AN FTI CONSULTING REPORT

Bad Tapes

The fallacy of using backup tapes for data archiving and how to strike back against data over-retention

EXPERTS WITH IMPACT™

FTI CONSULTING

Once touted as the pinnacle of long-term data storage, magnetic backup tapes have evolved into a data albatross around the necks of corporate Australia.

Storage costs, difficulty of data retrieval and the threat of regulatory action due to data over-retention loom over companies which continue to retain backup tapes as a permanent archive.

This report explores what led to data over-retention on tape, defines the current situation and outlines how to remediate data holdings to reduce ongoing operational costs and regulatory risk.

Part 1: Unwinding Data Immortality

Once heralded as the new 'oil' that kept the corporate engine running, the glut of data is now creating oil spills.

For decades, corporates have been hoarding data.

- **Business and strategic operations** have long adopted the philosophy of "Don't delete that! Let's keep it… just in case." This has led to many business units amassing massive data caches, without specific purpose and with little insight into what they hold. This often includes digital landmines, such as unneeded personal information or discoverable emails that legal teams would prefer were destroyed as soon as defensibly possible.
- **The big data gold rush** saw companies scraping their systems to fill data lakes and warehouses, with no clear idea of how to leverage it — leading to an uncontrolled environment with mountains of uncategorised data and hazy access controls, including messaging data, email archives and voice recordings.
- **Cost and convenience**, with historically low penalties for over-retention of data and low costs to keep it compared with the time and expense required to defensibly destroy it.[1]

Data risk has increased exponentially.

Now, the needle has moved on data risk.

In Australia, penalties for breaches of the Privacy Act have dramatically increased — to a maximum of AUD$50 million or 30% of adjusted revenue in the period of non-compliance.[1] The privacy regulator — the Office of the Australian Information Commissioner — has been newly empowered with increased staffing and funding.[2] And in the wake of data breaches of increasing severity and scale, the regulator is looking to crack down on the over-retention of personal data.

It's not just regulators. Class actions are on the rise — in response to data breaches, inadequate controls and loss of over-retained data, both customers and shareholders are looking for recompense and someone to blame.

And the regulatory burden is increasing — proposed amendments to the Privacy Act 1988 (Cth) promise new regulatory powers, more protections and personal rights, a direct right of action and a statutory tort of privacy to enable individuals to directly sue organisations for privacy infringements.

Penalties for Privacy Act breaches[1]

- AUD$50 million;
- three times the value of any benefit obtained through the misuse of information; or
- 30% of a company's adjusted turnover in the relevant period, i.e., the period of non-compliance.

Costs are skyrocketing

At the same time, corporates are feeling the pain of storing billions of unnecessary legacy files. Bloated storage mechanisms and countless stacks of magnetic data tapes abound, groaning with data that is misunderstood, unloved, and wholly unnecessary to the business.

Once touted as the pinnacle of long-term data storage, magnetic tapes have evolved into a data albatross around the necks of corporate Australia. Beyond the storage cost, accessing data via tape restoration is highly inefficient. Simply finding the right tape poses a challenge. Paying a vendor with an antiquated drive to read tapes can be expensive. Tapes go missing. And, as the life of tapes tops out at eight to twelve years, often, companies discover the tape they want is corrupted. The loss of a tape — whether misplaced or corrupted — could comprise a reportable incident, bringing the baleful eye of the regulator down upon the organisation. And the watchdog's gaze could uncover over-retention and other uncorralled data risks.

1. Tim de Sousa and Devina Potter. Australia Is Getting Serious About Penalties for Privacy Enforcement, FTI Consulting (31 October 2022).

2. Office of the Australian Information Commissioner, OAIC welcomes additional Budget funding, (9 May 2023).

It's time to bite the bullet on remediation

Keeping everything forever is not an option. To reduce data risk while ensuring regulatory compliance, corporates need to assess and remediate their data holdings urgently. The goal is to identify and transfer records of business required for regulatory requirements, legal hold data and data of high business utility to secure and accessible storage — and defensibly dispose of redundant, obsolete, trivial (ROT) or duplicative data.

This is easier said than done. Getting the balance right on over- or under-retention of data is a difficult juggling act, bounded by business needs, legal hold obligations and regulatory requirements. Companies need to show that they know what they have and why they have it. It's a time-consuming, whole-of-enterprise activity involving multiple systems and stakeholders, including IT, legal, risk and compliance. However, the risk is too great to continue to ignore.

