

# The Trouble with Retention and Disposition

---

How well is your firm coping with the growing pressures to manage data retention and disposition cost effectively and compliantly?





# The Trouble with Retention and Disposition

Chris Giles and Kandace Donovan | 17.10.2022

How well is your firm coping with the growing pressures to manage data retention and disposition cost effectively and compliantly? In this article, **Chris Giles** and **Kandace Donovan** explore the issues in more depth, point out the dangers, and suggest what best practice in data lifecycle management can look like.

Something that comes up a lot when we talk to law firms is that they don't have problems any more with data retention and disposition. COVID gave them the chance to digitally transform processes and scan their existing paper records. Scanning has vastly reduced the volume of physical records storage. Therefore, the firm's storage costs are now much more manageable. The problem has gone away. Or has it?

We believe it's a mistake to assume that all the firm's issues around data retention and disposition can be resolved by scanning. It's certainly the case that in the last few years the costs of physical storage have become uncomfortably high. Some big London law firms, for instance, are reportedly spending around £1m on storage annually. But the bad news for firms

that have scanned their documents is that the costs of electronic storage are also creeping up.

In particular, as firms look to transition from on-premise servers to cloud-based document management systems, they're finding that electronic data storage costs can also be prohibitively high. In particular it can cost firms a lot of money just to move from a maintenance model to a cloud-based subscription. This should increasingly propel firms to try to reduce their cost base by reducing the amount of data held.

As well, this inconvenient truth about storage costs crashes hard up against the fact that – traditionally, at least – lawyers are believed to be very much in favor of keeping everything forever. Ironically this stems from their supposedly risk-averse natures. The

irony lies in the fact that, as we'll see, increasingly there's actually as much risk, if not more, attached to keeping data as there is to getting rid of it. So, this article is about why firms need to adopt a more organized, balanced and long-term approach to data retention and disposition, why that's so hard, and how to get it done.

## The drivers of destruction

We've already covered cost as a major reason why law firms ought to be rationalizing the amount of data they keep. Firms of every size, in every country and location, are facing mounting storage bills. But there are also other costs that can result from a lack of systematic data retention and disposition. For one thing, when your excess storage is electronic, there's a heightened risk that the firm will be the victim of a cyberattack – simply because the attack surface is larger. And be in no doubt that the costs of a data breach can be considerable when they include lost productivity, ransomware payments (often more than one per breach), regulatory fines and the costs of hiring specialist data security experts so it doesn't happen again. Not to mention the reputational damage.

You might also argue that a data breach is more about data security than data management. But tell that to Tuckers Solicitors LLP, a UK criminal law firm with around 150 lawyers that was the subject of a ransomware attack in 2020. The attack led to the content of 60 court bundles – including medical files, witness and victim statements, and names and addresses – being published on the dark web.<sup>1</sup>

The UK regulator (the Information Commissioners Office) decided that Tuckers was liable for a fine because it had been negligent in implementing the appropriate technical and organizational measures, rendering itself vulnerable to attack. The point to note is that this negligence included breaching Article 5(1) (e) of the UK's Data Protection Act 2018, which requires personal data to be kept in a form that permits the identification of data subjects "for no longer than is necessary for the purposes for which the personal data is processed." In other words, Tuckers had hung on to this data for too long. The ICO felt the breach was sufficiently serious to warrant enforcement action, and the firm was fined 3.2 per cent of its gross annual income.

## Privacy legislation

As you know, the UK Data Protection Act – the UK's version of the EU's General Data Protection Regulation (GDPR) – is only one of many newish pieces of legislation created to safeguard the privacy of personal



data (often called PII for Personally Identifiable Information). Canada has its Anti-Spam Legislation (CASL). In lieu of federal regulation, the US is set to have an increasingly complicated maze of state legislation. As of July 2022, California, Colorado, Utah, Virginia and Connecticut had already signed state data privacy legislation into law and a further five north eastern states had draft legislation in committee.<sup>2</sup>

In respect of data retention and disposition, law firms will almost always hold some PII data, including dates of birth, addresses, social security numbers and banking information, in anything from property deeds to due diligence on directors done in the commission of M&A work. The net result is that this new legislation is driving firms in both Europe and North America to recognize they need to have policies and processes in place, or they run the risk of non-compliance and fines – for holding data they shouldn't, for holding data too long, and for failing to respond quickly enough to data subject access requests.

Nor are data privacy regulations the only type of compliance that firms call foul of. In the US, Sarbanes-Oxley Act 2002 (SOX or Sarbox) covers financial reporting, but also record keeping. This asks for organizations to retain financial information for set periods of time and in some cases indefinitely. SOX has sensitized corporate America at board level to the importance of data retention and disposition.

