Panel 8: Technological Tools for Protecting Privacy and Data Security in Litigation

The 13th Annual Sedona Conference Institute:
Protecting Privacy, Confidentiality, and Privilege in Civil Litigation
March 7–8, 2019
The Ballantyne Hotel & Lodge, Charlotte, NC

Dialogue leaders

- Jamie Brown
  - Lighthouse, Seattle, WA
- Corey M. Dennis
  - Pharmaceutical Product Development, LLC, Wilmington, NC
- Andrea L. D'Ambra
  - Norton Rose Fulbright US LLP, New York, NY
- Matthew F. Knouff
  - Complete Discovery Source, Inc.
- Eric J. Schwarz
  - Ernst & Young LLP, Dallas, TX





Agenda

- The Increasing Focus on Privacy
- Privacy Technologies
  - Achieving Privacy Compliance at the Level of Network Traffic
  - Encryption Overview and Considerations
- Data Minimization

Increasing Focus on Privacy Governments, Companies, Individuals

- Increasing global focus on privacy
  - More focus on Intelligence gathering/AML/CTF
  - Geopolitical developments – BREXIT, GDPR, CA Data Privacy
  - Facebook, Cambridge Analytica & Social Media practices
- Greatly enhanced AI capabilities
- Global movement towards more data localization and data privacy protection
- GDPR & California Consumer Protection Act

Privacy Technologies

Overview of Technology – Purposes

- Identify – aimed at locating personal data as a precursor to other activities (can't protect it if you don't know where it is)
- Remediate – focused on mitigating risk associated w/legacy data (e.g., classification, protection, disposal)
- Protect – ensuring controls are in place (e.g., encryption, access/entitlements, classification labels, retention/disposition)
- Respond – tracking/logging, detection, reporting, auditing

Key elements of Office 365

Exchange Online

-Email
-Calendar
-Contacts
-Tasks
-Notes
-Journal
-Exchange Public Folders

SharePoint Online

-Collaboration: Team Sites
-Intranet/portals
-Blogs/wikis
-Application development
-Enterprise Content Management
-Document libraries
-Enterprise file sharing: OneDrive for Business & document libraries

Yammer

-Enterprise social media: “Facebook for the corporation”
-Groups and communities
-Posts: free-text entries, comments, conversations
-Upload files (Word, Excel, etc.)
-Polls, praise
-Like, share, unlike

Built-In Information Governance Tools

-Retention and disposition
-Compliance
-Data protection
-File Plan

Skype for Business

-Instant Messaging (IM chats)
-Voice (call logs)
-Online meetings
-Presence
(Soon to be TEAMS)

Cross-O365 Apps

Applications and tools that are cross-platform and/or built from the ground up in Office 365
--Groups
-Planner
-Teams
-Telephony
- Multimedia

Office ProPlus

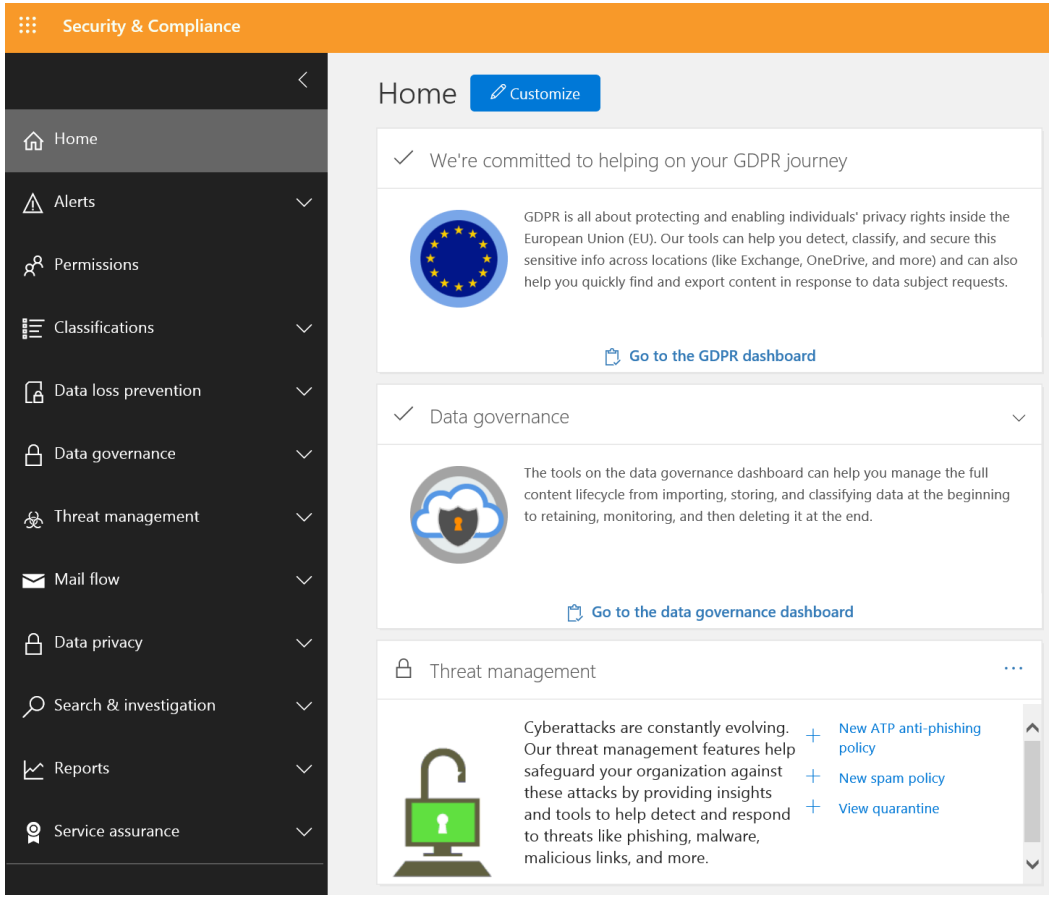
-Word
-Excel
-PowerPoint
-Outlook
-OneNote
-Access
-Publisher
Project

Built-In eDiscovery Tools

-Identification
-Preservation
-Collection
-Analytics
-Processing
-Review*
-Production*

