ARCHIVES AND MANUSCRIPTS, 2017
VOL. 45, NO. 2, 176–190
https://doi.org/10.1080/01576895.2017.1366864

Routledge
Taylor & Francis Group

Participatory cultures, trust technologies and decentralisation: innovation opportunities for recordkeeping

Cassie Findlay

Independent Scholar, San Francisco, CA, USA

ABSTRACT

Recordkeeping professionals build and manage systems that support the creation and maintenance of trustworthy records, however our approach to the design and implementation of such systems has suffered from a lack of innovation and a failure to collaborate effectively with allied disciplines. Contemporary society, politics and Internet culture are producing new models, tools and techniques which open up exciting possibilities for how recordkeeping systems might work, presenting both opportunities and challenges for recordkeeping professionals. In this article, some elements deemed necessary for trustworthy recordkeeping are identified and critically examined in light of the possibilities of participatory cultures, peer-to-peer business and trust through computation, in particular, blockchain technologies. Conclusions are drawn regarding what might be needed in order to adapt current models and practices to build new forms of recordkeeping systems that could enhance the agency of the individual in a networked society.

KEYWORDS

Recordkeeping; decentralisation; archives; blockchain; trust

Changing notions of trust in society

The information landscape today is a vast, complex and, at times, dangerous place. Disruptive innovations are challenging some of our fundamental assumptions about what is and is not trustworthy information, while at the same time information is becoming a more significant tool for political action than ever before. The 2016 Presidential election in the United States was dominated by challenges to the truthfulness of candidates and the sharing of 'fake news' online stories to spread disinformation, falsehoods and propaganda. Such efforts were amplified by the enormous reach of social media giants like Twitter and Facebook. As noted by researcher Liliana Bounegru: 'social media platforms have acted as engines to channel previously fringe universes of political culture, rooted in right-wing populism and post-truth politics, into the mainstream of American politics'.[1] The need for evidence with which to back up claims was seemingly not important to the consumers of this information. Indeed, as noted by Duncan Watts, 'a flagrant disregard for consistency and evidence may even be interpreted as a demonstration of power: the power to create one's own reality'.[2] Commentators argue that in certain actors' hands, information has become weaponised.

CONTACT Cassie Findlay findlay.cassie@gmail.com

This is not a new phenomenon – one only needs to look at the propaganda wars of the past to understand that – but one that is playing out with greater impact and a more widespread awareness amongst the public that it is occurring than was the case in the past.

In parallel with the continuing barrage of information attacks aimed at the public, the gathering of information on citizens by the State and by corporate entities has dramatically escalated. At no point in history has so much data on everyday citizens been gathered, retained and analysed. Personal data has become a new form of currency. Online services often require users to share their personal identity data with a myriad of corporations while having little say in how that information is used, and the monetary benefits of this data are unfairly distributed. What effects flow from the twenty-first-century panopticon on the trust that we place in our elected representatives and in the providers of services that have become essential to our daily lives? Research has shown that indiscriminate monitoring fosters distrust. In a 2012 study Marie-Helen Maras identified a growing sense of 'otherness' amongst European Union (EU) citizens as a result of knowledge of the existence and use of the databases born of the EU's data-retention directives.[3] Such 'otherness' and perceived lack of personal autonomy come hand in hand with a lack of trust in those who constructed the databases in which data on us is captured and stored. The notion of the database as embodying this hierarchical relationship between two actors, with all that relationship's shortcomings, has been explored in philosophy. Bruno Latour refers to the example of 'data bases [that are] are full of defects, that they themselves embody a rather crude definition of society, that they are marked by strong asymmetries of power, and above all that they mark only a passing moment in the traceability of the … connections'.[4] Instead, Latour proposes models for social behaviour which move from such hierarchical models – which he sees as increasingly unhelpful – to overlapping networks, allowing for more equitable transactions to take place.

In this climate, the need for strong and defensible systems for making and keeping trustworthy records of the actions and decisions of powerful people and organisations is pressing. As noted by Eric Ketelaar, 'Records act as instruments of power'.[5] The keeping of records by abusive governments serves to oppress its people. By keeping records of abuses, today in the form, for example, of smartphone recordings of police aggression towards minorities, such oppression can be highlighted and resisted. It is only by accessing this evidence, these primary sources, that citizens and fourth-estate actors can dig below the so-called 'fake news' to uncover the truth. It is only by keeping trustworthy records of our business and the conduct of affairs that there is the possibility of such reporting. It is only by assigning the proper context(s) and management information (metadata) to such records that they will remain available to the right people and groups at the right times. But what do we mean by 'trustworthy'? Trustworthy for whom? When? Is the recordkeeping/archives profession building the right kinds of systems for ensuring the continued creation, maintenance and use of such trustworthy records? In an era of unsurpassed surveillance, further questions arise about whether such systems for recordkeeping can embrace Latour's ideas of networks, not hierarchies, in the making and keeping of trustworthy records of our business and affairs. How can we ensure the records remain protected from tampering or loss and available over time? Available when needed, protected when required? In order to begin to conceptualise how new forms of recordkeeping might address some of these questions, it is necessary first to examine some of the trends and innovations that are changing some of society's most basic understanding of how we go about our civil and public lives.

