The defensible deletion of government email

The defensible deletion of government email

Abstract

Purpose

Two rival approaches to email have emerged from information governance thought:

- the defensible deletion (also called defensible disposition) approach by which emails are routinely deleted from email accounts after a set period of time;
- the Capstone approach where the email accounts of important government officials are selected for permanent preservation.

This paper assesses the extent to which the defensible deletion approach, when used in conjunction with efforts to move important emails into corporate records systems, will meet the needs of originating government departments and of wider society.

Design/methodology/approach

The paper forms the first stage of a realist evaluation of policy towards UK government email.

Findings

The explanation advanced in this paper predicts that:

- the routine deletion of email from email accounts will work for government departments even where business email is inconsistently or haphazardly captured into records systems, provided officials have access to their own emails for a long enough period to satisfy their individual operational requirements;
- the routine deletion of email from email accounts will work for wider society only if and when business email is consistently captured into other systems.

Originality/value

This paper maps TNA's policy towards government email against the approaches to email present in records management and information governance thought, and argues that it is best characterized as a defensible deletion approach. The paper proposes a realist explanation as to how defensible deletion policies toward email work in a government context.

Method

This paper forms the first stage of a realist evaluation of archival policy towards UK government email.

Realist evaluation is a logic of enquiry developed by sociologists Ray Pawson and Nick Tilley (Pawson and Tilley, 1997). Pawson and Tilley argue that in the social world a policy or programme achieves its intended outcome only if targeted stakeholders respond to it in ways intended by policy makers. If policy makers misread the reasoning and likely reactions of targeted stakeholders then the policy may have unwanted effects (Pawson, 2006, p27 and 28).

The UK National Archives (TNA) advises government departments to capture important emails into corporate records systems whilst routinely deleting email from email accounts (TNA, 2016). This paper presents an initial theory of how government departments are likely to react to such a policy. It asks whether they are likely to give:

- **the intended response** - taking serious and effective steps to ensure that important emails are captured into record systems, and promptly deleting emails from email accounts; or
- **an unintended response** - making token efforts to capture important emails into record systems, whilst retaining emails within email accounts for a period judged sufficient to satisfy the operational needs of individual officials.

Realists believe that no policy works for all stakeholders in all circumstances. This paper asks whether, in current circumstances, TNA's policy towards government email is likely to

work for government departments, and whether it is likely to work for stakeholders seeking to hold those departments to account.

Scientific realists believe, after Popper, that scientists in both the physical and social sciences make advances by developing new theories and by exposing the predictions made by those theories to test (Pawson, 2013, p3-5 and p9). Realist evaluation is a theory-driven evaluation method in which the researcher first develops an initial 'programme theory' of how the policy under evaluation works, and then exposes that theory to test.

This paper maps TNA's policy towards government email against the broad approaches to email present in records management and information governance thought, and argues that it is best characterized as a defensible deletion approach. The explanation presented in this paper was built through an exploration of the points of contention between the defensible deletion approach and the alternative Capstone approach that was adopted by the US National Archives and Records Administration (NARA) in 2013 (NARA, 2013). The points of contention are compiled from rival ideas found in the professional discourse on archival policy towards email.

This approach to building an initial theory through examining points of contention in an existing policy debate was recommended by Pawson as a way of ensuring that research was relevant to the questions upon which policy makers have to make decisions (Pawson, 2013, p165-167).

This paper develops an initial explanation of how defensible deletion policies towards government email work, and sets out ways in which this explanation could be tested.

Records management perspectives

Records management perspectives on how correspondence should be organised

The 1990s saw academics and practitioners working to establish recordkeeping approaches to support organisations in coping with the digital revolution that was being ushered in by the widespread adoption of email.

Bearman argued that recordkeeping requirements arose from business activities, and that email accounts were problematic to manage because they typically contained correspondence from a mixture of different business activities. He stated that:

> We cannot make any progress in managing electronic mail unless we can make the system identify the business transaction involved. (Bearman, 1994)

Bearman's insistence that records be linked to the business activity that they arose from was mirrored in the DIRKS methodology for the design and implementation of recordkeeping systems. The methodology was developed in Australia in the early 1990s and was later embedded into the International Records Management Standard (ISO 15489). Step B of the DIRKS methodology involved the analysis of an organisation's activities and the construction of a hierarchical business classification scheme. The methodology was maintained and updated well into the twenty first century (State Records Authority of New South Wales, 2003).