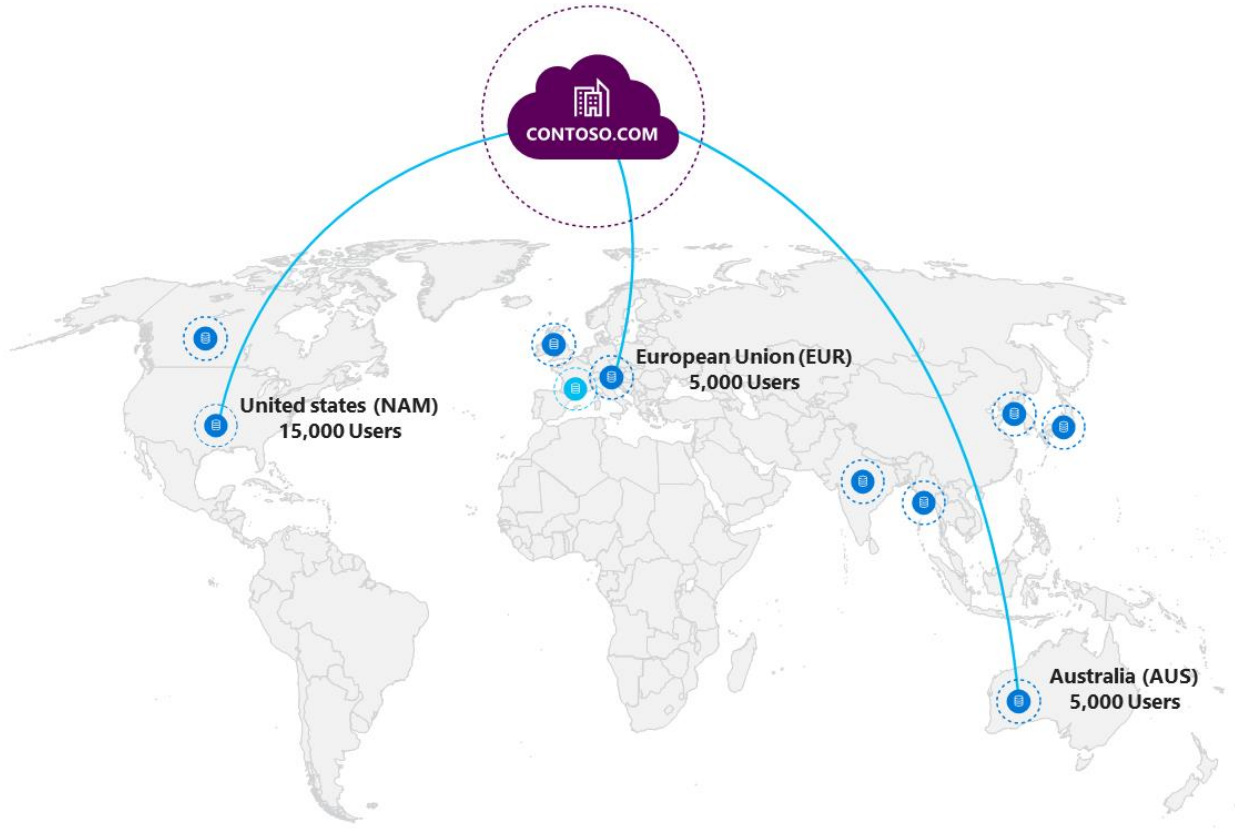
M365 Security & Compliance Center

- **Single "Portal" in Office 365**
- **Role Based Access Controls**
  - Audit trail of who was assigned what access, when, and by whom
  - Only see what tabs you have access to)
- **11 tabs organized around thematic areas**
  - Data Governance (retention & disposition)
  - Search and Investigation (eDiscovery)
  - **Data Privacy**
  - Email Threat Management



Multi-Geo

Global Data – Local Control



Benefits

- Allows a corporation to meet data residency requirements in countries that restrict the transfer of personal data (e.g., customer data, employee data, sensitive personal information).
- Allows US data not subject to residency requirements to remain in the US, where it can more easily be preserved, collected, searched and produced for US led investigations, litigation and regulatory matters.
- Allows all users, regardless of geo, to enjoy the benefits of data unification, including unified communication and collaboration, and without the latency associated with cross-border access.
- Allow for centralized management of data, technology and information, including by IT infrastructure, security, data governance, information governance, e-discovery and e-compliance functions.

Active Navigation – Use Cases

Discover and cleanse

Discover, classify, visualize and understand digital landfill

- Cost reduction
- Efficiency optimization
- Retention compliance

Sensitive data identification

Identify records/sensitive data (e.g. PCI, PII, HIPAA, FOIA)

- Regulatory (GDPR) compliance
- Proactive eDiscovery savings
- Risk reduction of data breach

Intelligent migration

Apply metadata against new repository structure & migrate

- Mergers & Acquisitions
- Data consolidation
- Data tagging for IG implementation

Content governance

Deploy policies on content for quality, health, value and compliance

- Automated analysis for consistent retention & IG
- Audit trails & management reporting

