



Sleeping Giant of Privacy, Security and E-discovery – Minimize Data to Minimize Risk

Wednesday, 19 February

08:00-09:00 PST

11:00-12:00 EST

16:00-18:00 CET



Introductions

Panelists



Fahad Diwan, JD, FIP

Director of Product
Marketing

Exterro



Paul Luehr

Partner and Co-
Leader of AI, Privacy,
and Data Security

Manatt, Phelps &
Phillips, LLP



Victor O. Adu-Gyamfi

Corporate
Investigations Team
Lead (Forensics and
E-Discovery)

Progressive Insurance



Robert Daniel

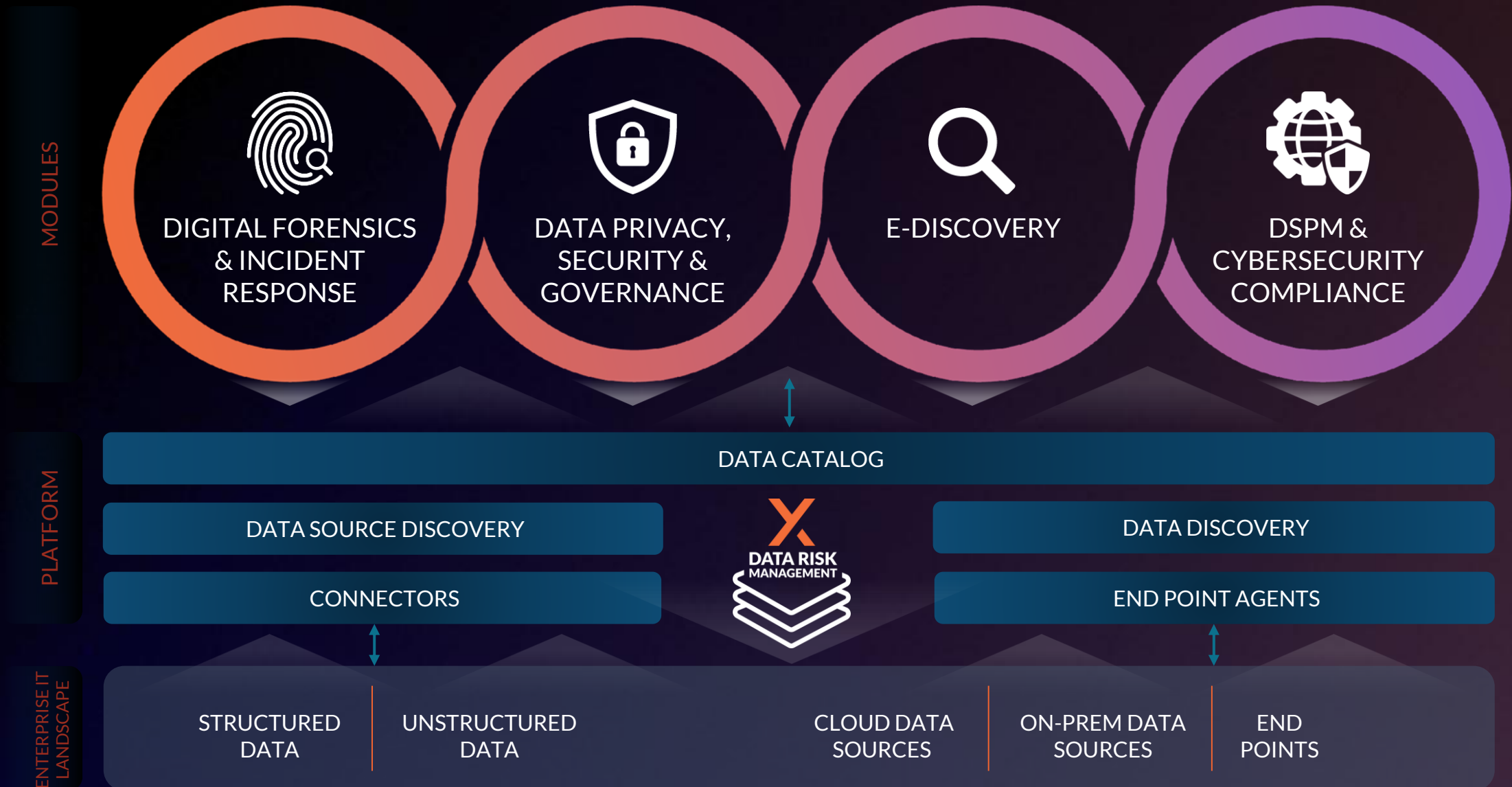
Senior Director -
Product Management
/ Financial Services