The struggle between network and hierarchy

The socio-political and technological environment in which we live and in which record-keeping now occurs is undergoing dramatic change. Shifts in societal norms and values, and radical innovations in keeping and sharing information that have occurred over the recent decades since the invention of the World Wide Web, are changing society's expectations of recordkeeping. As presaged in Latour's work, it has been argued that society is transitioning from hierarchical to networked models. It's a movement from centralised institutions of mandated trust, to networks of distributed democracy, a phenomenon which Paul Mason, economics editor for the UK's *Channel 4 News*, has described as the 'struggle between network and hierarchy'.[6] These changes have in part been triggered by the use of Internet-based technologies to do business in ways not requiring the traditional gatekeepers and intermediaries. There are various ways to characterise these trends but, for the purposes of exploration here, they have been labelled and grouped into the following phenomena:

- participatory cultures;
- peer-to-peer networks; and
- trust through computation.

Most obviously manifest in the rise of social media platforms, participatory cultures have acquired a new prominence and power in the twenty-first century. These cultures have been defined by Barney et al. as the 'the promise and expectation that one can be actively involved with others in decision-making processes that affect the evolution of social bonds, communities, systems of knowledge, and organisations, as well as politics and culture'.[7] Like systems for recordkeeping, media-based participatory systems are not about the technologies alone but also comprise the 'social, cultural, legal, political and economic institutions, practices and protocols that shape and surround them'. Participatory cultures reflect the prevailing values of the society in which they operate.[8] In Western, capitalistic democracies, the emerging media environment has become, Jodi Dean argues, an 'engine of commerce, consent and control'.[9] Or to put it another way: when an online service is free, you're the product.[10] However participatory cultures are also about communities, and benefits flow from the formation and mobilisation of communities. As Alberto Melucci explains: 'It means both taking part, that is, acting so as to promote the interests and needs of an actor, as well as belonging to a system, identifying with the "general interests" of the community.'[11] A widely recognised example of such communal promotion of interests can be found in the effects of the sharing of blogs and social media content during the Arab Spring, using content from outlets such as WikiLeaks to build political momentum. There are many other examples, on both sides of the political spectrum, from Black Lives Matter to the alt-right. As noted by Jillian York, 'it is clear that participatory media can be a powerful tool to harness energy and attention toward a diverse set of causes, in spite of government attempts to control information and infiltrate networks'.[12] An important characteristic of participatory cultures is the centrality and agency of the individual, alongside the strength and power of 'the crowd', united by sentiment or other factors, and connected online.

In parallel with the rise of participatory cultures we have seen the maturation of peer-to-peer technologies. Peer-to-peer (P2P) computing or networking is 'a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network

of nodes.'[13] In the 1990s and 2000s, anonymous file-sharing sites such as Napster and latterly BitTorrent were the most obvious manifestations of peer-to-peer technologies to the average Internet user. In these systems, reputation is critical, as it has become in other new economy platforms, such as the ride-sharing services Uber or Lyft, or the home-sharing service Airbnb. The difference between true P2P and these services is that corporations act as intermediaries, or 'rent-seekers', sitting between the consumer and the service providers, taking their slice of the revenue. True P2P means no such 'middle man' exists, either in technical terms or in terms of the actors' relationships. Instead, trust is supported by systems of reputation, for both the users and the purveyors of services.

The arrival in 2008 of a protocol for the transfer of virtual currency (Bitcoin), with the 'blockchain' as its central component, was a major advance for peer-to-peer, decentralised technologies.[14] In recordkeeping terms, blockchain technology creates a ledger or register. This is a register shared by users around the globe and is owned and controlled by no one. A key distinguishing feature of the blockchain is consensus; the blockchain algorithm enables distributed (global) consensus on who owns what currency. It is proof of work – proof of an action at a point in time (with Bitcoin, the mining and ownership of the currency). With no central authority and no controlling corporation, blockchain technology offers the possibility of decentralised proof which can't be erased or modified by anyone; competitors, third parties or governments. This is what distinguishes using the blockchain from other forms of data timestamping and authentication. It's about moving away from what Nozomi Hayase has called 'centralised institutions of mandated trust',[15] to networks of distributed business. Blockchain technologies are, in effect, authenticating mechanisms. Instead of relying on a central authority to certify the authenticity of a transaction, the proof of its veracity is demonstrated via distributed cryptographic confirmation. Silicon Valley tech entrepreneur and author Andreas Antonopoulos describes this as trust by computation. Antonopoulos notes:

> Trust does not depend on excluding bad actors, as they cannot 'fake' trust. They cannot pretend to be the trusted party, as there is none. They cannot steal the central keys as there are none. They cannot pull the levers of control at the core of the system, as there is no core and no levers of control.[16]

Blockchain-based records of transactions are immutable and incorruptible, and all parties privy to the 'ledger' can evaluate the provenance of the information in it to determine if there has been tampering.

Decentralised, peer-to-peer systems that utilise blockchain technologies have a number of other commonly agreed advantages, some of which have been neatly outlined by Vitalek Buterin:[17]

> Fault tolerance—decentralized systems are less likely to fail accidentally because they rely on many separate components that are not likely.
>
> Attack resistance—decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system.
>
> Collusion resistance—it is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants, whereas the leaderships of corporations and governments collude in ways that benefit themselves but harm less well-coordinated citizens, customers, employees and the general public all the time.