Achieving Privacy Compliance at the Level of Network Traffic

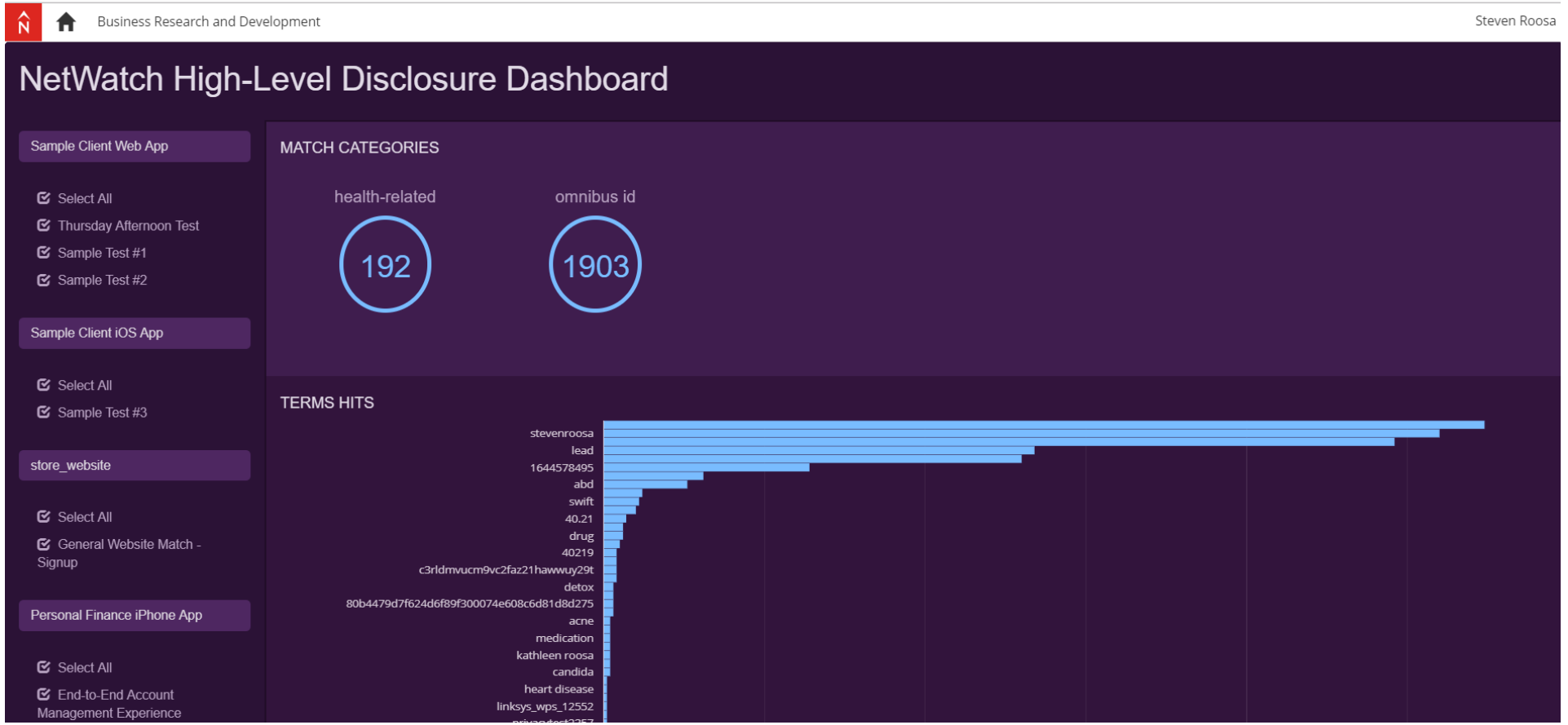
The Case for Network Traffic Analysis

- Most consumer/end-user data is collected from mobile apps, websites, and IoT devices
- 3rd Party data collection is most often done by the consumer's devices
- All of the data collection from consumer devices must use the Internet
- The data can be captured and analyzed in a proxy environment
- Privacy laws can be reduced to precise rules regarding the kinds of data collection constitutes a non-compliance
- These rules can be operationalized at the level of code

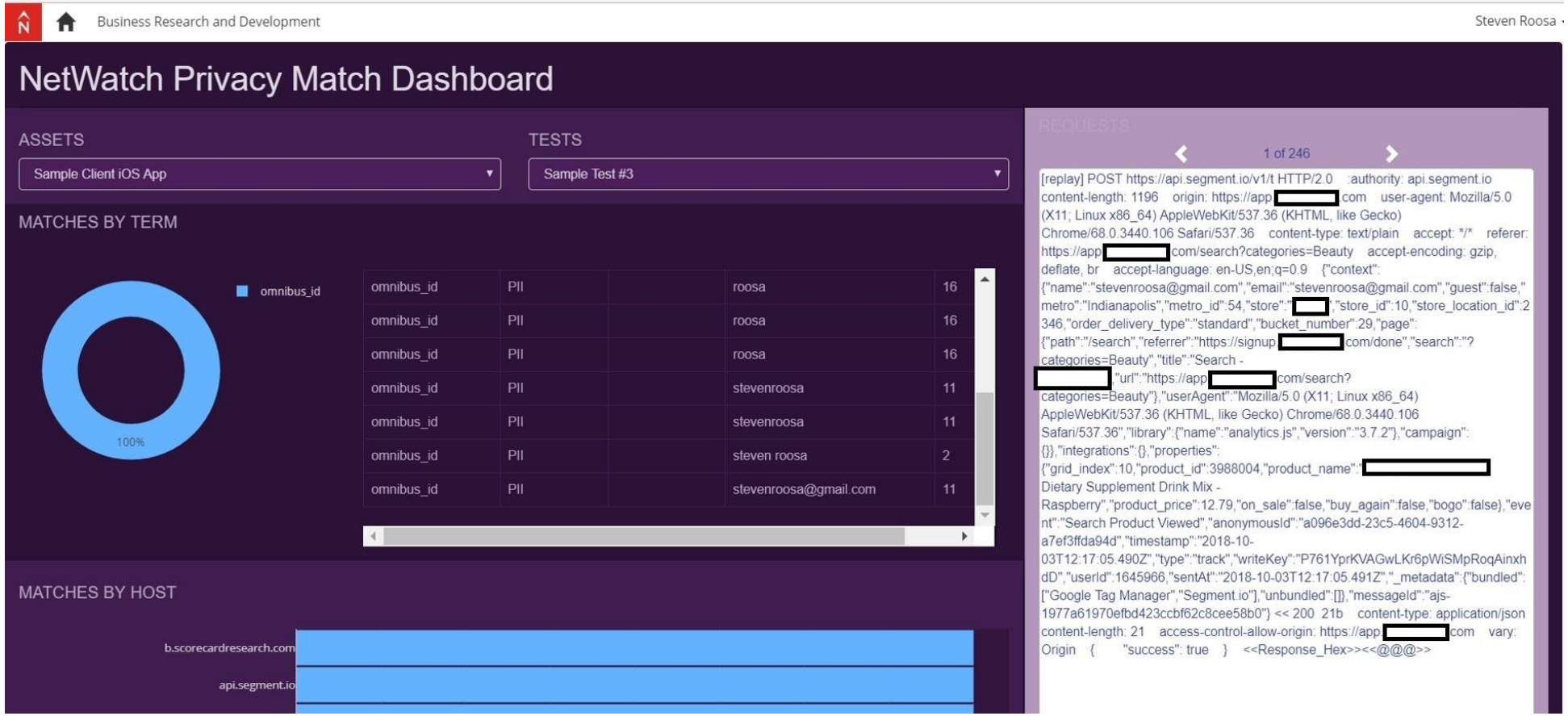
Norton Rose Fulbright's DATA Platform Client App

- Identify the specific kinds of consumer data collected
- Separate data by type: tracking; health; financial; etc.
- Identify the parties collecting data and the data they collect
- Locate the destination of all transmitted data
- Use this information to recommend privacy countermeasures; feature changes; and content for notices/disclosures/consents