Integreon

Session Outline

- Overview of Laws Mandating Data Deletion
- Real-World Examples & Case Studies
- Leveraging Technologies to Implement Data Deletion
- Conclusion and Q&A

Exterro Data Risk Management Platform



DATA PRIVACY, SECURITY & GOVERNANCE SUITE



Overview of Laws Mandating Data Deletion

U.S. and Int'l Data Minimization Requirements

1974



U.S. Privacy Act

"Each agency ...shall maintain in its records *only* such information about an individual *as is relevant and necessary...*"

1981



Fair Info Practice Principles (FIPPS)

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

2002



Privacy Rule:
Minimum Necessary Standard

When using, disclosing, or requesting PHI, "a covered entity or business associate must make reasonable efforts to limit [PHI] to the *minimum necessary...*"

2018



Article 5:
Processing Principles
Data should be "kept in a form which permits identification of data subjects for *no longer than is necessary...*"

2021



GLBA:
FTC Safeguards Rule
"[M]aintain procedures for the secure *disposal* of customer information in any format *no later than two years* after the last date the information is used..."

iapp U.S. State Data Minimization Requirements

California

“a business shall *not retain* a consumer’s personal information or sensitive personal information ... *for longer than is reasonably necessary* for that disclosed purpose.” Cal. Civ. Code § 1798.100(a)(3)

CPPA – April 2024
enforcement advisory on
data minimization

Colorado

“Controllers shall set specific *time limits for erasure* or to conduct a periodic review .” 4 CCR 904-3-6.07(B)



New York

Businesses must “dispose[] of private information within a reasonable amount of time after it is no longer needed...” NY Gen’l Bus Law § 899-bb-2(b)(ii)(C)(4)



Maryland

A controller may only collect or process “sensitive information” if it is “*strictly necessary*.” Maryland Online Data Privacy Act of 2024, § 14-4607(A)(1)

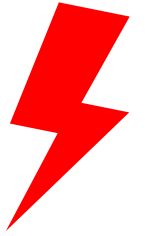




Data Minimization - Regulatory Actions

- **InfoTrax Systems** – FTC action alleged failure to implement a “process for inventorying and deleting consumers’ personal information ... that is no longer necessary.” (Jan. 2020)
- **EyeMed** – NY AG \$600K settlement, alleged failure to delete 6-year-old email. (Jan. 2022)
- **Drizly** – FTC action alleged failure to implement a “practice for inventorying and deleting consumers’ personal information stored on its network that was no longer necessary.” (Oct. 2022)
- **InMarket** – FTC action over geolocation data alleged retention of such data for 5 years – “longer than reasonably necessary.” (Jan. 2024)
- **Blackbaud** – FTC action alleged failure to “enforce its own data retention policies, resulting in the company keeping customer’s consumer data for years longer than was necessary.” (Feb. 2024)

Data Bloat – Impact on Incident Response



- **Increased costs**

- Investigations
- Notifications
- Public/media relations
- Regulatory fines/responses
- Litigation



- **Affected population**

$$\begin{aligned} & [\text{Current Population}] \times [\text{Related Parties}] \times [\text{Years of Exposure}] \\ & = [\text{Likely Affected Individuals}] \end{aligned}$$

Paul's Rule of 70x !

(e.g., 100 employees x 3-to-4 beneficiaries x 20 years = 7000 victims)

Real-World Examples & Case Studies

The Hidden Risks of Excessive Data Storage Optimizing Data Retention for Compliance, Efficiency & Risk Mitigation

Quote: *“The more hay in the stack, the harder to find the needle.”*

Key Idea: Storing excessive data makes it harder to extract intelligence when it’s needed.

