, M., & Catarci, T. (2003). Trusting data quality in cooperative information systems. In R. Meersman, Z. Tari, & D.C. Schmidt (Eds.), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. OTM 2003. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-39964-3_23

Dillo, I., & De Leeuw, L. (2018). CoreTrustSeal. Mitteilungen Der Vereinigung Österreichischer Bibliothekarinnen Und Bibliothekare, 71(1), 162–170. https://doi.org/10.31263/voebm.v71i1.1981

Dobratz, S., & Schoger, A. (2007). Trustworthy digital long-term repositories: The nestor approach in the context of international developments. In L. Kovács, N. Fuhr, & C. Meghini (Eds.), Research and Advanced Technology for Digital Libraries (pp. 210–222). Berlin, Heidelberg: Springer Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-74851-9_18.

Douglas, M., & Wildavsky, A. (1982). Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers. Berkeley, CA: University of California Press.

Dryden, J. (2011). Measuring trust: Standards for trusted digital repositories. Journal of Archival Organization, 9(2), 127–130.

Fischhoff, B. (1983). Acceptable Risk. Cambridge, MA, New York: Cambridge University Press.

Flynn, J., Slovic, P., & Mertz, C.K. (1994). Gender, race, and perception of environmental health risks. Risk Analysis, 14(6), 1101–1108. https://doi.org/10.1111/j.1539-6924.1994.tb00082.x

Gardoni, P., & Murphy, C. (2013). A scale of risk. Risk Analysis, 34, 1208–1227. https://doi.org/10.1111/risa.12150

Harmsen, H. (2008). Data Seal of Approval - assessment and review of the quality of operations for research data repositories (pp. 220–223). Presented at the iPRES 2008: The Fifth International Conference on Preservation of Digital Objects, London: The British Library. Retrieved from http://www.bl.uk/ipres2008/presentations_day2/34_Harmsen.pdf

Hart, P.E., & Liu, Z. (2003). Trust in the preservation of digital information. Communications of the ACM, 46(6), 93–97. https://doi.org/10.1145/777313.777319

Hilgartner, S. (1992). The social construction of risk objects. In J.F. Short, Jr. & L. Clarke (Eds.), Organizations, Uncertainties, and Risk (pp. 39–53). Boulder, CO: Westview Press.

Hitchcock, J.L. (2001). Gender differences in risk perception: Broadening the contexts. Risk: Health, Safety & Environment, 12, 179–204.

Hughes, T. (2012). The evolution of large technical systems. In W. Bijker, T. Hughes, & T. Pinch (Eds.), The social construction of technological systems (pp. 45–76). Cambridge, MA: MIT Press.

Hutter, B.M. (2005). "Ways of seeing": Understandings of risk in organizational settings. In B.M. Hutter & M. Power (Eds.), Organizational encounters with risk (pp. 67–91). Cambridge, UK: Cambridge University Press.

Hutter, B.M., & Power, M. (2005). Organizational encounters with risk: An introduction. In B.M. Hutter & M. Power (Eds.), Organizational Encounters with Risk (pp. 1–32). Cambridge, UK: Cambridge University Press.

Institute of Risk Management, Association of Insurance and Risk Managers & Public Risk Management Association. (2002). A Risk Management Standard. London: The Institute of Risk Management Retrieved from https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

International Organization for Standardization. (2009). Guide 73: Risk Management - Vocabulary (No. ISO Guide 73:2009) (p. 15). Geneva, Switzerland: International Organization for Standardization.

International Organbization for Standardization Technical Committee. (2018). Risk Management - Guidelines (Standard No. ISO 31000:2018). Washington, DC: International Organization for Standardization Retrieved from https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Jantz, R., & Giarlo, M. (2007). Digital archiving and preservation: Technologies and processes for a trusted repository. Journal of Archival Organization, 4(1–2), 193–213. https://doi.org/10.1300/J201v04n01_10

Jasanoff, S. (1986). Risk Management and Political Culture: A Comparative Study of Science in the Policy Context. New York: Russell Sage Foundation.

Jasanoff, S. (1998). The political science of risk perception. Reliability Engineering & System Safety, 59(1), 91–99. https://doi.org/10.1016/S0951-8320(97)00129-4

Kahneman, D. (2013). Thinking, Fast and Slow (1st pbk. ed.). New York: Farrar, Straus and Giroux.

Kaplan, S., & Garrick, B.J. (1981). On the quantitative definition of risk. Risk Analysis, 1(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Kasperson, R.E., & Kasperson, J.X. (1996). The social amplification and attenuation of risk. Annals of the American Academy of Political and Social Science, 545, 95–105.