Identify Transmitted Data Elements



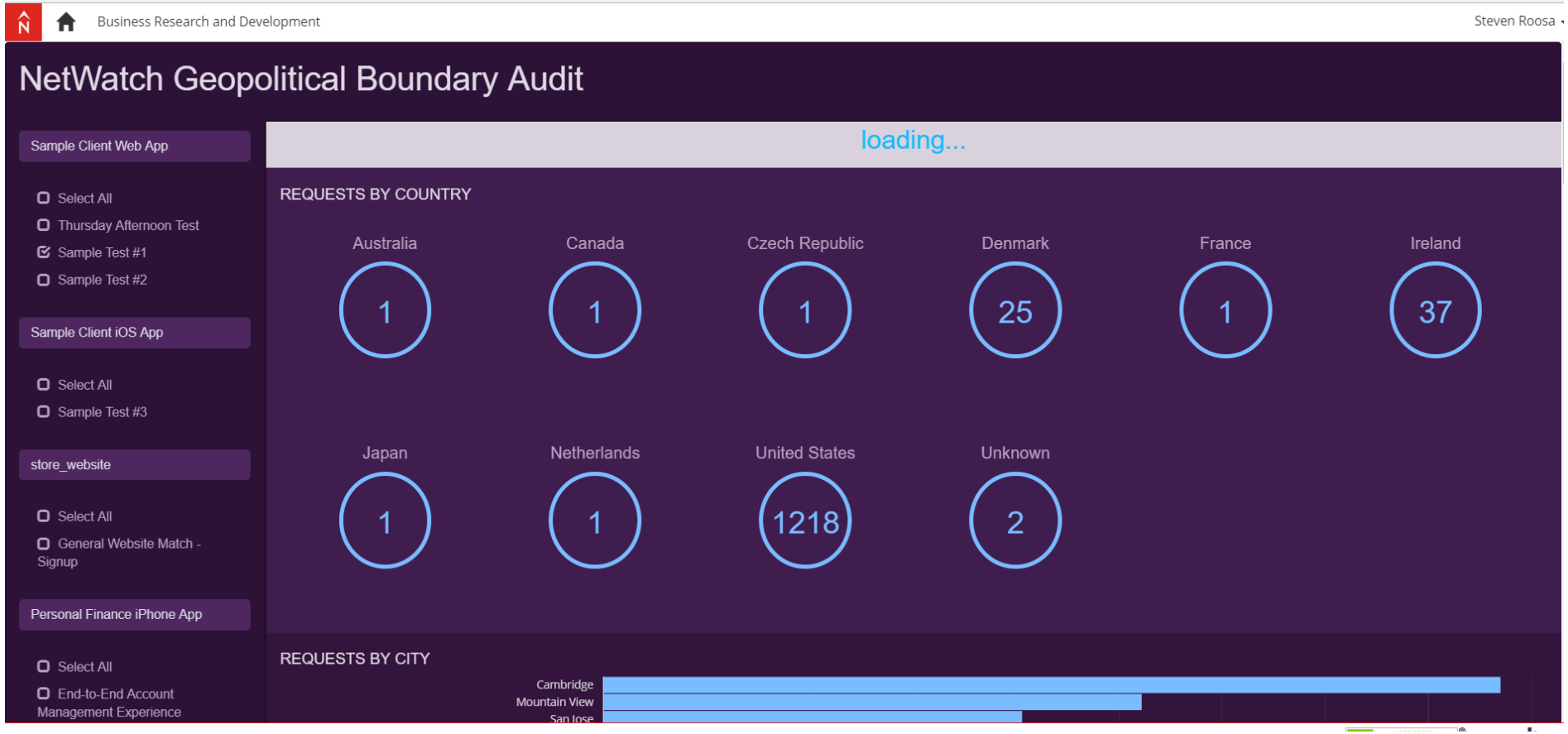
Detailed Drill Down on Network Traffic



Host-by-Host Analysis of Data Collected

host	request count	match count	match terms
play.googleapis.com	6	2	linksys_wps_12552, roosa, stevenroosa, stevenroosa@gmail.com
api.segment.io	5	4	74.91, roosa, stevenroosa, stevenroosa@gmail.com
api.mixpanel.com	4	4	c3rldmvucm9vc2faz21hawwuy29t
b.scorecardresearch.com	4	4	roosa
android.clients.google.com	3	3	roosa, stevenroosa, stevenroosa@gmail.com
www.googleapis.com	3	1	kathleen roosa, roosa, stevenroosa, steven roosa, stevenroosa@gmail.com
mail.google.com	2	2	kathleen roosa, roosa, stevenroosa, steven roosa, stevenroosa@gmail.com
skslm.swiftkey.net	1	1	swift
udm.scorecardresearch.com	1	1	roosa

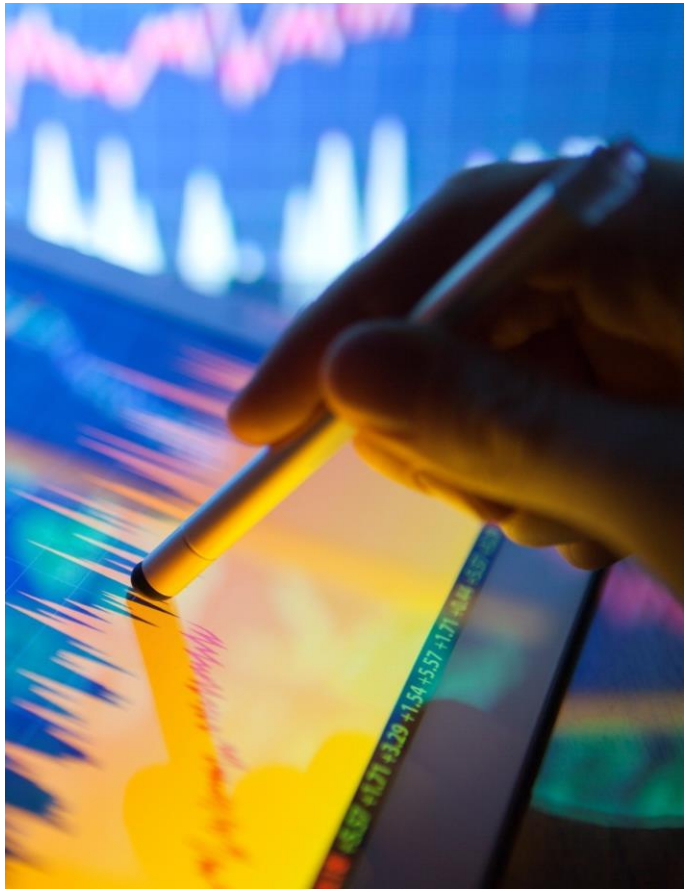
Locating Parties that Collect Data by IP address



Encryption Overview and Considerations

Overview and definitions

- **Encryption** is the process of transforming electronic information into a scrambled form so that it can only be accessed by those who have the algorithm or "key" to unscramble the data.
- Risks of not encrypting data
  - Illegitimate access to data
  - Unwanted modification of data
  - Loss of data

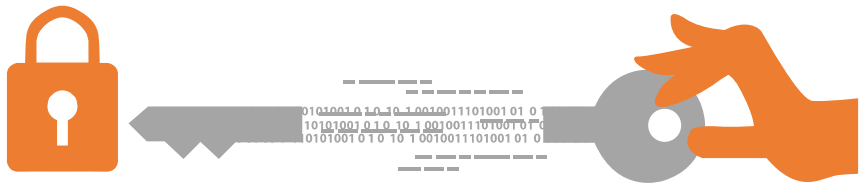


Encrypting data in motion and at rest

Data in motion

Active data that is traveling across a network or sitting in a computer's memory ready to be read, updated or processed.