The Hidden Costs of Excess Data Retention

- **Operational Inefficiencies** – Slower decision-making, bloated IT infrastructure.
- **Legal & Compliance Risks** – Increased exposure in litigation, audits, and regulatory scrutiny.
- **Security Vulnerabilities** – More data = higher breach risk

The Path to Data Clarity

Four Critical Steps:

1. Get a Complete Inventory of All Data Sources

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

2. Digitize All Data If You Can

- Improves accessibility, searchability & governance

3. Empower Legal Teams for Self-Sufficiency

- Automate data holds & releases
- Reduce reliance on IT for legal operations

4. Audit the Process Continuously

- Ensure policies match reality
- Identify gaps & mitigate risks proactively

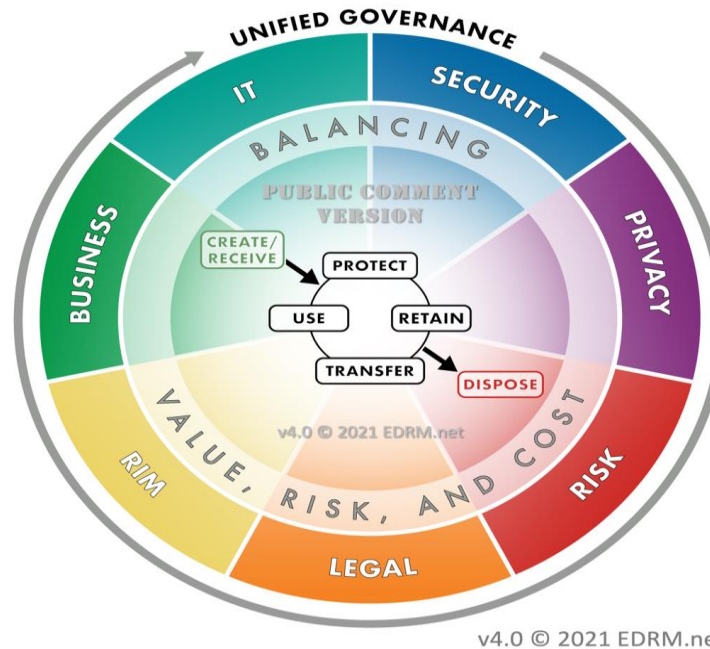
Practical Disposition Strategies

- Practical Discovery and Disposition
 - Initial thoughts on creating a Data Disposition strategy -
 - Just starting the project and getting all Stakeholders engaged was one of hardest parts
 - Need a strong Executive Sponsor at Corp level – RIM
 - Project Management and documentation will be critical with all the moving processes
 - Tactically Developing an Enterprise disposition strategy
 - Coordination across multiple business disciplines, will require patience. The bigger and more diversified your company the more patience you will need.
 - Need to group to lead the process for all stakeholders
 - Allow each stakeholder the opportunity to voice their needs from others.
 - Remember that all the Stakeholders have same basic objective, just from another perspective

Information Governance Model

IGRM Redesign – Inclusion of Risk Management functions including Privacy in the Information Governance decision process was part of the update to the IGRM as a part of the EDRM

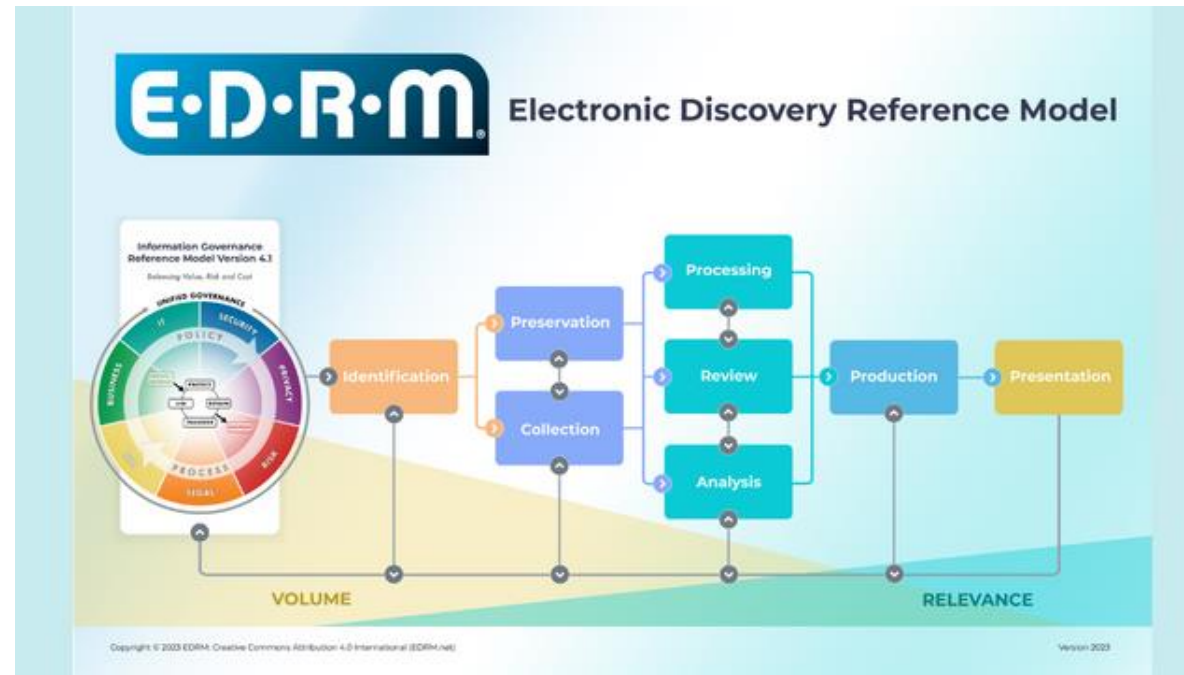
**Information Governance Reference Model
(IGRM)**