Duranti (1997) argued that one of the functions of a record system was to create an 'archival bond' between the different records of an organisation, by which every single document in the system had a relationship with all other documents within the system. Both Boudrez (2006) and Grandi (2011) used Duranti's theory of the archival bond to argue that important emails should be saved into a records system organised by business activity where they can be related to all other records arising from the same instance of a particular business activity.

The electronic records management system model

Duranti and her University of British Columbia project team collaborated with the US Department of Defense to produce the US DoD 5015.2 standard which outlined the functional requirements of electronic records management systems (Department of Defense, 1997).

The electronic records management model became the standard approach for government bodies in societies such as the US, UK and Australia. In the first decade of the twenty first century many government bodies in these administrations aimed to implement electronic records management systems on a corporate wide basis and instructed their officials to move

important emails into those systems. Since that time however the approach has come in for widespread criticism.

Baron and Attfield reported that:

> Anecdotal experience with DOD Standard 5015.2 applications has shown that many individuals do not reliably save, tag, drag or drop most of their email into electronic folders set up with well- intentioned archival purposes in mind. The compliance rate starts off low in this regard, and is invariably getting lower – simply due to massive volumes of information now confronting us all. Having to perform extra key strokes, no matter how few, on any substantial percentage of electronic communications during the working day, means the equivalent of having to pay a transactional toll per communication, in terms of lost time, energy and productivity. Few individuals wish to pay the price on a consistent and comprehensive basis, hence a world of incomplete if not haphazard recordkeeping. (Baron and Attfield, 2013 p583).

Don Leuders worked as a records management consultant specialising in DoD 5015.2 electronic records management system implementations. He became a strong critic of the electronic records management system approach. In a 2015 blogpost he argued that:

> *Manual email records management solutions will fail to be adopted by end users 100% of the time.* Short of sticking a gun to their head, no information worker is ever going to manually declare and classify email records. (Leuders, 2015).

In 2015, Sir Alex Allan in his review of UK government's digital records, found that the instruction to officials to move email into electronic records management systems 'seems to have been complied with even less rigorously than for other records' (Allan, 2015 p10).

In 2010, in the pages of this journal, James Lappin described the vacuum in records management thought and practice left by the decline and fall of the electronic records management system approach and asked 'What will be the next records management orthodoxy?' (Lappin, 2010). In fact the new paradigm that emerged to fill the vacuum has gone under the name of information governance, and does not think of itself as a records management paradigm.

Information governance perspectives

Information governance can be seen at one and the same time as:

- an umbrella discipline that contains records management as one of its component disciplines, alongside other disciplines such as data protection/privacy, data governance etc.;
- an evolution of records management in which records management is updating itself to adapt to the digital age;
- a rupture with records management that seeks to abandon certain records management beliefs deemed unsuitable for the digital age.

A look at some of the landmark outputs of information governance thought and practice, documents such as the Electronic Discovery Reference Model and Information Governance Reference Model (Duke Law, 2018), NARA's *Electronic Records Management Automation Plan* (NARA, 2014), the ARMA *Information Governance Maturity Model* (ARMA International, 2013), and the Sedona Conference *Principles and Commentary on Defensible Disposition* (Sedona Conference, 2018), reveals key differences between the concerns and ambitions of records management writers of the 1990s and the concerns of information government writers of the second decade of the twentieth century.

Notably absent from the above information governance outputs is

- any insistence that records be organised by business activity;
- any attempt to distinguish between records and non-records, or between records systems and non-record systems.

In their place comes:

- a recognition that any and every information system holds information that needs to be governed in accordance with information governance principles;
- a belief that only automated techniques can scale up to managing the volumes of content created and received by 21st century organsiations.

The information governance perspective does not require that organisations attempt to concentrate their records within one corporate records system. It acknowledges that records are likely to be kept in a variety of business applications that hold a variety of information from a variety of different activities in a variety of formats. The information governance response to this situation has been to focus on developing high level principles, that can be applied in a variety of different environments.

ARMA's Information Governance Maturity Model evolved out of their 'Generally Accepted Recordkeeping Principles'. One of the eight GARP principles states:

> An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements. (ARMA International, 2017).

Two rival policy approaches to email have emerged from information governance thinking:

- the defensible deletion (also called defensible disposition) approach by which emails are routinely deleted from email accounts after a set period of time;
- the Capstone approach where the email accounts of important government officials are selected for permanent preservation.

Neither of these two approaches are perfect, and the preference expressed in many of the documents cited above is for automated solutions if/when they become serviceable. The next section looks at the existing state of play with automation, before looking at the two policy approaches in more detail.

