

The privacy gym: Get your data in shape!

Wednesday, 21 May

08:00-09:00 PST

11:00-12:00 EST

17:00-18:00 CET



Panelists



Rebecca Perry, CIPP/US/G

Managing Director,
Strategy & Operations,
Data Privacy, Security & Governance
Solutions

Exterro



Matthew L. Miller, Esq.

SVP, Global Advisory Services Leader

HaystackID



K Royal, PhD, JD FIP, CIPP/E /US, CIPM, CDPSE

Global Chief Privacy Officer and Deputy General Counsel

Crawford & Company

Co-Host

Serious Privacy Podcast

exterro Safeguarding Your Digital World



Effectively Prepare & Respond when Data Risks Become Reality

Agenda

- 1. Why Your Data Needs a Workout: The Legal Case for Minimization
- 2. From Hoarder to Minimalist: Data Fitness Transformations
- 3. Leverage Technologies: Automate the Reps, Maximize the Gains
- 4. Cool Down & Q&A

Why Your Data Needs a Workout: The Legal Case for Minimization

Records, Information and Data are Everywhere!



Desired IG & RIM Program Enhancement Outcomes

Know all data we retain, control, or process

Know when we should get rid of our data

Know where all of our data is located or stored

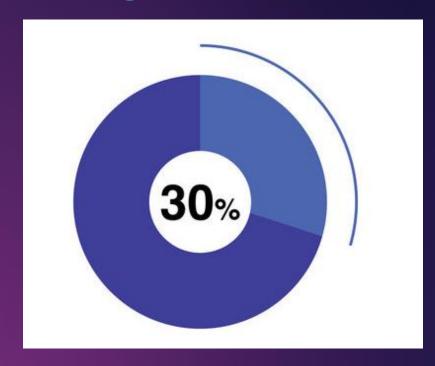
Know how long we should keep our data Without knowing what data we have, how can we know what data to protect, retain, or dispose?

Know what our data contains (content and metadata)

Know how to find the right data rapidly Control who can and should have access to our data

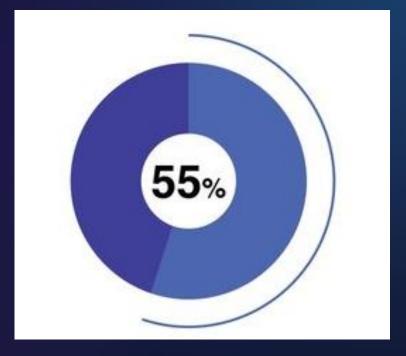
85% of Enterprise Data is ROT or Dark Data

ROT DATA



Redundant Obsolete Trivial Data

DARK DATA



Unknown or Untapped

Trimming the Fat:

The Sedona Conference Framework for Disposition

The Sedona Conference, Commentary on Defensible Disposition (2019) provides a framework for managing information no longer subject to legal or regulatory retention.

Principle 1

Absent a legal retention or preservation obligation, organizations may dispose of their information.

Principle 2

When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention.

Principle 3

Disposition should be based on Information Governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives.

Data Retention Obligations Under Privacy Regulations



- Transparency / Notice
- Data Minimization
- Purpose Limitation
- Storage Limitation

Privacy & Security Overlap

NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0 (January 16, 2020)

Figure 2: Cybersecurity and Privacy Risk Relationship

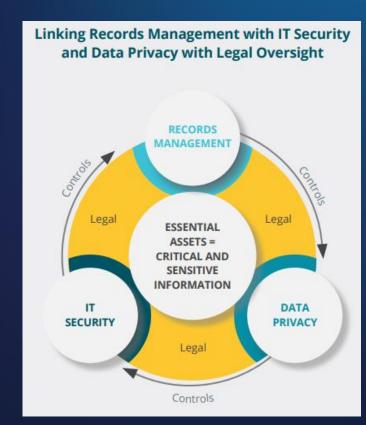
Cybersecurity Risks

Associated with
Cybersecurity incidents
arising from loss of
confidentiality, integrity, or
availability

Cybersecurity related Privacy events

Privacy Risks

Associated with Privacy events arising from data processing



NIST.SP.800-53r5, Security and Privacy Controls for Information Systems and Organizations (September 2020)

Data Breaches & Massive Fines

BlackBaud

"Reckless Data Retention Practices"



FTC Fine \$3M

- 2020 data breach impacting millions of people
- Failed to enforce their records retention schedule
- Exacerbated the number of individuals impacted.
- The average fine levied by the FTC for privacy and cybersecurity violations is \$45.7M

Disney

"Millions of Slack Messages Breached"



Internal Slack Messages

44 Mil

- 18,800 spreadsheets
- 13,000 PDFs
- Highly sensitive personal data about employees
- Unreleased projects & sensitive documents
- Class action lawsuit

From Hoarder to Minimalist: Data Fitness Transformations

Slim Down Your Data: A Defensible Approach

Organizational Benefits of Disposition	Defensibility of Purpose & Process Benefits
 Reduce enterprise and legal risks 	 Expand policy compliance
Decrease downstream eDiscovery costs	Meet regulatory obligations
 Increase ability to satisfy legal holds 	 Enable production of the right data
Reduce attack surface and lower risk of exfiltration	Satisfy courts, regulators, and auditors
Trim 3 rd party costs	
 Improve system performance 	
Reduce storage footprint	

