InfoGov World 2025

Implementing Defensible Disposal in Practice

Overcoming Common Challenges

Introductions

Anthony Diana

Partner, FinTech & Data/Emerging Technologies

Reed Smith

Greg Trulove

Vice President, Managing Deputy General Counsel, ERM

Sutter Health

John Goff

Managing Director - Information Governance, Privacy, and Security

FTI Consulting

Agenda

- What is Defensible Disposal?
- Core Challenges of Implementation
- Case Study: Actionable Strategies & Best Practices
- Q&A

What is Defensible Disposal?

Defensible disposal is the standardized, documented, and compliant process for **destroying or deleting data** and **records** that are **no longer needed**.

As a key component of a robust information governance program, it is also a crucial element of **overall data governance**, focusing on **mitigating the risks** associated with **over-retention.**

Core Challenges of Implementation

Data Hoarding

- Fear of spoliation
- Belief that data is an asset
- Lack of accountability

AI

- Diminishing data quality
- Unknown biases

Unclear Data Landscape

- Data growth
- Data silos
- Legacy media systems
- Lack of data insight

Legal & Regulatory Complexity

- Conflicting retention requirements
- Managing legal holds
- Ensuring defensibility

Technical & Operational Challenges

- Inadequate tools
- Complexity of deletion
- Lack of automation
- Training & employee buy-in

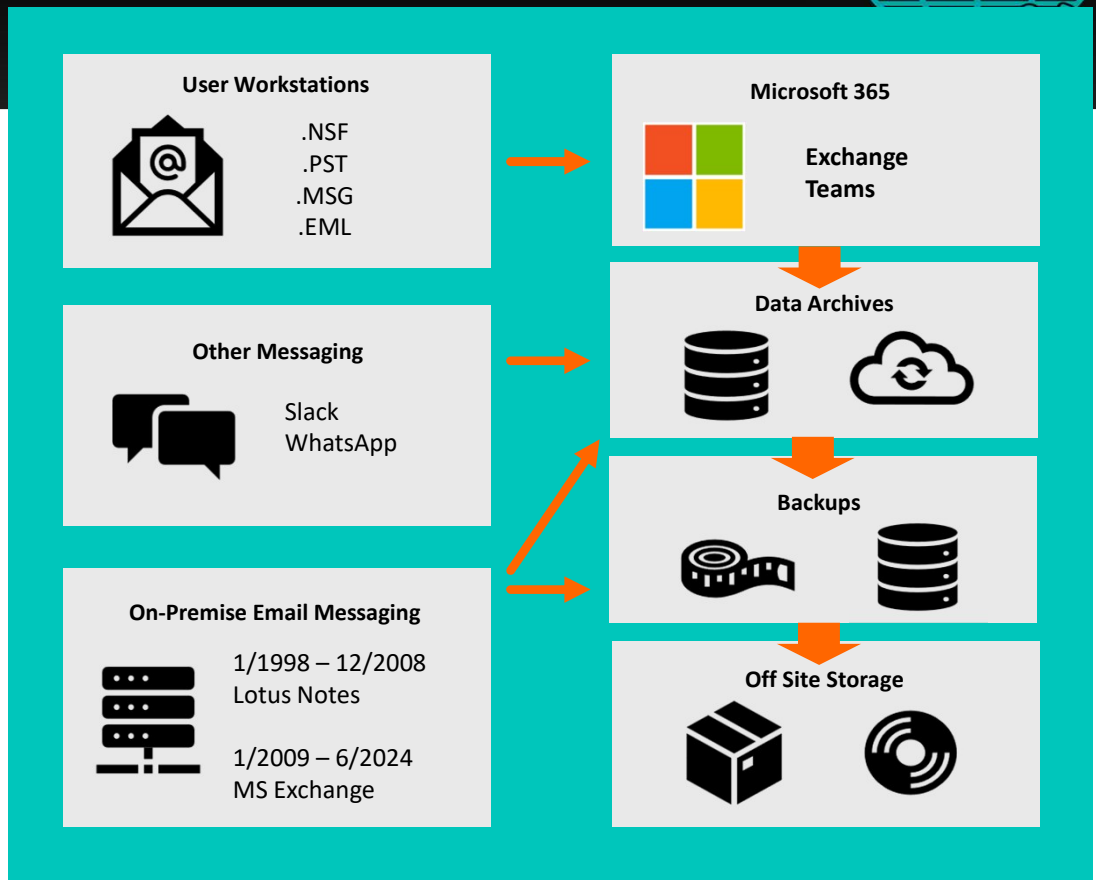
CASE STUDY

Actionable Strategies & Best Practices

As part if its roadmap, a client is moved from on-premise email and data archiving to M365 for active users. They would like to decommission legacy messaging systems to reduce their overall risk and costs associated with over retention of data.

The key challenge areas are:

- **Decommissioning of Legacy Systems:** All active users cut over to M365 in July 2024, but the legacy email platforms (Lotus Notes, MS Exchange) remain live due to ongoing legal and compliance concerns. In the past, end users were also allowed to save email locally via .NSF & .PST files.
- **Retention Non-Compliance:** The firm's established 3-year retention policy was never consistently enforced on the legacy email systems, leading to a massive accumulation of data past its defensible retention period.
- **Data Silos & Custodian Identification:** The Legal department maintains multiple, decentralized tracking systems to identify data associated with custodians, making data disposition complex and risky.
- **Legacy Backups:** While all on-premise systems are being backed up to disk as of January 2025, a significant challenge exists with physical tape backups stored offsite, which contain an unknown but large inventory of data that needs to be assessed.



Key Takeaways

Actual vs. Presumed Value

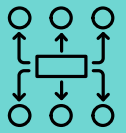
Retaining data indefinitely due to the belief it's a future asset, increases risk.

Actual AI Utility vs. Risk

Retaining low-value, outdated data "just in case" for AI undermines accuracy and fairness of models.

Data Inventory & Mapping

A data inventory and mapping effort is essential for applying holds and retention rules consistently.



Document Policies

Disposal must follow consistent, documented policies—not ad hoc decisions—to withstand legal scrutiny and protect against spoliation claims.

Consider Backups, Archives, and Shadow Copies

True defensible disposal requires processes that ensure data is unrecoverable when deleted.

Training & Culture

Retention and disposition is only defensible if followed. Regular training and cultural change are necessary to move away from "keep everything" behavior.

Thank you for attending!

Twitter: @InfoGovWorld
LinkedIn: @InfoGov World Magazine

www.InfoGovWorldConference.com
AIWorldconference.ai