The search for automated approaches

Automation is a broad term. There are many different potential purposes for the deployment of automation in relation to email, and many different automation methods to support those purposes.

Brogan (2009) and Baron and Attfield (2011) have regarded the simple act of capturing each email into an email archive as 'automation'. NARA categorized the Capstone approach as an

automated approach (NARA, 2014 p11), presumably because it captures emails as records without end-users having had to take any action.

Any development of an automated capability to identify and classify important emails would offer the prospect of bringing back to life the electronic records management system model and the ambition of integrating emails with other records arising from the same business activity. However commentators seem to have little confidence that a corporately scalable analytics, machine learning and/or search capability has yet emerged to automatically identify and classify important emails.

Leuders writes:

> Automated record classification using content analytics products doesn't work for emails…. even the best content analytic products require a minimum level of information to 'understand' and classify any item with an acceptable level of confidence. And given the extreme brevity and routine informality of most emails, the truth is they can very rarely be classified successfully in any real-world implementation. (Leuders, 2015)

In 2017 the UK Cabinet Office wrote:

> Some have argued …that it would be more effective to automate information management completely and remove general civil servants from the process. Although appealing, this is currently unfeasible in practice: technology (specifically the inability of analytics tools to identify context) is not powerful enough to remove any need for proper naming and saving. (Cabinet Office, 2017, p15)

The defensible deletion approach to email

The defensible deletion approach to email is based on the belief that emails accumulated in email accounts are of low value but high risk to the originating organisation, and that it is in the organisation's interests to delete them as soon as is operationally practical, whilst exempting from deletion emails for which there exists an ongoing legal obligation to retain.

Defensible deletion and information governance

The Sedona Conference stated that:

> The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program. (Sedona Conference, 2018)

They stated three principles for the defensible disposition of information:

- Absent a legal retention or preservation obligation, organizations may dispose of their information;
- When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention;
- Disposition should be based on information governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives. (Sedona Conference, 2018)

The rationale behind the defensible deletion of email

Turner (2014) quotes two cases where US courts had declined to take sanctions against an organisation that had been unable to produce email correspondence requested by the other party because they had deleted it under a routine deletion policy. He argued that deletion of information was likely to be acceptable to a court provided it was 'neutral, systematic, and universally applied' and provided legal holds were applied when required.

An example of a defensible deletion approach to email in government context was provided in a listserv post by a practitioner (Records Management UK listserv, 2015). The practitioner vividly described the inconvenience, cost and risk to her organisation of retaining email in email accounts:

> We brought in email archiving here to save £1 million in storage costs (e-storage is cheap, eh?). We later brought in a 7 year deletion rule for archived emails because the archive couldn't cope with the quantity of emails and nor could our Compliance and Legal teams, who were having to plough through millions of

> rubbish emails for FOI [Freedom of Information], DPA [Data Protection Act] or e-discovery. We advise that emails of value must be saved outside the archive in the relevant shared storage area (but with only 2 records managers we can't monitor or enforce this).

The approach of the above organisation is better characterised as a defensible deletion approach than an electronic records management system approach. The organisation was asking its officials to move important email into record systems, but no confidence was placed in the adequacy of capture of important emails into corporate records systems or shared areas. The justification for the routine deletion of email was the cost, risk and inconvenience of the retention of email beyond the 7 year period.

The Capstone approach to email

The ideas behind the Capstone policy

In a 2011 presentation Jason Baron, then NARA's Director of Litigation, set out a new policy approach to email that would later become known as the 'Capstone' approach.

Baron proposed that all emails created or received by senior officials be designated for permanent preservation. One downside of retaining the email account of a senior official permanently is that the email account is likely to contain personal and trivial mail. Baron proposed that:

> Agencies concerned about over-inclusion of email of a personal or truly ephemeral nature could allow for staff to delete emails from the in-box for a limited period of time (e.g. 60 or 120 days) with any emails remaining then automatically captured as permanent. (Baron and Attfield, 2013 p587)

NARA's Capstone policy for the email of federal agencies

In August 2013 NARA announced its Capstone policy on email, via a bulletin issued to heads of US federal agencies. The bulletin asked agencies to schedule the email accounts of officials at or near the top of an agency for permanent preservation, and allowed agencies to

determine for themselves whether those officials could delete non-record, transitory, or personal email from their accounts (NARA, 2013).

In NARA's own Capstone implementation they identified 48 roles as being Capstone roles, and gave those 48 officials a 'safe harbor' period during which they could delete emails they regarded as personal or trivial, prior to emails being archived (Sullivan, 2014).