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., … Ratick, S. (1988). The social amplification of risk: A conceptual framework. Risk Analysis, 8(2), 177–187. https://doi.org/10.1111/j.1539-6924.1988.tb01168.x

Keitel, C. (2012). DIN Standard 31644 and nestor Certification. Presented at the International Conference 2012: Cultural Heritage On Line, Florence, Italy. Retrieved from https://web.archive.org/web/20121127235326/http://www.rinascimento-digitale.it/conference2012-culturalheritageonline-programme.phtml

Kelton, K., Fleischmann, K.R., & Wallace, W.A. (2008). Trust in digital information. Journal of the American Society for Information Science and Technology, 59(3), 363–374. https://doi.org/10.1002/asi.20722

Konheim, C.S. (1988). Risk communication in the real world. Risk Analysis, 8(3), 367–373. https://doi.org/10.1111/j.1539-6924.1988.tb00499.x

Lachlan, K.A., Burke, J., Spence, P.R., & Griffin, D. (2009). Risk perceptions, race, and hurricane Katrina. Howard Journal of Communications, 20(3), 295–309. https://doi.org/10.1080/10646170903070035

Lavoie, B. (2008). The fifth blackbird: Some thoughts on economically sustainable digital preservation. D-Lib Magazine, 14(3/4), 1–9. https://doi.org/10.1045/march2008-lavoie

Lavoie, B., & Dempsey, L. (2004). Thirteen ways of looking at Digital preservation. D-Lib Magazine, 10(7/8), 1–13. https://doi.org/10.1045/july2004-lavoie

Lawrence, G.W., Kehoe, W.R., Rieger, O.Y., Walters, W.H., & Kenney, A.R. (2000). Risk Management of Digital Information: A File Format Investigation. Washington, DC: Council on Library and Information Resources. Retrieved from http://eric.ed.gov/?id=ED449802

Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving beyond normal accidents and high reliability organizations: A systems approach

to safety in complex systems. Organization Studies, 30(2–3), 227–249. https://doi.org/10.1177/0170840608101478

MacKenzie, D. (2012). Missile accuracy: A case study in the social processes of technological change. In W. Bijker, T. Hughes, & T. Pinch (Eds.), The Social Construction of Technological Systems (pp. 189–216). Cambridge, MA: MIT Press.

MacNeil, H. (2000). Providing the grounds for trust: Developing conceptual requirements for the long-term preservation of authentic electronic records. Archiv, 50, 52–78.

Maniatis, P., Roussopoulos, M., Giuli, T.J., Rosenthal, D.S.H., & Baker, M. (2005). The LOCKSS peer-to-peer digital preservation system. ACM Transactions on Computing Systems, 23(1), 2–50. https://doi.org/10.1145/1047915.1047917

McHugh, A., Ross, S., Innocenti, P., Ruusalepp, R., & Hoffman, H. (2008). Bringing self-assessment home: Repository profiling and key lines of enquiry within DRAMBORA. The International Journal of Digital Curation, 3(2), 130–142. https://doi.org/doi:10.2218/ijdc.v3i2.64

Mutula, S.M. (2011). Ethics and trust in digital scholarship. The Electronic Library, 29(2), 261–276. https://doi.org/10.1108/02640471111125212

National Science Foundation. (2011). Grant Proposal Guide (No. NSF 11–1). Arlington, VA: National Science Foundation. Retrieved from http://www.nsf.gov/pubs/policydocs/pappguide/nsf11001/gpg_index.jsp

Nelkin, D. (1989). Communicating technological risk: The social construction of risk perception. Annual Review of Public Health, 10(1), 95–113. https://doi.org/10.1146/annurev.pu.10.050189.000523

Nickel, P.J., & Vaesen, K. (2012). Risk and trust. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), Handbook of Risk Theory (pp. 857–876). Netherlands: Springer Retrieved from http://link.springer.com.proxy.lib.umich.edu/referenceworkentry/10.1007/978-94-007-1433-5_34.

Ohshima, S. (2010). Risks associated with digital preservation: Media deterioration, media obsolescence and file format obsolescence. Journal of Information Science & Technology Association, 60(2), 54–54.

Olofsson, A., Zinn, J.O., Griffin, G., Nygren, K.G., Cebulla, A., & Hannah-Moffat, K. (2014). The mutual constitution of risk and inequalities: Intersectional risk theory. Health, Risk & Society, 0(0), 1–14. https://doi.org/10.1080/13698575.2014.942258

Otway, H. (1992). Public wisdom, expert fallibility: Toward a contextual theory of risk. In S. Krimsky & D. Golding (Eds.), Social Theories of Risk (pp. 215–228). Westport, CT: Praeger Publishers.

Parthasarathy, S. (2007). Building genetic medicine: Breast cancer, technology, and the comparative politics of health care. Retrieved from http://site.ebrary.com/id/10173530

Perrow, C. (1999). Normal Accidents: Living With High-Risk Technologies (updated). Princeton, NJ: Princeton University Press.