To date, applications for blockchain technologies have mostly been found in the realms of finance, property, contracts and identity. Amongst these domains we can see requirements both for high-volume recordkeeping solutions and for more ad-hoc, tailored solutions to specific needs, including:

- centralised registries controlled and/or maintained by governments for land ownership;
- systems supporting the creation and management of signed contracts with retailers or service providers, records of which are retained by both parties or by one party with limited access for the user;
- financial management systems used by banks to record the exchange of money; and
- proof of identity systems such as birth registries or systems for confirming eligibility to open bank accounts.

Blockchain technologies are a technological infrastructure for true peer-to-peer recordkeeping and, potentially, a tool for personal recordkeeping that fulfils the requirements for persistent, trustworthy records of our own experience, transactions and interactions, to be retained for our purposes and shared at our instruction. A tool that enables greater individual agency as a recordkeeping entity, as opposed to reliance on a mandated trust institution which keeps records on our behalf. It may be argued therefore that, by enabling these defences against corruption of information or accidental loss of information, decentralised systems can claim greater trustworthiness over those that rely on a central authority. Such systems are seen by many has having almost limitless applications – beyond file sharing to new models for governance, and to replace existing economies. Indeed, one of the leading thinkers on P2P, Michel Bauwens, has proposed P2P phenomena as an emerging alternative to the capitalist society.[18] However, current barriers to entry of understanding how to use the technologies, a lack of user-friendly interfaces and the problems associated with energy consumption that their use entails should also not be underestimated.

How has recordkeeping responded to these innovations?

Historically, many recordkeeping system models have mimicked the broader structural features of the society in which they operate. These structural features have predominantly, in political systems like Australia's, been hierarchical in nature. So we can look to the widespread adoption of centralised file registry systems such as those used by Australian colonial authorities, to see the origins of the prevailing model for government records management in the twentieth and early twenty-first centuries. Unfortunately, our most commonly implemented models for recordkeeping systems have remained stuck in these old paradigms despite the developments described above. Many implementations remain siloed and unable to adequately capture the rich context of multiple interacting parties over time, frameworks for information access remain blocked from reform, and centralised power continues to exert influence over the types of records that are created and kept, as well as the failure to document, or to suppress. The possibilities of the Internet to free us from the risks inherent in keeping all of our (archival) eggs in one basket have not been adequately explored. No existing mandated authority is immune today from the risks of defunding or being 'legislated away'. As noted by Peter van Garderen, 'even exemplary collections like Trove are subject to economics and the political whims of their owners. In this case, a conservative Australian government that slashed funding and suggested looking for private donors to maintain the collection.'[19]

The effects of the inadequacies of today's systems for recordkeeping are serious, and manifold. In addition to failures to capture authoritative records that represent fully the complexity of our lives and business, we can also look at high-profile recordkeeping system failures such as the #CensusFail debacle to understand that where there once was almost automatic and unquestioning trust in the recordkeeping practices of governments,[20] this has been seriously eroded. While doing an imperfect job at supporting and advancing the interests of governments, today's recordkeeping systems implementations are also failing to empower groups that are in desperate need of empowerment. Recordkeeping is still stalled in traditional models of centralised control and the writing of history by the powerful – even many projects investigating participatory models for archives start with the assumption that the recordkeeping acts documenting the individual experience are set up and controlled by the more powerful entity.

There are, however, encouraging explorations of alternative models within the recordkeeping profession. Indigenous attitudes to evidence and memory, for example, offer us another perspective on – and an opportunity to learn about – what it means for records to be trusted by a community of people, and for people to have agency in the keeping of those records. In recent years, serious efforts to understand these differences and address them have been undertaken in the archival community. In Australia the Monash University-led Trust and Technology project examined these differences in some depth by speaking to Koorie people, assessing their experience with archival services and exploring new tools and methods. The project's final report notes that: 'Koorie knowledge cannot be made to adhere to the usual institutional/sectoral boundaries of archival programs.'[21] Amongst its seven key recommendations, the project participants proposed:

- a recalibration of the rights of the 'subjects' of records, in this instance Koorie people, to 'set the record straight', and
- acknowledging that Koorie people are currently afforded few rights over that part of their knowledge which is in archival institutions, finding ways to give effect to Koorie rights over this knowledge.[22]

We have also, in recent years, seen a significant rise in the creation of community archives online. In his 2011 article 'Archival Activism: Independent and Community-led Archives, Radical Public History and the Heritage Professions',[23] Andrew Flinn explores developments in this independent, non-professionalised archival activity, including what he terms 'radical or counter-hegemonic public history-making activities'. Flinn cites examples that are largely concerned with creating archives that address gaps in official traditional archives: the black LGBT experience in the UK, for example, or the daily lives of the East London working class. In the US, Witness.org's Yvonne Ng has described a number of community-centred archive initiatives that have emerged from Black Lives Matter movement including the Preserve The Baltimore Uprising 2015 Archive Project and Documenting Ferguson.[24] As Ng explains, the projects share a 'collaborative approach between traditional archives and archivists, community organisers, and concerned individuals'.[25] The Documenting The Now project has developed a tool and a community around supporting the ethical collection, use and preservation of social media content, with a particular focus on protest movements.[26] Here we see projects that come from a progressive standpoint, interested in themes of equality and anti-discrimination, of claiming a place in history for those who have been hidden or

voiceless. These are projects that are both products of our web-based culture and, arguably, a response to early twenty-first-century 'post-truth politics'.