Information Governance

The IGRM redesign group wanted to stress these things in the redesign and acknowledge that IG is continuous and engaging stakeholders is a must for good IG

A well-designed IG process is the foundations to a good and efficient EDRM process. The IGRM is in front of the EDRM to reflect the critical nature of the IGRM to your EDRM



Risk Reduction and Takeaways

Business and risk reduction drivers behind data deletion projects

- Reduce cost of storage - \$4 per box per month is \$48 per box per year and it adds up to a lot of money going out the door when you have thousands to tens of thousands on boxes in storage
- Reduce risk and fines of non-regulatory compliance. An IG process that includes annually reviewing regulatory retention requirements to your retention schedule should be foundational. Make it a routine annual process.
- Reduce legal risk by no longer having data that could be responsive to legal matters

Key Takeaways

- Include all risk partners to ensure defensible disposition. All relevant partners must be engaged to leave no gaps in your process.
- As a baseline, you need a Consistent workflow, adequate documentation, evidence of approvals to fully support the decision processes in the future... Possibly in court or before a regulator

Roadmap for Implementing Data Deletion

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

Key Steps

- Identifying all data sources
- Identifying data sources with personal and sensitive data
- Identifying data that must be retained:
 - Legal holds
 - Retention requirements
 - Business reasons

Challenging to Do Manually

- Limited resources
- Data proliferation
- Quickly out-of-date
- Complex

Leverage Technologies to Reduce the Pain

- Automated Data Mapping
- Data Catalog
- Legal Hold
- Data Retention

Roadmap for Implementing Data Deletion

1. Identify high-risk systems
2. Catalog sensitive and personal data in high-risk systems
3. Identify data on a legal hold
4. Identify data that must be retained because of retention regulations
5. Identify data necessary for business reasons
6. Minimize unnecessary data!
7. Pat yourself on the back and do a little dance to celebrate 😊

Leverage Technology to Increase Effectiveness and Reduce Pain

0. Identify and implement technology provider that offers all necessary solutions
1. Identify high-risk systems → Data Source Discovery
2. Catalog sensitive and personal data in high-risk systems → Data Discovery & Data Catalog
3. Identify data on a legal hold → Legal Hold
4. Identify data that must be retained because of retention regulations → Data Retention
5. Identify data necessary for business reasons → Data Catalog
6. Minimize unnecessary data!
7. Pat yourself on the back and do a little dance to celebrate 😊

Conclusion and Q&A

Connect with us!



Paul Luehr

Partner and Co-Leader of AI, Privacy, and Data Security,
Manatt, Phelps & Phillips, LLP

LI: <https://www.linkedin.com/in/paul-luehr/>

Email: bluehr@manatt.com



Fahad Diwan, JD, FIP

Director of Product Marketing, Exterro

LI: <https://www.linkedin.com/in/fahaddiwan/>

Email: fahad.diwan@exterro.com



Victor O. Adu-Gyamfi

Corporate Investigations Team Lead (Forensics and E-Discovery),
Progressive Insurance

LI: <https://www.linkedin.com/in/victor-o-adu-gyamfi/>

Email: VICTOR_O_ADU-GYAMFI@progressive.com



Robert Daniel

Senior Director - Product Management / Financial Services,
Integreon

LI: <https://www.linkedin.com/in/robert-daniel-6728365/>

Email: Robert.Daniel@integreon.com

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/ACtQeZ45GA>

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