The Capstone Retention Schedule

In April 2015 NARA issued a Capstone Retention Schedule to federal agencies (NARA, 2015). The schedule set out three retention rules for federal email:

- email in the email accounts of senior officials should be retained permanently;
- email in the email accounts of other officials (with the exception of officials in support and administrative roles) should be retained for seven years;
- email in the email accounts of support and administrative roles should be kept for three years.

Key features of the Capstone approach

Three distinct features of the Capstone approach are that it:

- **endeavours to make email accounts manageable** whereas the electronic records management system approach and the defensible deletion approach had both argued that email accounts were unmanageable;
- **focuses end-users on identifying trivial and personal email to be deleted from email accounts** whereas previous approaches had focused end-users on identifying important emails to move into a records system;
- **makes no attempt to assign emails to the business activity that they arose from** email accounts are subject to retention rules that are based on the roles carried out by the account holder.

Policy towards UK government email

TNA has kept an unchanged policy to email throughout the past two decades, namely that important emails should be moved into corporate records management systems whilst emails in email accounts should be subject to routine deletion. During this time the thinking of TNA towards information management in general has changed considerably, in line with a general shift from records management to information governance thinking.

In the first half of the first decade of the twenty first century TNA policy on email drew its justification from the electronic records management system approach. At the time TNA was running a certification regime for electronic records management system products, and belief in the electronic records management system model was strong amongst the practitioner community, the vendor community and the academic community.

In the second decade of the twenty first century belief in the electronic records management system model faded, and TNA's policy on email now appears to draw its justification from a defensible deletion logic. TNA's latest restatement of its email policy came in 2016, when it issued its *Guidance Principles on the Auto-deletion of Email* (TNA 2016). These guidance principles were sandwiched between two important reports: Sir Alex Allan's *Review of Government Digital Records* (Allan, 2015), and the *Better Information for Better Government* report (Cabinet Office, 2017) which responded to Allan's findings.

Sir Alex Allan found the capture of email into government electronic records systems to be ineffective and recommended that the government consider adopting a Capstone approach to email (Allan, 2015, p10). The Cabinet Office in response made no denial that the capture of emails into record systems was ineffective, but rejected Allan's Capstone recommendation on the grounds that the selection of important email accounts for permanent preservation was likely to cause personal and trivial correspondence to be retained longer than necessary. In the opinion of the Cabinet Office this over-retention would be contrary to UK data protection principles, the GDPR, and UK public records legislation. (Cabinet Office, 2017 p10).

TNA's *Guidance Principles* state that 'under an auto-deletion rule information of value must be identified and not deleted' (TNA, 2016). However nowhere in the *Guidance Principles* is there a mention of any mechanism that would make deletion of emails from an important email account conditional upon adequate capture of correspondence from the account into an electronic records management system.

There is one paragraph that deals with capture:

> ***Automatically capture emails*** *– Implement technologies that integrate your email and EDRM solutions. Solutions that allow emails to be dragged and dropped or automatically captured into the corporate records area will assist in allowing users to comply with your records management and retention policies.* (TNA, 2016)

We have seen that the Cabinet Office, writing a year after these guidelines, had no faith that the process of record capture could be automated. 'Drag and drop' is a manual rather than automated process and Allan had found the capture of email into record systems to be ineffective despite the deployment of 'drag and drop' by many government departments.

Exploring the points of contention between the defensible deletion and Capstone approaches

The proportion of email correspondence that needs to be treated as a record

There is little significant difference between the defensible deletion and the Capstone approach when they are applied to the email accounts of officials that are not dealing with matters of which government departments/agencies are expected to keep a permanent record. Both approaches would typically result in the deletion of the contents of such email accounts after a relatively short number of years.

There is a very significant difference between the defensible deletion approach and the Capstone approach when applied to the email accounts of officials that are dealing with matters of which government departments/agencies are expected to keep a permanent record. In the continued absence of automation:

- a defensible deletion approach is likely to result in the deletion of most of the contents of such accounts after a relatively short number of years (saving only those emails which have, by exception, been moved to a corporate record system or placed under some sort of legal hold);

- a Capstone approach is likely to result in the permanent retention of most of the contents of the email accounts of such officials (saving only those emails which have, by exception been identified as personal or trivial).

When applied to the email accounts of officials in important government roles, defensible deletion, in the absence of automation, is likely to result in an under-retention of correspondence of historic value. At the time of writing the predominant method for identifying important emails is to ask officials to move such emails into a corporate record system. This method has been sharply criticised by commentators, as related above, and evidence suggests it is inadequate for the task.