In contrast, perhaps to the online community archives model described above, we have also recently seen other projects that are more concerned with the agency of the individual as part of the recordkeeping contract. Considering the recordkeeping needs of children who are under the guardianship of the state is, for example, a particularly pressing matter for recordkeeping professionals' attention today. In his remarks at the Australian Society of Archivists conference in Sydney in 2016, care leaver Frank Golding stated: 'In the vast majority of cases, the official records do not supply a coherent narrative that meets the need to know the truth about the past, and to tell the truth to others such as our children.'[27] Golding further proposed: 'Children in out-of-home care today can and should have the right to make a contribution to their record as it develops.'[28] What if this idea is extended to the making of their own records? This idea has been taken up by the Setting the Record Straight: For the Rights of the Child Initiative. The Initiative, which includes a National Summit being held in Melbourne in 2017, was organised, in part, as a response by the Australian recordkeeping community and allied groups to the findings of the Royal Commission into Institutional Reponses to Child Sexual Abuse, which commenced in 2013 and continues to date. The Initiative calls for the design and implementation of the infrastructure to support an 'independent lifelong living archive for every child who experiences out-of-home care.'[29] This is described as: 'A secure, distributed, networked, digital archive populated by children themselves and by their care givers, case workers, teachers, and health professionals. It would support a child's identity, memory and time in out-of-home care and be accessible throughout his or her life.'[30]

Despite the efforts being made in vanguard projects like those described above, many of us in the recordkeeping profession have, to date, been hampered in our efforts to innovate by a lack of sophistication in the tools we use and by our reliance on institutions of power to serve as verification and authentication agents in recordkeeping processes. We have, it may be argued, failed to fully grasp the opportunities presented by Internet phenomena and technologies described above, making the job of meeting the needs of people and communities seeking recordkeeping systems of their own much more difficult. Internet-based innovation and a flatter, more P2P-based model for recordkeeping have the potential now, however, to come together in new forms of recordkeeping systems that overcome problems associated with trust, fragility and resourcing. Systems which have the potential to rebalance the scales in the making and keeping of records of the individual experience. However, in order for the profession to make a useful contribution to the design of such systems, we must be sure we understand what we ourselves mean by trust in recordkeeping.

Existing understandings of trust in recordkeeping

The recordkeeping and archives community as a whole has conducted extensive research and developed many standards and guides on how records and the systems that make and keep them may be regarded as trustworthy by the communities they serve. This includes requirements from standards from the International Organization for Standardization and national bodies as well as research and guidance from international collaborative projects like the InterPARES (International Research into the Preservation of Authentic Records in

Electronic Systems) Project.[31] It also includes work that has focused on the role, governance structures and capabilities of custodians and the functionalities of repositories, such as sets of requirements and standards for trustworthy repositories developed on the basis of the Open Archival Information Systems (OAIS) reference model or the Trusted Third Party Repositories (TTPR) model, originally developed in South Korea.[32]

What do these investigations tell us about notions of trust as it is understood in the recordkeeping and archives world?

Since the adoption of the ideas of David Bearman by Australian recordkeeping professionals in the mid 1990s,[33] the development of the first Australian Standard on records management, AS 4390, in 1996, and the contemporaneous emergence of records continuum theory at Monash University, Australian recordkeeping theory and practice has focused heavily on the notion of the recordkeeping system and its processes, driven by the use and management of metadata for records, as the means for making and keeping trustworthy records, in any context and over time. Since this period, these concepts and principles have been used in the development of many tools and guides, including the widely adopted 'DIRKS' methodology (Designing and Implementing Recordkeeping Systems), the first International Standard on records management, ISO 15489:2001 Records Management, and its successor, ISO 15489:2016 Records Management. Such approaches favour routine, predictable processes for making and managing records, based on decisions (preferably accountable and consultative) by the recordkeeping system owner about what records are made, why, for whom and how they are to be managed.

Other projects concerned with the trustworthiness in recordkeeping have identified the resources, reputation and trustworthiness of the custodian or repository as a means to assuring the trustworthiness of the records. A report from the second phase of the InterPARES Project from 2008, for example, stated that a 'trusted custodian should be designated as the preserver of the creator's records'.[34] However the ubiquity of the Internet across all facets of business and society has since prompted a greater focus on how this kind of understanding translates to the online world. A successor to the earlier InterPARES work, the InterPARES Trust (ITrust 2013–18) is a multinational, interdisciplinary research project exploring issues concerning digital records and data entrusted to the Internet, including with the adoption of models and methods described in this article. Its research goal is described as 'frameworks that will support the development of integrated and consistent local, national and international networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet, to ensure public trust grounded on evidence of good governance, and a persistent digital memory'.[35] Amongst the products to date is Vicki Lemieux's 2016 analysis of blockchain technologies against requirements for trustworthy recordkeeping drawn from ISO 15489 and the United States' Generally Accepted Recordkeeping Principles (GARP).[36] Lemieux found that a mix of technical and non-technical controls will always be needed to engender trust in records, and that blockchain in itself cannot guarantee trust. As the technology matures, we are indeed seeing the emergence of a variety of non-technical mechanisms being put in place to help user communities and others who rely on blockchain records to trust them.[37]