Despite the difficulty and complexity, corporates must begin remediation as soon as possible:

- Identify what is needed, and what isn't
- Preserve what you must in secure and searchable storage to enable inspection and use
- Get rid of files and data that exposes the organisation to risk and liability.

Ask yourself these questions:

- Do you have a data inventory?
- What is your most historic record?
- What is your most sensitive data type?

Part 2: Embracing Purpose

Using backup as an archive creates more problems than it solves.

Many companies have long confused backups with archives. However, these two types of data repositories are designed for completely different purposes. Backups are meant to help organisations restore their IT systems in the event of an incident or disaster. They're not intended for long-term storage — in fact, they're not very good at it. That's a job for archives!

So — what's the difference between archives and backups?

	Archive	Backup
Purpose	Future reference, regulatory compliance or legal purposes	Restore systems and original data in case it gets damaged
Age	Historical data	Current data
Contains	Regulatory and legal hold data only	All production information
Nature	Usually, the only remaining copy	Multiple data copies
Access	Easily searchable so files can be quickly located and retrieved if needed for legal or compliance reasons	Ideal for recovering applications or complete systems; not easily searchable, time consuming and expensive to search and access individual files
Longevity	Designed to store data for lengthy compliance timelines	Designed to support a disaster recovery timeline, measured in days or weeks

Backup tapes should not be confused with archives — they are different types of data repositories:

- Backups help organisations restore IT systems due to an incident or disaster
- Archives are intended for long-term storage.

Ask yourself these questions:

- Are you using backup tapes as archives?
- Do your backup tapes contain personal information?
- How many backup tapes do you hold?
- What is the oldest backup tape you have?

Part 3: Dark Data, Dark Days

Magnetic backup tapes make for terrible long-term archival storage.

Because magnetic backup tapes were never designed to be used as archives, long-term catalogue retention is an afterthought at best. When beginning remediation projects, it's common to find vast arrays of storage media with unknown contents. Thousands of tapes sit in archive boxes whose custodians have long since left the business. The catalogue that once tracked the contents has been lost. This is 'dark data': data that is known to exist, but is not understood.

Why don't tapes work as long-term archival storage?

Magnetic backup tapes suffer from:

- **Limited life span** – The effective life span of magnetic tapes spans from eight to twelve years – archived data is often kept for much longer. Beyond that time scale, data will need to be migrated to new tapes, or a different medium.
- **Environment** – To prolong the life of backup tapes, they must be kept in optimal climate-controlled environments. Slight deviations in temperature or humidity will reduce storage life. These environments are expensive to establish and maintain.
- **Labels and catalogues** – Each tape should have a physical label, ideally a detailed barcode. Each tape should also have an electronic catalogue that details the contents of the tape. Establishing and maintaining an adequate catalogue requires clear processes, shared institutional awareness and sustained effort, over years. As such, organisations often hold many hordes of tape without any catalogue, or perhaps only a handful of words or a single sentence to describe terabytes of data.
- **Poor data availability** – Locating and extracting tape-based data is time-consuming, expensive and often futile. The chances of finding all required data in a complete and defensible manner are low. A single backup can span multiple physical tapes. If one tape is missing or corrupted, the rest is likely unusable.

Accessing archival data should be fast and simple. If it's not, the wrong storage solution is in place. In our experience, organisations facing litigation that have been forced to draw data from their backup tapes find it a slow, frustrating and expensive process that has complicated or compromised discovery and threatened their position in the matter.

Ask yourself these questions:

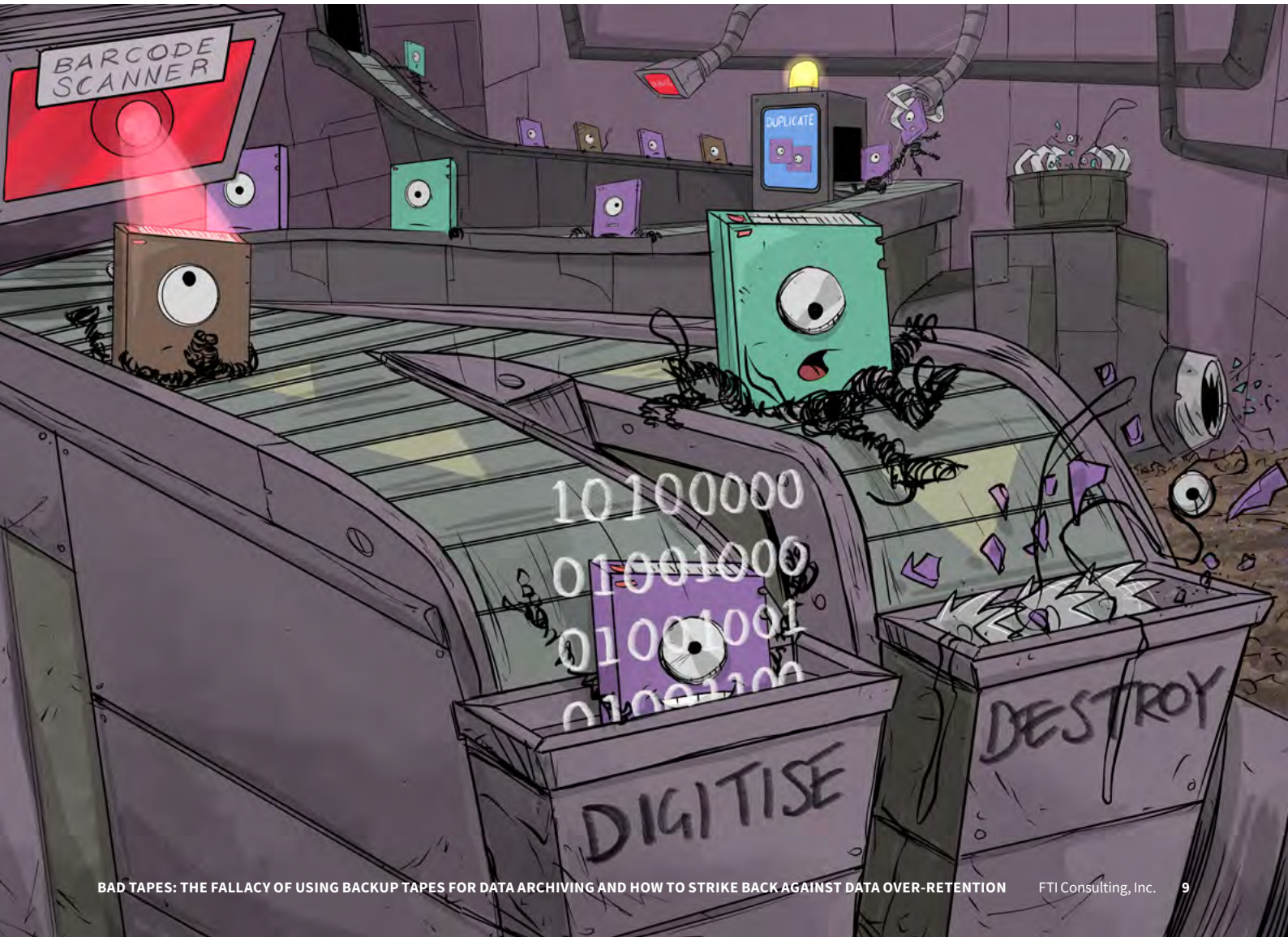
- How many tapes do you have?
- How many different types of tapes do you have?
- Do you know how old your tapes are?
- Do you know where all tapes are held?
- Do you have a tape catalogue?
- How much are you paying each month to store tapes?
- Is any of this really necessary, or are you using tape backups as an archive?

Part 4: The Path to the Digital Future

What does it take to remediate legacy tape data?

If magnetic data tapes are bad archives (see Part 2: Embracing Purpose), and if tapes have a limited lifespan, then something has to change, and soon. That something is format. As organisations worldwide embark on major data risk mitigation projects, FTI Consulting supports them by extracting and preserving relevant data in more modern, easier-to-access platforms: cloud storage platforms with clear access controls, metadata tagging and user-friendly interfaces to enable searchability.

But before abandoning tapes for this halcyon digital future, there are a few things to consider. Technology solutions should align with your organisational strategic goals and policy. Before building the future, know what is needed. Policy objectives should be well defined and supported by appropriate standards and processes. Cementing the policy framework gives the remediation plan structure and a clear destination that supports long term goals.