A Capstone approach would also be dependent on the judgement of officials – this time to identify trivial and personal items of correspondence. We can anticipate that it would in most cases result in an over-retention of trivial and personal email (although it is also possible that in some cases officials may be tempted, or instructed, to use the safe harbour period to delete politically contentious correspondence).

In adjudicating between a Capstone policy and a defensible deletion policy the key judgement to be made concerns the extent to which email correspondence has value (or lacks value). This question can be formulated as follows: is society likely to need, for the purposes of historical accountability, to have the major part of the correspondence of the key officials of its administration retained permanently? Or would the retention of a minority of the correspondence of key officials suffice?

Different perceptions of the value of email

The views of information governance commentators, archivists and records managers are sharply divided when it comes to the question of the extent to which email correspondence has value.

The practitoner quoted above had been scathing in her listserv post about the millions of 'rubbish emails' that cluttered up her organisations' email archive (Records Management UK listserv, 2015).

Leuders holds a similar view of the lack of value possessed by email in email accounts:

> ***Very few emails actually hold any real long term value…*** in reality, all but an extremely small number of emails at almost any given organization are worthless soon after they are sent. Yep, *worthless*. What's more, with a few simple, strategic records management policies in place, those few emails could likely be eliminated, too. (Leuders, 2015).

Leuders holds that emails are not only worthless but also potentially dangerous:

> …people tend to write really stupid stuff in emails. Far more idiotic stuff then they would write anywhere else. (Leuders, 2015)

However there is evidence that those elements in society who seek to hold government to account regard email accounts as a valuable record. Andrew Waugh, policy manager for the Public Record Office of Victoria in Australia, wrote that:

> Evidence of the value of email systems as record systems can be found in any modern governance or accountability investigation, such as a royal commission, audit report, ombudsman's investigation, or even in investigative journalism. Without exception, emails form the key planks of a modern investigation and feature prominently in the final report. In 2012, the then Victorian Auditor General and Victoria's Deputy Ombudsman, independently, told a seminar of Victorian records professionals that, while their investigators looked at the records [in electronic records management systems], the smoking gun was always in the email. (Waugh, 2014)

The difference in viewpoint between Leuders on the one hand and the Victorian Auditor General on the other can be identified as a simple difference of interest: an auditor is looking for smoking guns whilst a records manager is working for organisations who may be concerned about what smoking guns lurk unnoticed in their email servers.

Cox identified back in 2008 the possibility of a divergence of interests in relation to email correspondence, with records managers, thinking of their own organisation's interests, wishing to destroy correspondence in email accounts after a relatively short time, and archivists, thinking of society's interest, wanting some email accounts to be preserved permanently (Cox, 2008).

In the next section this paper hypothesizes that the polarization of views on the value of email are a consequence of the fact that the switch of correspondence medium from hard copy to email radically increased the cost and risk to originating organisations of keeping correspondence. This cost and risk is born by originating organisations, not by external society. It hypothesizes that from society's point of view the value of correspondence appears to be undiminished after the move from hard copy correspondence to email.

Towards an explanation for differing perceptions of the value of email

The disintermediation and decomposition of correspondence

The coming of email in the 1990s brought with it the '3vs' 'volume, velocity and variety' which Laney (2001) argues characterises information in the digital age. Email disintermediated correspondence, collapsing the time and space between sender and recipient, and removing the intermediaries between them.

This disintermediation increases the velocity of correspondence by allowing recipients to reply to an email within minutes. Any increase in the velocity of correspondence leads to an increase in the volume of correspondence exchanged within any one day, month, year. In effect correspondence is decomposed into smaller units.

This paper hypothesises that the greater the velocity of correspondence the less time an individual has to think about what they are writing and the less guarded each individual item of correspondence becomes.

It can therefore be expected that the correspondence of any given senior official poses a greater risk to a government department after the coming of email than would the correspondence of a similar senior official before the coming of email.

The value of email in aggregation

This paper makes the hypothesis that the total value of the correspondence exchanged by a senior official *after* the coming of email is neither significantly greater nor lower than the

total value of all the correspondence exchanged by a similar senior official *before* the coming of email.

This hypothesis can be tested in a thought experiment. The hypothesis implies that if the UK had decided to exit the European Union prior to the coming of email (for example in 1989) the historical value to society of the correspondence of a senior official working on aspects of UK strategy for the exit would have been neither greater nor lesser than the historical value of the email correspondence of an official charged with a similar task in 2016.