The digital preservation community, closely associated with the recordkeeping and archives world, has also placed emphasis on the importance of trust in its models and best-practice standards. This can be seen, for example, in standards for trusted digital repositories. Greg Bak has examined the notion of trust in relation to standards that have been

widely adopted for keeping digital archives,[38] using the Trusted Digital Repository project at Library and Archives Canada as a case study. Bak proposes that it is user perceptions of trust which matter, rather than relying on standards, audits and certification, and that archives and other memory institutions should move away from proclaiming themselves to be *trusted*, to proposing that they can be *trustworthy*. He explains that this is not what he terms a technocratic version of trust, one that depends on technology and mandate, but rather it is about the formation and sustaining of relationships within a community. This is perhaps a challenging notion to many government archives, given that, as Hugh A Taylor observed in the 1980s: 'Most of our customers do not complain since we enjoy a monopoly of the business. There is nowhere else to go.'[39] Much has changed in the information landscape since that time, including in relation to access to government records. And yet it is also true that public trust in government and its agencies is at an all-time low in many Western democracies.[40] The failure of our recordkeeping tools and techniques to keep pace with changes in society – as demonstrated by #CensusFail and many other less high-profile cases – has no small part in this.

Regardless of the extent to which an organisational recordkeeping system or institutional archive might successfully promote itself as a trustworthy keeper of records, however, problems remain. We understand today that in fact the reliance on *any actor* – government, business, charity, church or other – to control and fund the necessary infrastructure for recordkeeping activity allows, whether to a minor or severe degree, a perspective bias that affects how records are made and kept, and also leaves open the possibility of corruption. This problem – especially where financial matters were concerned – brought about the idea of recordkeeping that need not rely on the use of a recordkeeping system controlled by either of the parties involved in a transaction. This idea of a neutral space in which records needing to be trusted and protected for the benefit of multiple parties may be made and kept is found in the work done in the International Standards arena on the TTPR. This was developed as a solution to problems associated with asserting authenticity and ensuring longevity for digital records, particularly in instances where those records may be subject to legal challenge. The team behind the TTPR's development into an International Standard has said: 'In many cases legal admissibility of digital records managed by organization's records systems cannot be ensured. As a result, there is a growing need for services by neutral third parties which guarantee these characteristics for digital records.'[41] The similarity between the goals of the TTPR initiative and the way that blockchain technologies are designed to enable trust but without need of a 'trusted third party' is noticeable.

A new paradigm?

Reviewing these projects, we might summarise what has been generally been regarded as important for trustworthy recordkeeping as:

(1) a person, entity or community with the authority, means and ability to design, implement and maintain a recordkeeping system;
(2) a person, entity or community who can make realistic assurances of the integrity and persistence of the records it keeps, now and into the future;
(3) a set of routine, accountable and agreed processes for making and managing records; and

(4) for some types of transactions, a trusted third party who can verify the authenticity of the record(s) of the transaction.

Turning back to lessons learned from the emerging networked society, we might then add to these requirements a need for:

(5) recordkeeping systems structures that give greater agency to the individual, rather than to the institutions that have traditionally had the required resourcing, mandate and status to keep 'verified' records.

By integrating the principles and tools of the networked society into existing recordkeeping models, exciting opportunities for person-centric, trustworthy systems of recordkeeping emerge. In such systems, records are regarded as authentic by virtue of (machine-enabled) community consensus rather than through control by an institution of economic or state-sanctioned power. In this way, our implementations could perhaps have a chance of rebalancing the inherent power structures of recordkeeping systems in ways that align with Latour's ideas on networks. Such systems, once established, would present a low barrier to entry for many types of communities, requiring little human capital for maintenance and no centralised infrastructure. Could this be the beginnings of a response to the Setting the Record Straight: For the Rights of the Child Initiative's call for an 'independent lifelong living archive', the needs of community archiving projects and other emerging recordkeeping problems?

How do we get there?

To start to consider this question we must return to core recordkeeping understandings. Appraisal – explained using the Australasian understanding of this activity in the latest edition of the International Standard ISO 15489 as the recurrent analysis of context, business, requirements and risk for the purposes of defining what records to make and how to manage them – is an essential starting point. By conducting appraisal we can gather data on:

- the cultural, technological and socio-legal contexts in which the recordkeeping takes place – including the legal framework;
- the agents and stakeholders involved in the 'business' at hand;
- a detailed understanding of the recordkeeping needs and expectations of these actors; and
- a detailed set of requirements for records and their management that addresses questions of access, use and usability, metadata and retention.

The design and implementation of recordkeeping processes based on the results of such appraisal will then, for a decentralised, blockchain-based model, need to take account of some of the key characteristics of these technologies. Design decisions will need to start with an acknowledgement that records today are most usefully conceptualised as collections of data, inclusive of contextualising metadata and metadata that both manages and accounts for events in the record's existence. In a blockchain-based implementation, it is unlikely that the full content of records will be recorded in the ledger, but that instead it will serve the purpose of a traditional ledger. That is, to register a business event, whether it be a financial transaction or acceptance of a contract. Of course records will often be comprised of different types of data, including in unstructured forms such as documents. It is possible to register the existence of a document (PDF or JPEG, for example) using a hash that is

recorded in a blockchain, but this is just a 'fingerprint' for the document, not the document's full content. Where additional elements of the record require linkage to such data or documents, it will be achieved logically, using identifiers and locational metadata. These other elements might exist in any other system, but to truly take advantage of decentralisation, a decentralised storage and management system could be implemented. Examples of such systems include the InterPlanetary File System (IPFS) or Storj.[42] The design and implementation of recordkeeping based on blockchain technologies will also need to address questions of access and use over time. Data on blockchains is by default unencrypted, and indeed its model is built on the availability of the data to all in the network. However, there are mechanisms by which access can be restricted – for example, by encrypting certain elements on a blockchain and handing out the keys to the relevant participants.[43] These problems of restricting access are primarily concerned with the blockchain ledger records, as opposed to decentralised strorage solutions noted above, which generally enable access control in more conventional – and familiar – ways.