Building a clear path and sighting the destination — maturing the data governance framework

Consider data governance and system frameworks

Develop or review the following:

- Disaster recovery and crisis plans
- Structured and unstructured data strategy (what to hold, how to hold it, approved storage locations)
- Archive strategy
- Backup strategy
- Decommission strategy

Legal:

- Retention policy and schedule
- Legal holds register
- Watching brief on regulatory change – data retention and privacy obligations

Strategy and operations:

- Consider downstream business use of data and potential de-identification requirements
- Expansion into different geographical regions and the impact on existing of proposed storage and archive solutions
- Agility in the M&A market, ensuring data risk posture supports business aspirations as an attractive investment, or in preparation to acquire an entity and merge systems

Walking down the path — remediating data holdings

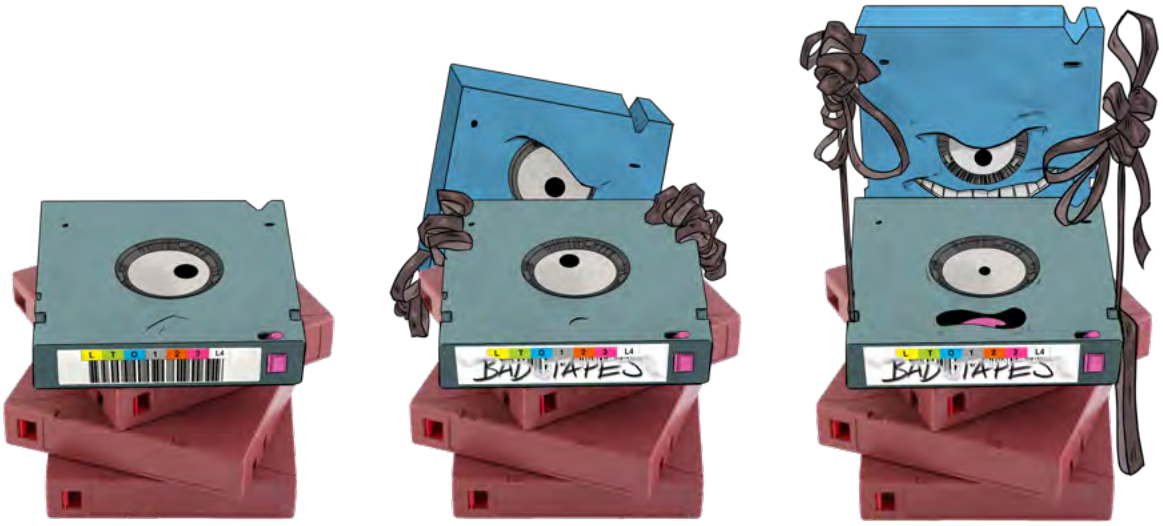
With the destination in sight, it's time to plan how to get there. The steps along the journey might include:

- **Triaging data** – gather existing catalogues, identifying key data assets
- **Assess** – Apply a retention schedule to the data to work out what is needed and what isn't; identify ROT tapes (redundant, obsolete and trivial), such as blanks or corrupted tapes
- **Dispose** of ROT tapes
- **Index** the remaining tapes
- **Classify and review** the data to identify required data assets
- **Defensibly dispose** of unneeded data, subject to formal approvals; document all disposal.

At the destination, with a leaner, fully indexed dataset, it's time to ensure practices enable the organisation to take advantage of all the work. Minimise data collection and creation, classify data to enable searchability and implement systems to comply with retention schedules. Don't build up a new data horde. (See Part 5: From the Ashes Comes New Growth)

Ask yourself these questions:

- Are you storing unneeded personal information on tape?
- Are you storing regulated data on tape? Are you confident you can restore that data?
- Does your data governance framework provide the necessary clarity to guide a remediation project?
- Do you have a retention schedule? Is it up to date with current laws and your business practices?



Part 5: From the Ashes Comes New Growth

As privacy legislation gains teeth and records management moves files into the cloud, organisations must prepare for a new era of data risk.

Sweeping privacy reforms will soon require Australian companies to either de-identify or erase increasing amounts of personal information on request. Meanwhile, panicked and ill-prepared moves to cloud storage are reducing effective data controls.