A final motivation for getting to grips with data retention and disposition is simply because there's a cost to spending too long searching for information because you have so much to wade through. There's also

a cost to recreating documents that can't be found. And in some circumstances, there may well be fines if things are never found or not found quickly enough, as Cushman & Wakefield plc, a real estate services firm in Chicago, has discovered.

In July 2022 Cushman & Wakefield was held in contempt of court for failing to comply with subpoenas to produce documents relating to an investigation by the New York State attorney-general into the financial practices of longtime client Donald Trump and the Trump Organization. Cushman & Wakefield had produced “hundreds of thousands” of documents, but not what the court wanted. And whether it honestly couldn't find them or simply didn't want to, the firm incurred fines of \$10,000 per day until the documents were forthcoming. It illustrates another potential cost of not being in control of data in an efficient way.<sup>3</sup>

In summary, and given this thicket of regulatory and legislative complication, it follows that the less data firms retain unnecessarily, the less risk they're exposed to, the less resource they need to manage it, and the easier it is to control. So much for why firms should get on top of record retention, disposition and destruction; next, what are the challenges of doing so?

## The challenges of retention and disposition

It's probably fair to say – as with much else in life – that if data retention and disposition was easy, everyone would be doing it. The challenge is that there are a lot of moving parts, and it's especially hard at the

beginning because that's the point at which firms must confront and tame the largest volume of data.

The first step is understanding what you have, in both electronic and physical formats. Almost inevitably material will straddle many systems, media and decades and will be dispersed across several sites, including remote archive facilities. Law firms must also take into consideration that it's not just work product that they're the stewards of. There will also be other administrative records, most notably HR files and financial records.

Once the firm knows what it has, it then needs to determine the “trigger” dates for everything held. These will be used to populate the firm's retention schedule – we will discuss this more later. The trigger date is the date that triggers some action in respect of the data, either when it should be sent off site, archived, destroyed, or returned to the client. Returning material to clients is jurisdiction-dependent. In the US, for example, most Bar Associations see matter material as belonging to the client and therefore clients should be contacted and given the option of having it returned or destroyed.

Conversely, in the UK, firms don't routinely return material to clients unless there's a specific request to do so from the client, or it's in Outside Counsel Guidelines (OCGs), or it's stipulated in the engagement letter. (Unsurprisingly, as firms realize the full cost and complexity of record retention and disposition, they're increasingly likely to cover the issues in client engagement letters, which might include details such as what defined step closes the matter, what will be returned





to the client, what happens if the firm can't find the client at that point, what will be destroyed, etc. But that doesn't help firms dealing with material acquired before such provisions were in place.)

Returning to trigger dates – these will also be determined by jurisdiction. The retention period for matter material is generally at least five years in most jurisdictions and typically either seven or 10 years. But what does that actually mean? Is it 10 years after the matter closed, or 10 years from when the firm no longer worked with the client, or 10 years after billing activity ceased even if the matter remains open? (Some matters are never closed.) Firms need to make a clear decision on this.

Meanwhile for HR records, the trigger date will likely be a predefined period after the date the individual left the firm. And financial records are typically ready for review seven years on from the end of the financial year they relate to. But caution needs to be exercised because, as noted, retention periods will change from jurisdiction to jurisdiction, and so within a global firm, potentially from office to office.

In addition, retention periods will also vary between practice groups – because some types of records need to be retained for longer than others. Specifically, wills, property deeds and other documents with a “wet” (i.e. ink) signature need to be kept for much longer – although the supporting documents that contributed to the final will or deed don't usually have to be kept beyond the jurisdictional period.

Then there are the exceptions. If the firm has reason to believe that there may be some type of future action or litigation in relation to any given matter, client or activity, then the pertinent information should be retained. Many lawyers like this a lot and may want to use it as a pretext to keep nearly everything. But also bear in mind that in many jurisdictions there's a statute of limitations for legal malpractice (known as the limitation period in the UK).<sup>4</sup>

Also, in lieu of statutes of limitation applying, common sense should prevail. Say a matter covers the purchase of a business. Ten years after the transaction has been completed, the likelihood of litigation will be very low, so a 10-year retention schedule should be considered reasonable.

Another exception – as alluded to above – is when the OCGs stipulate the retention period. So, firms also need to keep track of any commitments that will override “standard” trigger dates, along with any non-standard data destruction requirements.

## The challenges of enforcement

Once firms know what they have and they know the respective trigger dates, they then need to feed



these into a retention, disposition and destruction schedule that is controlled by the firm's retention policy and supported by agreed procedures. Policies and procedures are needed to ensure that the necessary steps for safe retention and disposition are conscientiously followed by everyone. Because another risk is that the firm doesn't enforce its own policy. And when materials slated for destruction get kept, or records that should be kept are destroyed, it can expose the firm to yet more risk, suspicion, investigation, and liability.