Using these understandings, we might be able to arrive at a systems architecture which is based on robust recordkeeping analysis and embraces decentralised technologies (amongst a mix of technical and non-technical elements), with the individual interacting and recording their own interactions. For each recordkeeping requirement, we must think beyond the institutional, the separate 'capture' of records by agents involved in the transactions, and think instead of co-creation and keeping of records using a system that is designed and operated by consensus amongst a family, a community, an institution or a government, and which requires minimal maintenance once established. Metadata which supports access and permissions at a granular level. A secure digital identity which can serve as an anchor for both civic life and personal memory-making.

A call to action

There are a plethora of projects, from the academic research, business and government domains, that recordkeeping professionals can learn from in constructing these new-paradigm systems. Just a small sample includes:

- Peter Van Garderen has proposed a 'Decentralised Autonomous Collection' architecture,[44] to enable a set of digital information objects to be stored for ongoing re-use with the means and incentives for independent parties to participate in the contribution, presentation and curation of the information objects outside the control of an exclusive custodian. In this model, recordkeeping requirements could be encoded as business rules by its initial implementers and, Van Garderen proposes, updated by its subsequent participants using smart contracts deployed on blockchain technology.
- A number of projects and commercial enterprises are building applications for identity management and personally controlled data storage utilising blockchain technologies. These include the Enigma project at MIT and the Estonia e-residency initiative.[45] Such tools could be adapted to the needs of a particular community and serve as a repository for identity data as well as a registry for personal records, linked to a distributed file storage platform such as the IPFS.
- Smart contracts based on blockchain technologies can negotiate rights, payments and the performance of services automatically. Smart contracts could be designed to offer trustworthy exchange of value or information between members of a community. The

robustness of the recordkeeping in this environment could serve to protect the interests of participants without the need to involve a centralised authority. Metadata could be incorporated into the recording of the exchanges that links to additional contextual information about the agents, functions and records that make up the activity, offering a richer record for future use and memory-keeping. A candidate for the development of such contracts is Ethereum,[46] a public blockchain platform.

Further research and experimentation is, however, needed on the use of these technologies in the design and implementation of recordkeeping systems for specific cases. In particular, research into and testing of encryption key management as a means for managing access. A range of questions may be asked here, such as those posed by Antony Lewis: 'What needs to be encrypted: All data at rest? Data in motion? The whole database? Data within specific database fields? And who will be able to decrypt it and when? How will permissions be granted? Can permissions be revoked?'[47] Recordkeeping professionals already have a body of knowledge and experience in access and permissions metadata management – research is needed into how this can be operationalised in blockchain environments. In addition, given the opportunities for more person-centric recordkeeping that come with this technology, projects that test the functional requirements for evidence of the individual, as originally called for by Chris Hurley and Sue McKemmish in the 1990s along with the requirements proposed by the Setting the Record Straight Initiative, are also desirable.[48]

Looking forward

Decentralised technologies and public ledgers are still finding their place in the world. The networked society is pushing back against a worldwide lurch towards authoritarianism and ubiquitous online surveillance. At this time and place, recordkeeping, made more available for genuine participation by all, using community-agreed rules, languages and structure, secure and private when needed, with the sustainable preservation of this evidence and memory, is needed more than ever. Partnerships with potential user communities, developers and digital service designers will be essential to the effort to make the creation, capture and use of recordkeeping processes that rely on blockchain technologies 'fit for purpose' and user-friendly, whatever their objective. Recordkeeping expertise, and in particular accountable and thorough appraisal work and the use of innovative methods for deploying records controls using metadata, will be critical in these efforts as we, as a profession, look to position our skillset in this new networked society.

Endnotes

1. Liliana Bounegru, 'Three Ways in Which Digital Researchers Can Shed Light on the Information Politics of the "Post-Truth" Era', available at *<https://blogs.lse.ac.uk/impactofsocialsciences/2017/02/06/three-ways-in-which-digital-researchers-can-shed-light-on-the-information-politics-of-the-post-truth-era/>*, accessed 20 April 2017.
2. Duncan Watts, 'Rebuilding Legitimacy in a Post-truth Age', available at *<https://medium.com/@duncanjwatts/rebuilding-legitimacy-in-a-post-truth-age-2f9af19855a5>*, accessed 20 April 2017.
3. Marie-Helen Maras, 'The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the "Others"?' *International Journal of Law Crime and Justice*, vol. 40, no. 2, April 2012, pp. 65–81.