The average number of items of correspondence exchanged per day has been exponentially larger after the adoption of email than before. It can therefore be predicted that the average value of each item of correspondence is exponentially *smaller* after the adoption of email than before.

If this theory of the decomposition of correspondence is true then two consequences logically follow:

- the email correspondence of a senior official may still have immense value in aggregation, even while individual emails within the account lack any appreciable value on their own - the perception of Leuders that emails are worthless is not therefore in contradiction with the perception of the Victorian Auditor General that email accounts are more valuable to an investigation than are corporate record systems;
- any approach that seeks to identify emails of exceptional importance to move into a record system is unlikely to enable the adequate reconstitution of the business correspondence of a senior official.

Predicting the reaction of government departments to TNA's policy towards email

The possible reactions open to government departments

An archival policy advising government departments to move important email into corporate record systems whilst deleting those emails that remain in email accounts could result in one of three response from government departments, only one of which is the intended response. The department could either:

- take serious and effective steps to move business emails into corporate record systems accompanied by the short term deletion of email from email accounts*;*
- make token efforts to move business emails into corporate record systems, accompanied by the routine deletion of email from all email accounts*;*
- make token efforts to move business emails into corporate record systems accompanied by the retention of some, most or all email accounts as records.

The next section of this paper attempts firstly to identify whether government departments are likely to routinely delete email from email accounts, and then attempts to predict whether departments are likely to take serious steps to move business emails out of email accounts.

The deletion of email from email accounts

Email accounts are the first method of organizing correspondence in the history of government recordkeeping that does not allow an official new-to-post to view the correspondence of their predecessor (see Zhang, 2015 for a history of the organisation of correspondence in the United States). The fact that personal correspondence is typically present in individual email accounts means that the email account of any official cannot usually be made accessible to their successor.

Waugh wrote that the time periods set for the deletion of emails from email accounts

> …are usually absurdly short and certainly not based on any analysis of the functions the records support. (Waugh, 2014)

TNA stated in 2016 that the period after which UK government deleted email from email accounts varied from department to department but was ‘currently ranging from 90 days to four years’. (TNA, 2016, p2)

The deletion of the correspondence of say, a senior government economist, after four years or less does indeed look to be an 'absurdly short' period when compared with how long the correspondence of such an official is likely to have been kept before the coming of email. However there is a pragmatic reason behind this absurdity. The retention of an email account, even of a very important official, gives no benefit to a government department *for day-to-day operational purposes* once the individual email account holder has left their post.

This paper hypothesises that:

- government departments are indeed likely to delete emails routinely from email accounts as intended by the TNA's policy, but for different motivations than TNA intends;
- the deletion will be carried out irrespective of how low a percentage of business correspondence is captured into corporate record system or other shared area;
- the deletion happens not because the department is confident that business email is adequately captured into corporate records systems, but because the department knows that the retention of email in email accounts brings them no operational value once an individual official has left his/her post.

The capture of business emails into corporate record systems

The findings of Sir Alex Allan's review of government digital record keeping (Allan, 2015) suggests that UK government departments have not taken effective steps to move important emails into record systems. One way of interpreting this would be to argue that the hypothesis advanced in this paper (that the email correspondence of an important official has value in aggregate) must be wrong on the grounds that:

- if a record is important enough to have permanent value to society it will also be important to the government department, at least in the short to medium term;
- the willingness and ability of government departments to function with only a tiny minority of their business correspondence being captured into a record system implies that only a tiny minority of an official's correspondence is needed as a record.

An alternative reading however is that the reason why government departments have not taken effective steps to capture business emails into record systems may be because their

officials are able to refer to emails in their email accounts for all or most of the period in which their correspondence is likely to be of most use to them, namely the two years after the correspondence is sent and received. In this hypothesis government departments are using email systems as record systems, without treating them as record systems.

Baron and Attfield described this phenomenon when they wrote about email archive tools. These tools enabled organisations to store the bulk of the contents of email accounts outside of their live email servers by simply capturing every email sent or received into the archive. Baron and Attfield argued that an email archive would

> … be perceived to be an institution's *state of the art records management scheme* and it will be increasingly difficult to convince end-users to continue any semblance of other means of recordkeeping in the face of the knowledge that email archiving exists. (Baron and Attfield, 2013 p583)

Baron and Attfield predicted that emails in email archives would be like 'fireworks' - very important for a short period of time, but leaving no permanent trace behind them. They ascribe this to:

> the desire on the part of institutions to save everything for the here and now, but to delete (almost) everything after a prescribed period of years. (Baron and Attfield, 2013 p583)

Baron and Attfield's explanation fits in with the hypothesis advanced in this paper that the bulk of an official's correspondence is needed as a record of their work.