- Common encryption methods include:
  - Transport layer encryption
  - End to end encryption



Data at rest

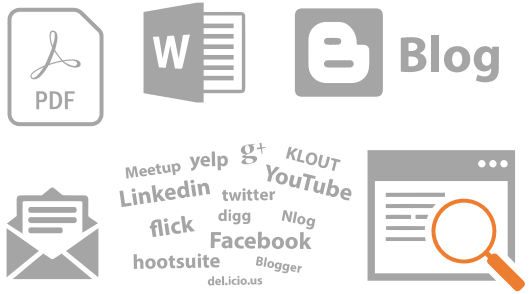
Inactive data which is stored physically in any digital form. Examples include: files stored on hard drives or USB thumb drives, files stored on backup tape and disks, and files stored off-site or on a storage area network.

- Common encryption methods include:
  - Full disk encryption
  - File system encryption
  - Database encryption
  - Volume level encryption

Encryption considerations for structured vs. unstructured data

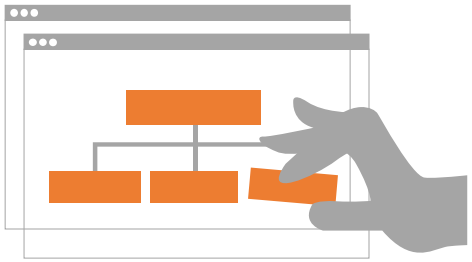
Unstructured data

- What is the volume of data to secure?
- Does the data contain sensitive business or personal data?
- Is the data subject to regulation?
- How is the storage device/platform secured?
- Who has access and what is the access level?
- Can the data be anonymized or pseudonymized?



Structured data

- What is the volume of data to secure?
- Does the data contain sensitive business or personal data?
- Is the data subject to regulation?
- How is the storage device/platform secured?
- Who has access and what is the access level?
- Do certain records, fields or tables require more or less protection?
- Can the data be anonymized or pseudonymized?



Anonymization and pseudonymization

Anonymization

- Recital 26 of the GDPR defines anonymized data as "data rendered anonymous in such a way that the data subject is not or no longer identifiable."
- EU's Article 29 Data Protection Working Party (WP29) acknowledges that true anonymization is difficult to achieve without rendering the data useless, so most firms are opting for pseudonymization.

Patient	Date of prescription	Symptom
REDACTED	1/1/2018	Cough
REDACTED	2/3/2018	Congestion
REDACTED	2/28/2019	Cough

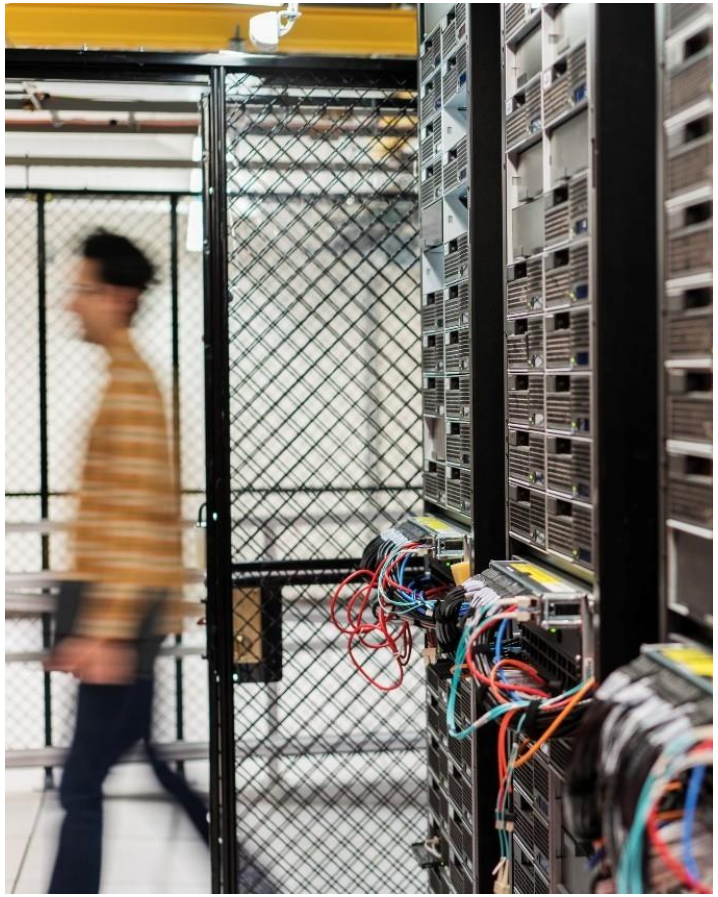
Pseudonymization

- Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."

Privacy ID	Patient Name
a124ghxz	John Doe
f346nazw	Sam Smith
32qrz	Polly Privacy

Patient	Date of prescription	Symptom
a124ghxz	1/1/2018	Cough
f346nazw	2/3/2018	Congestion
q868rtsb	2/28/2019	Cough

Considerations for vendors or processors



- Who will have access to your data?
- What encryption protocols do they use?
- Is data encrypted at rest and in motion?
- How is the physical hardware secured?
- Is multifactor authentication available for the system used to access the data?
- What rules do they have that govern password management?
- How do they handle sensitive business or personal data?
- Do they have an encrypted file transfer system for moving data from your secured environment to theirs?

Data Minimization

The Concept of Data Minimization

- To collect only that data necessary to accomplish a specified purpose.
  - Related to length of time data is retained
- What is “relevant” vs. what is “necessary”
- Sedona Principle 3 – International Principles on Discovery, Disclosure & Data Protection in Civil Litigation
- Privacy rights vs. U.S.-style discovery
  - Privacy is more of a consumer rights issue in the U.S. (sectoral) vs. a individual right elsewhere in the world.
  - Parties may obtain discovery regarding any non-privileged matter that is relevant to any party’s claim or defense and **proportional to the needs of the case**, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

Data Minimization in the U.S.

- Generally U.S. Law focuses on data security, not necessarily purpose limitation or data minimization
- Some exceptions/considerations:
  - HIPAA Minimum Necessary Rule – Purpose Limitation
  - California Consumer Privacy Act – Private Right of Action
- *"We at Apple are in full support of a comprehensive federal privacy law in the United States. There and everywhere, it should be rooted in four essential rights: First, the right to have personal data minimized. Companies should challenge themselves to de-identify customer data — or not to collect it in the first place."*
  - Apple CEO Tim Cook speaking at the 2018 International Conference of Data Protection and Privacy Commissioners in Brussels

Data Minimization (Minimisation) Around the World - EU

- GDPR
  - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed
    - No use for another purpose without additional protections (e.g. consent)
  - Minimization under the GDPR
    - Article 5 – Principles relating to the processing of personal data
    - Article 25 – Data protection by design and by default
    - Article 47 – Binding corporate rules
    - Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
    - Recital 156
- EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
- Article 29 WP Filtering Process