4. Bruno Latour, Pablo Jensen, Tommaso Venturini, Sébastian Grauwin and Dominique Boullier, '"The Whole is Always Smaller Than its Parts" – A Digital Test of Gabriel Tardes' Monads', *The British Journal of Sociology*, vol. 63, issue 4, December 2012, pp. 590–615.
5. Eric Ketelaar, 'Archival Temples, Archival Prisons: Modes of Power and Protection', *Archival Science*, vol. 2, no. 2, 2002, pp. 221–38.
6. Paul Mason, 'The End of Capitalism Has Begun', *The Guardian*, 17 July 2015, available at *<https://www.theguardian.com/books/2015/jul/17/postcapitalism-end-of-capitalism-begun>*, accessed 20 April 2017.
7. Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne and Tamar Tembeck (eds), 'Introduction', in *The Participatory Condition in the Digital Age*, University of Manitoba Press, Minneapolis, 2016, p. viii.
8. ibid., p. xi.
9. Jodi Dean, *Democracy and Other Neoliberal Fantasies*, Duke University Press, Durham, NC, 2009.
10. The origins of this widely used statement are unclear, but it seems to have come into widespread use around 2010, including in a talk given by security expert Bruce Schneier at the RSA Europe security conference in London in October of that year. See 'Facebook is Deliberately Killing Privacy, Says Schneier', *Information Age*, 13 October 2010, available at *<https://www.information-age.com/facebook-is-deliberately-killing-privacy-says-schneier-1290603/>*, accessed 8 August 2017.
11. Alberto Melucci, *Nomads of the Present: Social Movements and Individual Needs in Contemporary Society*, Temple University Press, Philadelphia, 1989, p. 174.
12. Jillian York, 'From *TuniLeaks* to Bassem Youssef', in Barney et al., p. 55.
13. Wikipedia contributors, 'Peer-to-Peer,' *Wikipedia, The Free Encyclopedia*, available at *<https://en.wikipedia.org/w/index.php?title=Peer-to-peer&oldid=774382301>*, accessed 21 April 2017.
14. Bitcoin has been explained as 'a cryptocurrency and a digital payment system. The system is peer-to-peer, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a blockchain. Since the system works without a central repository or single administrator, bitcoin is called the first decentralized digital currency.' Wikipedia contributors, 'Bitcoin', *Wikipedia, The Free Encyclopedia*, available at *<https://en.wikipedia.org/w/index.php?title=Bitcoin&oldid=790397330>*, accessed 14 July 2017. Blockchain has been explained as: 'a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and a collusion of the network majority. Functionally, a blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically."' Wikipedia contributors, 'Blockchain', *Wikipedia, The Free Encyclopedia*, available at *<https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=790001523>*, accessed 14 July 2017.
15. Nozomi Hayase, 'The Blockchain is a New Model of Governance', *Coin Desk*, 26 July 2015, available at *<https://www.coindesk.com/consensus-algorithm-and-a-new-model-of-governance/>*, accessed 21 April 2017.
16. Andreas Antonopoulos, 'Bitcoin Security Model: Trust by Computation', *O'Reilly Radar*, February 2014, available at *<https://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html>*, accessed 20 April 2017.
17. Vitalek Buterin, 'The Meaning of Decentralization', available at *<https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274#.npi0wpwl5>*, accessed 8 August 2017.
18. Michel Bauwens, 'The Political Economy of Peer Production', available at *<https://journals.uvic.ca/index.php/ctheory/article/view/14464/5306>*, accessed 21 April 2017.

19. Peter Van Garderen, 'Decentralized Autonomous Collections', *Medium*, 11 April 2016, available at <*https://medium.com/on-archivy/decentralized-autonomous-collections-ff256267cbd6*>, accessed 26 April 2017.
20. The Australian Bureau of Statistics announced in the lead-up to the 2016 census that they would be retaining name-identified personal data for a period of some years, a divergence from past practice. Public consultation on this change had been minimal, and members of the public and Parliament raised concerns about data security and privacy. The online system used to collect census data was then subjected to a Distributed Denial of Service Attack, causing it to crash. For more see Stilgherrian, 'Censusfail: An Omnishambles of Fabulous Proportions', *ZDNet*, 26 October 2016, available at <*https://www.zdnet.com/article/censusfail-an-omnishambles-of-fabulous-proportions/*>, accessed 21 April 2017.
21. 'Koorie Archiving: Trust and Technology – Final Report', available at <*https://www.monash.edu/it/our-research/research-centres-and-labs/cosi/projects/trust/deliverables/final-report*>, accessed 21 April 2017.
22. ibid.
23. Andrew Flinn, 'Archival Activism: Independent and Community-led Archives, Radical Public History and the Heritage Professions', *InterActions: UCLA Journal of Education and Information Studies*, vol. 7, no. 2, 2011, pp. 1–20. Available at <*https://escholarship.org/uc/item/9pt2490x*>, accessed 8 August 2017.
24. Yvonne Ng, 'Community-based Approaches to Archives from the Black Lives Matter Movement', *Witness.Org*, available at <*https://blog.witness.org/2015/09/community-based-approaches-to-archives-from-the-black-lives-matter-movement/*>, accessed 8 August 2017; Preserve The Baltimore Uprising 2015 Archive Project, available at <*https://baltimoreuprising2015.org/*>, accessed 8 August 2017; Documenting Ferguson, available at <*www.digital.wustl.edu/ferguson/*>, accessed 8 August 2017.
25. Ng.
26. Documenting the Now, available at <*https://www.docnow.io/*>, accessed 8 August 2017.
27. Frank Golding, 'The Care Leaver's Perspective', *Archives and Manuscripts*, vol. 44, no. 3, 2016, p. 162.
28. ibid.
29. Royal Commission into Institutional Reponses to Child Sexual Abuse, available at <*https://www.childabuseroyalcommission.gov.au/*>, accessed 8 August 2017.
30. ibid.
31. The InterPARES Project is an international research initiative in which archival scholars, computer engineering scholars, national archival institutions and private industry representatives are collaborating to develop the theoretical and methodological knowledge required for the permanent preservation of authentic records created in electronic systems.
32. Consultative Committee for Space Data Systems, Reference Model for an Open Archival Information System (OAIS), June 2012, available at <*https://public.ccsds.org/Pubs/650x0m2.pdf*>, accessed 27 April 2017; International Standard ISO/TR 17068:2012, Information and Documentation – Trusted Third Party Repository for Digital Records, available at <*https://www.iso.org/standard/58087.html*>, accessed 27 April 2017.
33. Notably, Bearman's work as presented in *Electronic Evidence* (published by Archives & Museum Informatics, Pittsburgh, 1994) on functional requirements for evidence in recordkeeping.
34. Luciana Duranti, Jim Suderman and Malcolm Todd, 'A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records', March 2008, available at <*https://www.interpares.org/public_documents/ip2(pub)policy_framework_document.pdf*>, accessed 28 April 2017.
35. InterPARES Trust, 'Research', n.d., available at <*https://interparestrust.org/trust/about_research/summary*>, accessed 28 April 2017.
36. Vicki Lemieux, 'Trusting Records: Is Blockchain Technology the Answer?' *Records Management Journal*, vol. 26, no. 2, pp. 110–39.
37. For example, in 2017, various US jurisdictions passed laws recognising blockchain records as a type of electronic record for the purposes of the Uniform Electronic Transactions Act