The policy also has to be legal and reasonable. For instance, a court would likely rule that destroying all complaints about the firm isn't reasonable. Procedures have to be put in place. For instance, a procedure for suspending a destruction schedule should the need arise. It all needs to be signed off by firm management and department heads because it's important they understand and agree to follow the firm's retention schedule. Unfortunately, however, we've heard of instances where the retention schedule takes months if not years to be approved by the necessary individuals.

Once there's an approved retention policy and schedule in place, it becomes a matter of following through on what's mandated. This can also be hard. Especially the first time that a firm, particularly a larger or older firm, starts putting a retention schedule into practice, it will likely entail a really big effort, because there's probably a great deal of material to get through and some of it may be very old. It's often the case that firms have material going back decades. We even know of some UK firms with records dating back to the 1700s.

The complication of the task is deepened by the need to rule out the possibility of future litigation, or to check for historic value before destruction. It's particularly hard to assess matters if the attorneys who worked on them have moved on or passed on. And sometimes the client no longer exists – but that needs to be verified, and beneficiaries sought. Firms need to try to locate entities in such a way that they can demonstrate due diligence to a court if necessary. Some US firms are dedicating whole departments and extraordinary amounts of effort to this task.

There's also the problem that none of this work produces any revenue. Which will dull the appetite of any senior lawyer or partner who's tasked with spending unbillable hours reviewing long lists of material. And it does have to be them – because they're the ones who know the client, what the matter includes, whether something should be selectively retained, and whether or not a potential action could arise from any given matter.

As well, and as much as many IT and records management people fully understand the challenges and are passionate about information governance, the people who're charged with making the decisions very often don't grasp the risks involved in keeping information. It follows that asking them to go through lists of perhaps tens of thousands of records and getting them to commit to their destruction can be tough. It's not unknown for lawyers to review great long list of documents for destruction, only to strike through the whole lot with a red pen and write 'Hold'. Or for them simply to postpone actioning requests from the information governance team to review thousands of records until a window of time opens up – which could mean a very long delay.

## Across the line

How then do you get lawyers across the data destruction line? Well, it's about making the process as simple as possible and giving individuals all of the information needed to make positive disposition decisions. And to be clear, the aim is to achieve disposition. Otherwise, all the effort is in vain, and the firm's costs and liabilities are undiminished.

One approach that works is to use software to organize the many complexities of retention and destruction. For example, to bring all the data sources together using an engine that applies the firm's retention policies and reflects the firm's authorization requirements as they apply to different clients and matters in different practice areas. Then workflow processes can be applied.

Information should be delivered in as simple an interface as possible and should allow decisions to

be made at the matter level. The partners or matter responsible lawyers tasked with authorizing data destruction should be able to easily see that, for example, no payments are outstanding from the client and that the firm's criteria for "closed" matters have been met. It can also be valuable to give lawyers the opportunity to dig down further into records as necessary, so that they have as much information at their fingertips as is necessary to reach a destruction decision.

Then at last, we're at the point of destruction. This also needs to be done properly. Paper needs to be shredded or pulverized. Electronic files have to be overwritten a certain number of times to ensure that the material is deleted beyond retrieval or reconstruction. Firms need to keep an audit trail showing the steps taken, including who approved the destruction, when it happened, and, if destruction was put on hold for any reason, why. Firms will have to create records to record the records they've destroyed. But this is all part of how they can ensure the minimum exposure to risk and cost in respect of record retention and disposition.



**Chris Giles** is CEO and Director of Information Governance at LegalRM, which creates market-leading software, services and solutions for records, risk and compliance management and serves some of the world largest law firms as well as blue chip organizations from other industry sectors.



**Kandace Donovan** is LegalRM's Vice President Operations, North America.

- 1 <https://www.nelsonslaw.co.uk/ico-fines-tuckers-solicitors/>
- 2 <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>
- 3 <https://www.ft.com/content/e2620e22-9593-4781-89f0-3b91a6bce694>
- 4 <https://legalmalpracticeattorneys.org/legal-malpractice-research/harsh-rule-statute-limitations-legal-malpractice-cases/>

## About iCompli, from LegalRM

iCompli, from LegalRM, is an intuitive information governance platform for risk-savvy law firms that want to manage the life cycle of their assets from a single, comprehensive application.

For numerous law firms across the world, iCompli simplifies and automates client file transfers, retention, disposition, and overall compliance of both physical and electronic assets from multiple information repositories, seamlessly and securely.

Plus, it delivers the most powerful physical records tracking database available on the market today. Firms have the option of using iCompli's barcode tracking or RFID capabilities for managing physical records in conjunction with the system's information governance features, all within a simple user interface.

To find out more visit [www.legal-rm.com](http://www.legal-rm.com).



 [legal-rm.com/icompli](http://legal-rm.com/icompli)

 [legal\\_rm](https://twitter.com/legal_rm)

 [legal-rm](https://www.linkedin.com/company/legal-rm)