Pidgeon, N. (1998). Risk assessment, risk values and the social science programme: Why we do need risk perception research. Reliability Engineering & System Safety, 59(1), 5–15. https://doi.org/10.1016/S0951-8320(97)00114-2

Renn, O. (1991). Risk communication and the social amplification of risk. In R.E. Kasperson & P.J.M. Stallen (Eds.), Communicating Risks to the Public (pp. 287–324). Netherlands: Springer Retrieved from http://link.springer.com.proxy.lib.umich.edu/chapter/10.1007/978-94-009-1952-5_14.

Renn, O. (2008). White paper on risk governance: Toward an integrative framework. In O. Renn & K.D. Walker (Eds.), Global Risk Governance (pp. 3–73). Netherlands: Springer.

Renn, O., Burns, W.J., Kasperson, J.X., Kasperson, R.E., & Slovic, P. (1992). The social amplification of risk: Theoretical foundations and empirical applications. Journal of Social Issues, 48(4), 137–160. https://doi.org/10.1111/j.1540-4560.1992.tb01949.x

Rijpma, J.A. (1997). Complexity, tight–coupling and reliability: Connecting normal accidents theory and high reliability theory. Journal of Contingencies and Crisis Management, 5(1), 15–23. https://doi.org/10.1111/1468-5973.00033

RLG-NARA Digital Repository Certification Task Force. (2007). Trustworthy Repositories Audit & Certification: Criteria and Checklist, Version 1.0. Retrieved from http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

Ross, S., & McHugh, A. (2006). Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management. Presented at the iPRES 2006. New York: Digital Curation Centre.

Rowe, W.D. (1977). An Anatomy of Risk. New York: Wiley.

Royal Society (Great Britain) & Study Group on Risk. (1983). Risk Assessment: Report of a Royal Society Study Group. London: Royal Society.

Slovic, P. (1987). Perception of risk. Science, 236(4799), 280–285. https://doi.org/10.1126/science.3563507

Smith Rumsey, A. (2016). When We Are No More: How Digital Memory Is Shaping Our Future (Kindle Edition). New York: Bloomsbury Press.

Starr, C. (1969). Social benefit versus technological risk. Science, 165 (3899), 1232–1238. https://doi.org/10.1126/science.165.3899.1232

Starr, C. (2003). The precautionary principle versus risk analysis. Risk Analysis, 23(1), 1–3. https://doi.org/10.1111/1539-6924.00285

The National Science Foundation. (2018). National Science Foundation FY 2019 Budget Request to Congress (nsf18022). The National Science Foundation. Retrieved from https://www.nsf.gov/pubs/2018/nsf18022/nsf18022.pdf

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131.

van Est, R., Walhout, B., & Brom, F. (2012). Risk and technology assessment. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), Handbook of Risk Theory (pp. 1067–1091). Netherlands: Springer Retrieved from http://link.springer.com.proxy.lib.umich.edu/referenceworkentry/10.1007/978-94-007-1433-5_43.

Vaughan, D. (1996). The challenger launch decision: Risky technology, culture, and deviance at NASA. Chicago: University of Chicago Press.

Vaughan, D. (2005). Organizational rituals of risk and error. In B. M. Hutter & M. Power (Eds.), Organizational Encounters with Risk (pp. 33–66). Cambridge, UK: Cambridge University Press.

Vaughan, E., & Seifert, M. (1992). Variability in the framing of risk issues. Journal of Social Issues, 48(4), 119–135. https://doi.org/10.1111/j.1540-4560.1992.tb01948.x

Vermaaten, S., Lavoie, B., & Caplan, P. (2012). Identifying threats to successful digital preservation: The SPOT model for risk assessment. D-Lib Magazine, 18(9/10), 1–21. https://doi.org/10.1045/september2012-vermaaten

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why? Daedalus, 119(4), 41–60.

Wilkinson, I. (2001). Social theories of risk perception: At once indispensable and insufficient. Current Sociology, 49(1), 1–22. https://doi.org/10.1177/0011392101049001002

Wynne, B. (1992). Misunderstood misunderstanding: Social identities and public uptake of science. Public Understanding of Science, 1(3), 281–304. https://doi.org/10.1088/0963-6625/1/3/004

Yakel, E., Faniel, I., Kriesberg, A., & Yoon, A. (2013). Trust in digital repositories. International Journal of Digital Curation, 8(1), 143–156. https://doi.org/10.2218/ijdc.v8i1.251

Yoon, A. (2014). End users' trust in data repositories: Definition and influences on trust development. Archival Science, 14(1), 17–34. https://doi.org/10.1007/s10502-013-9207-8

Yoon, A. (2016). Data reusers' trust development. Journal of the Association for Information Science and Technology, 68, 946–956. https://doi.org/10.1002/asi.23730