Data Minimization (Minimisation) Around the World - Canada

- Purpose limitation and data minimization (for collection, use and disclosure of both the type and volume of data) are key principles under Canadian Law
  - Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)
  - *Personal Information Protection Act* – Alberta
  - *Personal Information Protection Act* – British Columbia
  - *An Act Respecting the Protection of Personal Information in the Private Sector* – Quebec

Data Minimization (Minimisation) Around the World – South America

- Brazil – *General Law of Data Protection* (August 15, 2020)
  - Privacy principles akin to the GDPR, including the need for data minimization
- Argentina – *Law 25,326 Personal Data Protection Law*
  - New law proposed by President Mauricio Macri - Bill No. MEN-2018-147-APN-PTE
- Chile – A framework of general and sectoral laws in addition to rights granted under Article 19, No. 4 of the Constitution

Data Minimization (Minimisation) Around the World – APAC

- China – *Personal Information Security Specification* (May 1, 2018)
  - Part of the larger Cybersecurity Law framework governing information and communications
- Japan – *Act on Protection of Personal Information* (APPI)
  - Adequacy designation on January 23, 2019
- 7, India – *Personal Data Protection Bill 2018*: DRAFT
  - Privacy a fundamental right though not absolute
  - Purpose, collection and storage limitations

Data Minimization Benefits

- In addition to compliance with privacy laws and regulations
- Mitigate threat vectors
- Decrease storage costs
- Reduce eDiscovery costs
- Have you realized any other benefits?

Basic Steps Towards Data Minimization

- Data mapping & categorization
  - PII/Special Category ID
- De-NISTing
- Deduplication
- Application of Filters
  - File types
  - Date filters
  - Search terms
  - Conceptual filtering
- PII/Special Categories
  - Redaction
  - Pseudonymization/Anonymization

Data Minimization

When Production is Required, Consider Potential Risk Mitigation Strategies

E-Discovery Vendor Selection/Processing

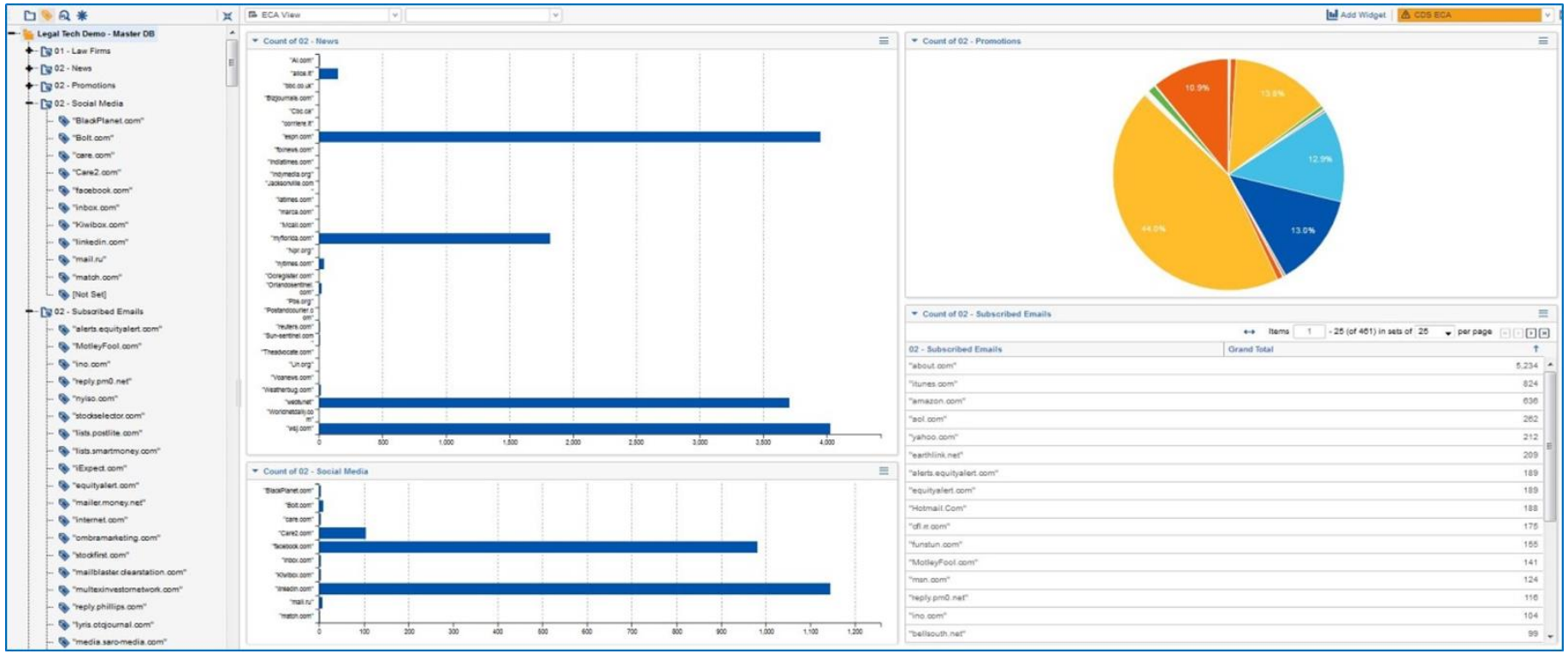
- Process data in the jurisdiction where it resides
- Consider using the same vendor in both jurisdictions so that U.S. data can be de-duplicated against data located overseas
- Consider sampling the de-duplicated data to determine whether an argument can be made that relevant data does not exist in the unique data population
- Select a vendor that is Privacy Shield Certified
- Use available technology to minimize the volume of data that needs to be reviewed prior to production and to reduce the overall burden on the organization, including deduplication, standard filtering (e.g., using date ranges or search terms), early case assessment, and predictive coding/technology assisted review