Get Buy-In by Identifying Strategic Benefits



Reduce Risk of Litigation and Fines



Reduce Expected Cost of a Data Breach



Reduce Storage Costs



Reduced E-Discovery
Costs and Cyber
Insurance Premiums

Your Data Fitness Plan: 4 Moves to Strengthen Compliance

Identify structured & unstructured data
Assess what's critical vs. obsolete

1
EVERGREEN DATA MAP

2
ACTION RETENTION POLICIES

4 STEPS

Boost accessibility

Improve governance & compliance

Ensure policies match reality Identify gaps & mitigate risks

4
ONGOING PROGRAM
OF

3
OPERATIONAL
CAPACITY

Automate data holds & releases Reduce reliance on IT for legal

Roadmap for Implementing Data Disposition

RIM Enhancement Program: Controls for Better Data Risk Management

Identifying & classifying information assets

- Leveraging attributes & labels determine inventories of large bucket classification categories such as:
- Critical / Sensitive
- Irrelevant / ROT

Reduces organizational risk

costs in non-consumer facing areas

- Reduces structural
- **Enables** operationalizing policies on the network

Enables remediation & data disposition

- Legal
- Compliance
- IT security
- Privacy
- Risk

- eDiscovery costs
- Storage costs
- Employee data retrieval time
- Data protection costs

- Enforce records schedules
- Enforce defensible data disposition
- Narrow the critical busines legal hold data universes
- De-identification, obfuscation, masking, tokenization
- Anonymization, guarantining, redaction
- Migration, archiving
- Encryption
- Sanitization, deletion

Harmonize Overlapping Obligations







Data Retention & Disposition



RoPA Manager



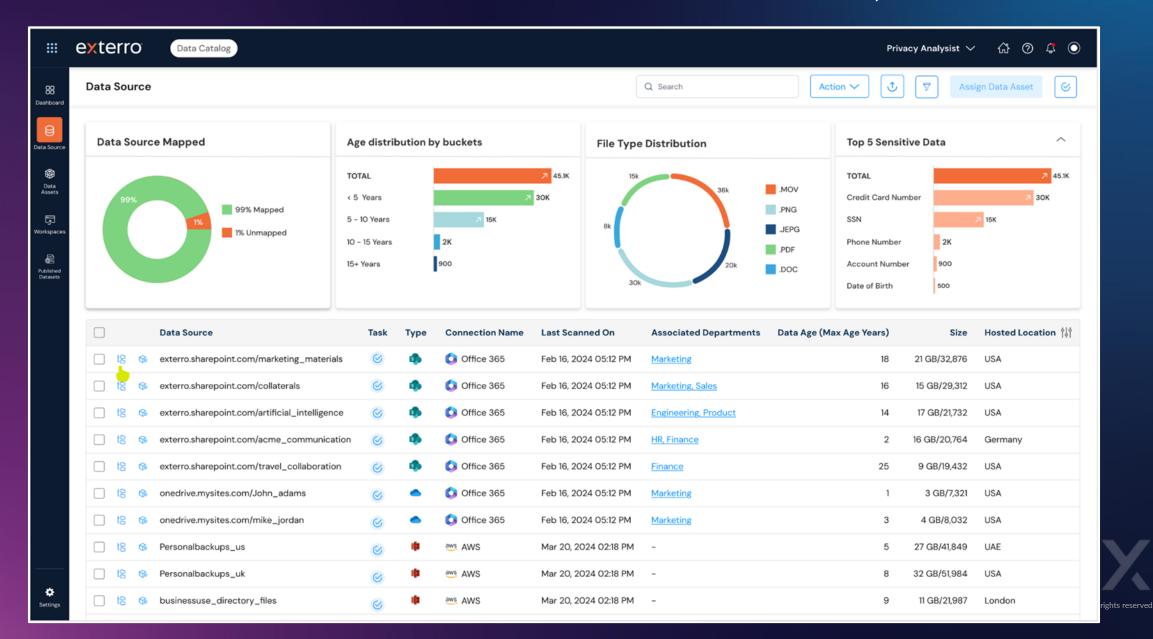
Privacy Rights
/ DSAR



Legal Holds



Data Examination: Understand & Classify Data



Your Data Fitness Plan!

Identify high-risk systems — Data Source Discovery



Catalog sensitive and personal data in high-risk systems



Data Discovery & Data Catalog

Identify data on a legal hold — Legal Hold



Identify data that must be retained because of retention regulations



Data Retention

Identify data necessary for business reasons

Data Catalog



Minimize unnecessary data! — Data Disposition



Find and produce personal data on request



Consumer Requests Fulfillment

Cool Down and Q&A

Thank You!



Rebecca Perry, CIPP/US/G

Managing Director, Strategy & Operations, Data Privacy, Security & Governance Solutions

Exterro



Matthew L. Miller, Esq.

SVP, Global Advisory Services Leader

HaystackID



K Royal, PhD, JD FIP, CIPP/E /US, CIPM, CDPSE

Global Chief Privacy Officer and Deputy General Counsel

Crawford & Company

And

Co-Host **Serious Privacy Podcast**

Keep Training: Free Tools to Help You Stay in Shape

- Data Retention Handbook
- Infographic: The Sleeping Giant of Privacy & Security: Data Deletion
- Privacy Program Assessment Checklist

& more







Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/ACtQeZ5411

Thank you in advance!

For more information: www.iapp.org



Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings or to obtain a copy of the slide presentation please contact:

livewebconteam@iapp.org