or local evidence law. Source: Sheppard Mullin Richter & Hampton LLP, 'Nevada Passes Pro-blockchain Law', 14 June 2017, available at <*https://www.jdsupra.com/legalnews/nevada-passes-pro-blockchain-law-15604/*>, accessed 13 July 2017.

38. Greg Bak, 'Trusted by Whom? TDRs, Standards Culture and the Nature of Trust', *Archival Science*, vol. 16, no. 4, 2016, pp. 373–402.
39. Terry Cook and Gordon Dodds (eds), *Imagining Archives: Essays and Reflections by Hugh A. Taylor*, Scarecrow Press, Lanham, 2003, p. 124.
40. This may be demonstrated in the metrics on trust and credibility gathered, for example, for the 2017 Edelman Trust Barometer, a study involving 33,000 respondents across 28 countries. The Edelman report found that two-thirds of the countries surveyed are 'distrusters' (under 50% trust in the mainstream institutions of business, government, media and NGOs to do what is right). Edelman, '2017 Edelman Trust Barometer', 2017, available at <*https://www.edelman.com/trust2017/*>, accessed 22 April 2017. Thanks to Barbara Reed (@BarbaraREED) for linking to this on Twitter.
41. International Organization for Standardization, 'Trusted Third Party Repository for Digital Records' n.d., available at <*https://www.iso.org/standard/58087.html*>, accessed 28 April 2017.
42. Inter Planetary File System is a protocol designed to create a permanent and decentralised method of storing and sharing files. IPFS, available at <*https://ipfs.io/*>, accessed 14 July 2017; Storj is a platform, cryptocurrency and suite of decentralised applications that stores data in a secure and decentralised manner. Storj, available at <*https://storj.io/*>, accessed 14 July 2017.
43. Antony Lewis, 'So, You Want to Use a Blockchain for That?' *Coin Desk*, 22 July 2016, available at <*https://www.coindesk.com/want-use-blockchain/*>, accessed 14 July 2017.
44. Peter Van Garderen, 'Decentralized Autonomous Collections', *Medium: On Archivy*, available at <*https://medium.com/on-archivy/decentralized-autonomous-collections-ff256267cbd6*>, accessed 28 April 2017 .
45. 'Enigma', available at <*https://www.enigma.co/*>, accessed 8 August 2017; 'Estonian e-residency', available at <*https://e-estonia.com/e-residents/about/*>, accessed 8 August 2017.
46. 'Ethereu Homestead Release Blockchain App Platform', available at <*https://www.ethereum.org/*>, accessed 8 August 2017.
47. Antony Lewis, op. cit.
48. Sue McKemmish, 'Evidence of Me', *The Australian Library Journal*, vol. 45, no. 3, 1996, pp. 184–87.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Cassie Findlay has worked as a government archivist, recordkeeping consultant, instructor/lecturer and information policy adviser. She has won a number of industry awards for her writing and for standards development, and has served in committees and leadership roles with the International Council on Archives and the Australian Society of Archivists. Cassie led the establishment of the digital archives program at State Archives and Records NSW, and was the Project Lead for the most recent review of the International Standard on Records Management, ISO 15489. She holds a Master of Information Management (Archives/Records) from the University of New South Wales and a Graduate Diploma in Management. Cassie is a co-founder of the recordkeeping and archives discussion group the Recordkeeping Roundtable. Hailing originally from Sydney, Australia, Cassie relocated to San Francisco in 2016.