Mobile Solutions for Minimization

In-country culling, filtering, pseudonymization, anonymization and redaction

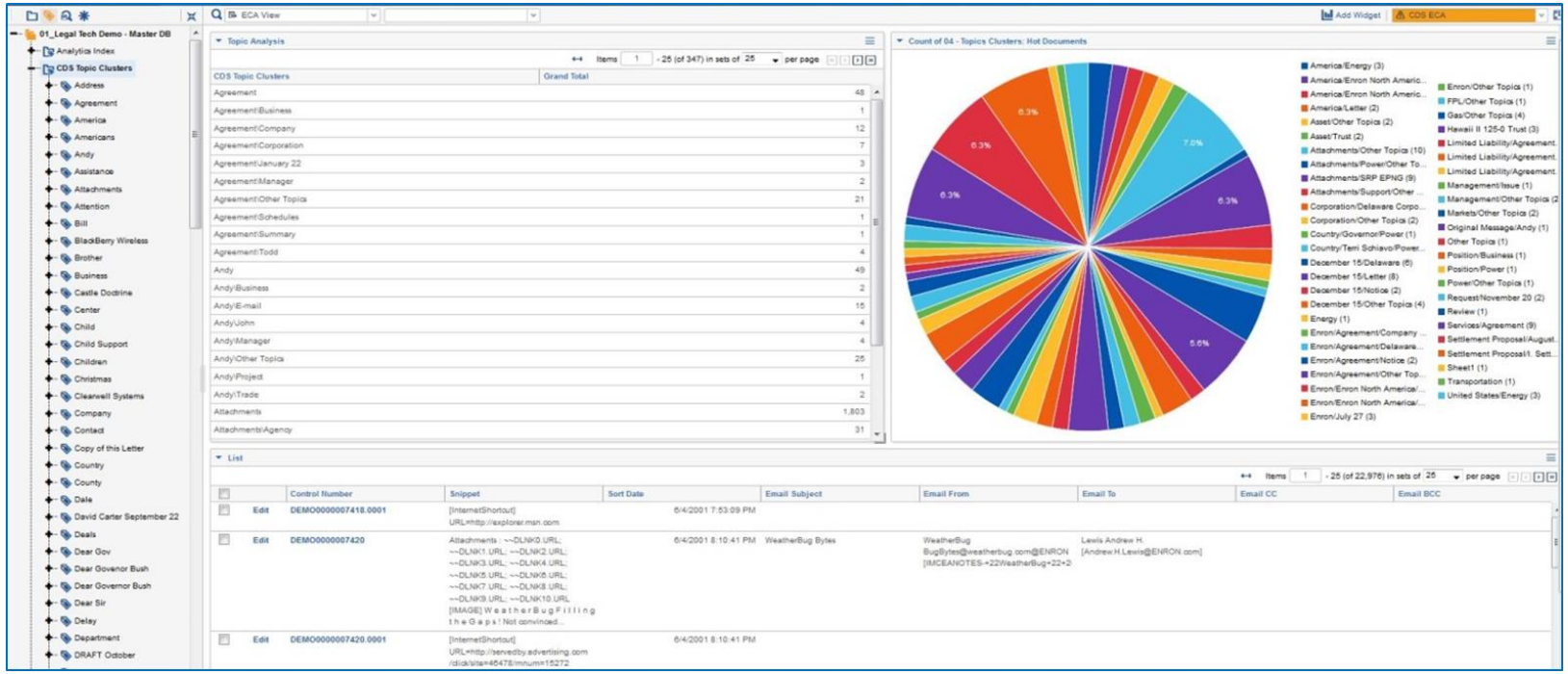
Non-Responsive Data Elimination

Subscriber information and other promotional items



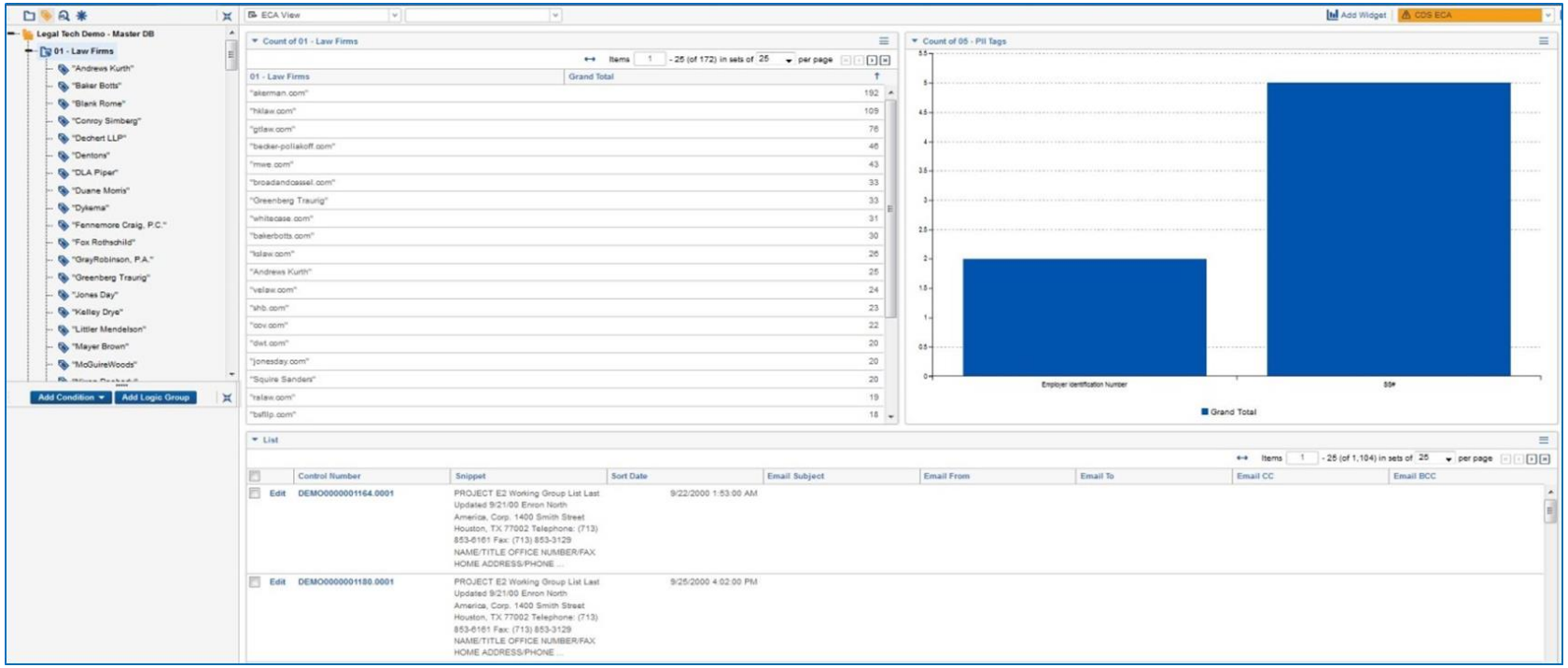
Topic Clusters

- Automatically generated based on document details
- Speed classification and prioritization of document sets for redaction