The coming of email, coupled with the trend of increasing access-to-information rights for citizens, has substantially increased the total cost, inconvenience and risk to government departments of keeping the business correspondence of an official, without increasing the total value of that correspondence.

The value of the correspondence of any official to government departments tends to degrade over time. It can be hypothesised that the point in time at which the cost and risk to a department of retaining business email correspondence outweighs the value to them of keeping that correspondence arrives far quicker after the coming of email than it did before the coming of email.

If a government department was to succeed in moving business email correspondence into a corporate record system, then that correspondence would be governed by retention rules that are comparable to those set for pre-email correspondence. It can be hypothesized that this would result in the department having to retain correspondence long after its cost and risk exceeded its value to them.

The instruction to officials to move important emails into corporate record systems has survived in UK government and elsewhere long after the records management beliefs that underpinned it have disappeared. This paper hypothesises that the instruction has survived because it imposes little or no burden on officials. They have no need to comply with the instruction because they have access to correspondence in their email accounts for as long as they are likely to need it. Their department is unlikely to try to enforce the instruction (for example by deleting emails from email accounts after a very short time period) as enforcing it would add to their cost and risk by capturing a higher volume of email into records systems.

Towards a realist explanation of TNA's policy towards UK government email

An initial explanation

The initial realist explanation advanced in this paper is that government departments will for the most part regard business email correspondence as a cost, a risk and a liability. They will therefore refrain from making serious efforts to move the bulk of business email correspondence from email accounts into record systems, for fear of simply transferring the cost and risk from one system to another. They will instead allow officials to keep emails in their email account for as long as they need them for their individual operational needs.

The initial explanation hypothesises that:

- a majority of the email correspondence of key officials, and in particular a large majority of the sent items, are business emails;
- injunctions to officials to move important records into a record system currently result in only a tiny minority of items of business correspondence being moved into a record system;

- even when automated techniques become available, government departments are unlikely to apply them to the task of identifying business email and moving it into record systems as any such application of automated techniques would result in a very large and very unwelcome increase in the volume of email captured into corporate record systems.

Exposing the explanation to test

The paper concludes with what, from a realist evaluation point of view, is the most important part of the paper, the part that exposes the proposed explanation to test by making specific predictions about observable reality.

The initial explanation advanced in this paper may be tested by establishing:

- **the proportion of sent emails captured into corporate record systems** – the explanation predicts that a very small percentage of sent items are captured into government records systems;
- **the length of time government departments allow emails to remain in email accounts** – the explanation predicts that government departments rarely if ever routinely delete correspondence in a short enough time to incentivise officials to move emails to record systems;
- **whether the routine deletion of email from email accounts is conditional on adequate capture of business email into record systems** – the explanation predicts that government departments will continue with routine deletion even when they know that they are not consistently capturing business email into corporate record systems;
- **the extent to which government departments use automated methods to identify important emails and move them to a record system** - the explanation predicts that government departments will rarely choose to apply automated technologies such as machine learning, auto-classification or analytics to the identification of important emails, even when the department is applying such technology to other types of record.

REFERENCES

Allan, A. (2015), "Review of Government Digital Records", Cabinet Office, available at: https://www.gov.uk/government/publications/government-digital-records-and-archives-review-by-sir-alex-allan (accessed 25 March 2017).

ARMA International (2013), "Information Governance Maturity Model".

ARMA International (2017), "Generally Accepted Recordkeeping Principles".

Baron,J.R. and Attfield, S. (2013), "Where Light in Darkness Lies, Preservation, Access and Sensemaking Strategies for the Modern Digital Archive", in *Proceedings of The Memory of the World in the Digital Age: Digitisation and Preservation. An international conference on permanent access to digital documentary heritage, 26-28 September 2012, Vancouver, British Columbia, Canada,* UNESCO 2013, available at: http://www.unesco.org/new/en/communication-and-information/events/calendar-of-events/events-websites/the-memory-of-the-world-in-the-digital-age-digitization-and-preservation/. (accessed 18 August 2018).

Bearman, D. (1994), Managing Electronic Mail, *Archives and Manuscripts*, Vol. 22 No.1, pp. 28–50.

Boudrez F. (2006), Filing and archiving e-mail, Antwerp, , available at http://www.edavid.be/docs/filingArchiving_email.pdf , (accessed 11 September 2018).