Once tape archives and data assets have been remediated, act strategically to avoid facing similar problems in the future. To take back control of data and avoid creating new data risk problems in the future, there are a few key actions:

- **Clarify the rules and keep them current** – Uplift or re-design the policy framework to comply with evolving global regulations and modern technologies. Review the framework regularly to ensure it stays up to date.
- **Embed privacy by design** – When creating new or modifying existing storage systems, start with a privacy impact assessment to proactively identify and mitigate risk. This way, new initiatives won't create downstream issues.
- **Operationalise retention schedules** – Set up a taxonomy for all documentation and train the workforce to save key documents (contracts and financial records) in appropriate storage.
- **Assign roles** – Data stewards should have accountability over data within select systems and teams. Data committees should be collated to enable a quorum of relevant stakeholders to make defensible disposal decisions.
- **Establish de-commissioning procedures** – Make sure people know what to do with old systems and data. What must be remediated, how will this happen, who will do it, and when?
- **Embrace automation** – Explore ways to use technology to make it easier to comply. Implement retention labels and classification to enable automatic alerts that retention periods have been expired and to enable disposal.

When Tape Remediation Saves the Day: Story 1

Decommissioning legacy systems

A multinational financial services institution needed to remediate its legacy data environments, enable defensible disposal and comply with the EU's General Data Protection Regulation (GDPR).

Scoping legal hold obligations

FTI Technology interviewed dozens of in-house and outside counsel to identify all legal matters and the various data sources impacted, scoping nearly 800 legal matters for legal hold obligations.

Information was aggregated into a master list, enabling the team to track preservation, release and dispose of expired legal holds and provide retention management around the entire process going forward.

Culling for preservation and disposal

Privacy and governance experts identified various discoverable information sources, including messaging data, email archives, voice recordings, structured data collections, loose files, backups on discs and tapes.

All information sources contained data that was relevant to thousands of custodians across hundreds of legal matters.

Progressing defensive data disposal

FTI Consulting helped the client make significant progress with its global defensible data disposal initiative, including:

- Establishing new legal hold workflows
- Decommissioning 1,000+ legacy applications, messaging systems and data archives across APAC, EMEA and the Americas
- Defensibly deleting billions of legacy documents no longer needed.

When Tape Remediation Saves the Day: Story 2

Let down by an outside storage provider

A global client had more than 50,000 backup tapes, along with hard drives, floppy discs and boxes of paper records, in storage with an outside vendor that needed remediation. But the vendor had misplaced and mixed up many of the client's stores.

Untangling the mess

When the storage vendor's mistakes threatened the remediation project, FTI Technology created an itemised inventory of all data.

A quick response in recovering the storage provider's forensic mistakes was integral to getting the remediation workstream back on track.

Supporting defensible disposal

All 50,000 of the client's legacy, duplicate backup tapes have now been destroyed.

FTI Technology also identified and remediated thousands of unnecessary non-tape media storage, closed container tapes and open media tapes.

Preventing over-preservation

The expert team helped the client defensibly remove a significant volume of data that could have led to potential future legal and regulatory costs.

The client now has a disaster recovery policy and procedures to prevent future over-preservation, including storing backup tapes for no longer than 180 days.

When Tape Remediation Saves the Day: Story 3

Expiring third-party systems

A global financial services institution needed to identify and preserve messaging data saved on backups tapes for 17,000 custodians in the U.S., Asia Pacific and Europe on EMC Data Domain.

The client had outsourced its global messaging infrastructure to a third-party provider and needed to preserve backup data for legal and regulatory purposes before the vendor contract expired.

Identifying custodian data

FTI Technology executed a plan that would not interrupt day-to-day business operations for remote and on-site employees.

The team identified data for 17,000 custodians exclusive to the EMC Data Domain backup environments, and extracted all required data to a system that would provide easier access for long-term storage.

Supporting defensible disposal

FTI Technology's experts developed workflows to identify, validate and extract relevant custodian data exclusive to backups so it would be preserved and easily accessible for future use.

Avoiding business disruption

To ensure business as usual operations continued, the team worked with IT, legal and e-discovery staff to develop a solution and workflows to inventory and track the preserved data as part of daily operations.

For help remediating your organisation's backup tapes or to discuss all things data, contact:

CHRISTOPHER HATFIELD
Managing Director
Information Governance, Privacy & Security
+61 437 373 130
christopher.hatfield@fticonsulting.com

JOHN GOFF
Managing Director
+1 404 460 6267
john.goff@fticonsulting.com

TIM DE SOUSA
Managing Director
+61 413 248 107
tim.desousa@fticonsulting.com

ROSE MORGAN
Director
+61 466 800 864
rose.morgan@fticonsulting.com

Need to get a better understanding of your data risk position?
Complete our short, anonymous self-assessment at:
ftitechnology.com/datarisksurvey

The illustrations in this report have been specially commissioned by professional illustrator Phil Buckenham.