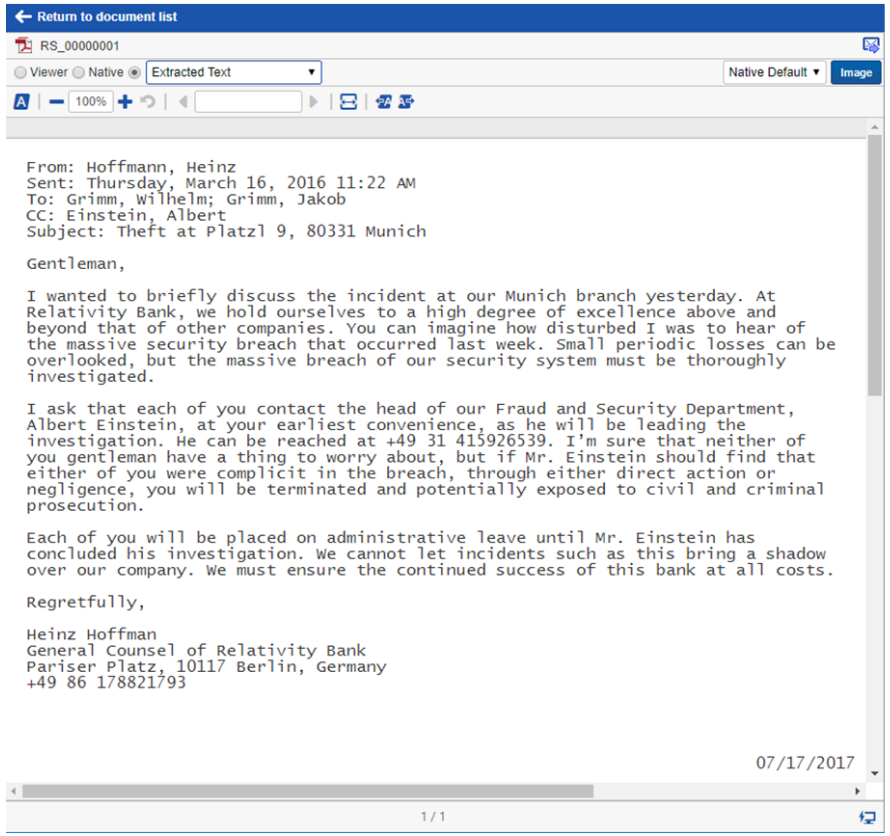
Privilege Screening

- Law firm communications
- PII/Health information and other Regular Expressions

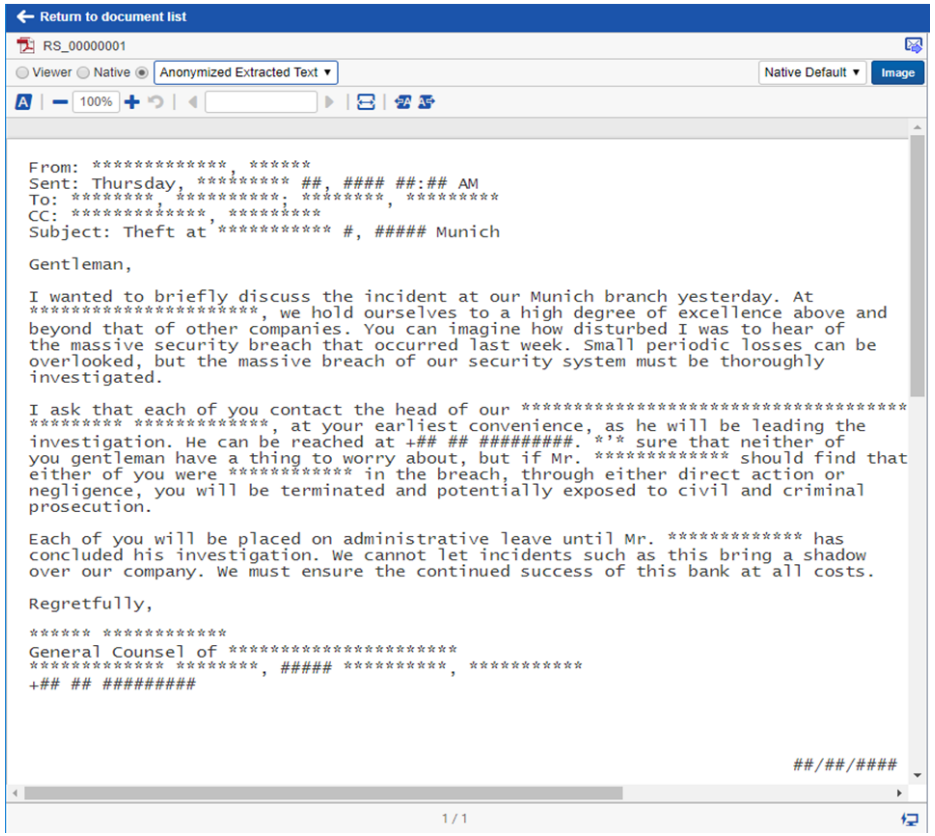


Automated Anonymization/ Pseudonymization

BEFORE



AFTER



Auto-Redaction

- Integrated into the attorney workspace
- Automatically identify PII, PHI, and sensitive data types via pattern recognition
- Auto-redact based on keywords, phrases or regular expressions
- Quality control workflow
- Native Excel redaction

Review In-Country/Continent

When Production is Required, Consider Potential Risk Mitigation Strategies

Data Export/Transfer Agreements

- Have legal counsel and e-discovery vendors execute data export/transfer agreements to ensure that data transferred to the U.S. is afforded appropriate protections by the parties handling it in the U.S.

Document Review

- Have review performed in the jurisdiction where the data resides
- Review for standard issues (e.g., privilege, relevance) but also to determine whether any information subject to the data protection laws is "objectively necessary" to the U.S. litigation (note that this may not be the same as whether the document itself is relevant)

Review In-Country/Continent

When Production is Required, Consider Potential Risk Mitigation Strategies

Document Production

- Consider offering to produce the relevant documents in the jurisdiction where the data resides (or in another authorized country)
  - Can be "produced" for review in a database controlled by the client
    - Opposing party can then identify specific documents that are truly needed for the U.S. litigation and which must, therefore, be transferred to the U.S.
    - Note that review of the documents by the opposing party may still need to be conducted by non-U.S. counsel/individuals

May also consider producing to local counsel in the jurisdiction where the data resides (or in another authorized country), with restrictions on export of data to U.S. subject to agreement

Review In-Country/Continent

When Production is Required, Consider Potential Risk Mitigation Strategies

Document Production (cont.)

- If producing the relevant documents in the U.S., consider:
  - Making the documents available to opposing party in an e-discovery tool selected/controlled by the client, with protective order restrictions on which documents may be printed or downloaded (instead of providing a copy of the production)
  - Requiring the opposing party to use an e-discovery vendor that is approved by the client (e.g. Privacy Shield certified)
  - Requiring that the opposing party's vendor enter into a data transfer/export agreement with the client
- **Document the process, including all steps to protect private information!**

Protective Orders

Make sure you have protective order in place and advocate for provisions that:

- Expressly acknowledge data privacy issues
- Require documents containing personal information to be marked/stamped so those documents can be easily identified and tracked
- Prohibit public disclosure of documents containing personal information, subject to applicable U.S. laws
- Restrict the use of the data to the U.S. litigation
- Restrict access to the documents containing personal information to certain personnel
- Require that specific data security standards/processes be applied to documents containing personal information
- Require destruction of the documents at the conclusion of the litigation

Questions and comments?