Brogan, M. (2009), "Clipping Mercury's Wings: The Challenge of Email Archiving'. *Archives and Manuscripts* Vol. 37 No. 1, pp 12-26.

Cabinet Office (2017), "Better Information for Better Government", available at https://www.gov.uk/government/publications/better-information-for-better-government (accessed 11 September 2018).

Cox, R.J.(2008), *Personal Archives and a New Archival Calling: Readings, Reflections and Ruminations*. Duluth, Minnesota.

Department of Defense (1997), "Design Criteria Standard for Electronic Records Management Software Application - DoD 5015.2-STD".

Duke Law (2018) "Electronic Discovery Reference Model" available from https://www.edrm.net/frameworks-and-standards/edrm-model/ (accessed 19 October 2018).

Duranti, L. (1997), "The Archival Bond" *Archives and Museum Informatics* Vol.11 No. 3–4, pp 213–218.

Grandi, M. (2011), "Guidelines and Recommendations for E-Mail Records Management and Long-Term Preservation", available from http://www.interpares.org/ip3/display_file.cfm?doc= ip3_italy_gs05b_final_report.pdf (accessed 24 September 2018).

Lappin, J. (2010), "What will be the next records management orthodoxy?" *Records Management Journal,* Vol 20 No. 3, pp. 252-264

Laney, D. (2001), "3D data management: Controlling Data Volume, Velocity and Variety" Meta Group, Gartner, available at https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (accessed 11 August 2018).

Leuders, D. (2015), "Email Records Management- Part 1: The Truth" (blogpost), available at https://nextgenrm.com/2015/12/30/email-records-management-part-1-the-truth/ (accessed 11 August 2018).

NARA (2013), "NARA Bulletin 2013-02: Guidance on a New Approach to Managing Email Records (aka "Capstone")" http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html (accessed 10 May 2017).

NARA (2014), "Managing Government Records Directive: Automated Electronic Records Management Report/Plan", available at https://www.archives.gov/files/records-mgmt/prmd/A31report-9-19-14.pdf (accessed 11 August 2018).

NARA (2015), "White Paper on The Capstone Approach and Capstone GRS" . Available from: https://www.archives.gov/files/records-mgmt/email-management/final-capstone-white-paper.pdf, (accessed 28 March 2017).

Pawson, R. (2006) *Evidence-based Policy*, Sage.

Pawson, R. (2013), *The Science of Evaluation,* Sage.

Pawson R. and Tilley N. (1997), *Realistic Evaluation,* Sage.

Records Management UK listserv (2015), "Re: Do you ask questions about records management as part of weekly meetings or annual appraisals?", available at: https://www.jiscmail.ac.uk/cgi-bin/webadmin?A2=ind1506&L=RECORDS-MANAGEMENT-UK&F=&S=&P=95953 (accessed 31 August 2018).

Sedona Conference (2018), "Principles and Commentary on Defensible Disposition" (Public Comment Version), available at https://thesedonaconference.org/sites/default/files/publications/Principles%20and%20Commentary%20on%20Defensible%20Disposition.pdf (accessed 31 August 2018).

State Records Authority of New South Wales (2003) "Strategies for Documenting Governance Business: the Dirks Manual", available at https://www.opengov.nsw.gov.au/publications/17383 (accessed 26 October 2010).

Sullivan, S.J. (2014), "NARA's Capstone Email Management Implementation: Technical Perspective" (powerpoint presentation), available from https://www.archives.gov/files/records-mgmt/email-management/capstone-technical-perspective-session-03-11-14.pdf (accessed 20 August 2018).

TNA (2016), "Guidance Principles on the Auto-Deletion of email", available from http://www.nationalarchives.gov.uk/documents/information-management/guidance-principles-on-the-deletion-of-email.pdf (accessed 9 September 2018).

Turner, R. (2014), 'The Case for Defensible Deletion' in The Global Legal Post, published 16 May 2014, available at http://www.globallegalpost.com/blogs/commentary/the-case-for-defensible-deletion-8135494/ (accessed 14 August 2018).

Waugh, A. (2014), "Email–a bellwether records system" in *Archives and Manuscripts,* Vol. 42 No.2, pp.215-218, available from: http://rkroundtable.org/2014/06/30/email-a-bellwether-records-system/ (accessed 25 March 2017).

Zhang, J (2015), "Correspondence as a documentary form, its persistent representation, and email management, preservation, and access", *Records Management Journal*, Vol. 25 No.1, pp. 78-95.