Canopy

CASE STUDY

Wotton Kearney Speeds Up Data Breach PII Review by 15% with Canopy

OVERVIEW

Wotton Kearney is an undisputed leader in the provision of legal services to the insurance industry in Australia & New Zealand. The firm has handled several hundred cyber, privacy, and data protection incidents and claims, including some of the largest and most complex incidents in the Asia Pacific region.

An Australia-based financial advisory and accounting business suffered a credential compromise, affecting several mailboxes (PSTs) and endangering sensitive financial information. The company's cyber insurer enlisted WK's Cyber Forensics Service for breach response.

SOLUTION

Seeing a real need to be able to more quickly assess the nature of breaches and help organizations meet non-negotiable notification deadlines, all while managing the cost of cyber claims for insureds and insurance partners, WK chose Canopy's Data Breach Response software as the right tool for the job.

RESULTS

With Canopy's purpose-built efficiencies to help document reviewers speed through batching, reviewing spreadsheets, and linking compromised PII to people, WK's team completed their PII review 15% faster than with alternate tools.

©2025 Canopy Software, Inc.

An Australia-based financial advisory and accounting business suffered a credential compromise, affecting several mailboxes (PSTs) and endangering sensitive financial information. The company's cyber insurer enlisted Wotton Kearney's Cyber Forensics Service for breach response, including the subsequent investigation and notification.

WK is one of Australia & New Zealand's undisputed leaders in the provision of legal services to the insurance industry. In less than three years, the firm has handled several hundred cyber, privacy, and data protection incidents and claims, including some of the largest and most complex incidents in the Asia Pacific region.

Because WK knew upfront that this compromised data set likely contained a great amount of personally identifiable information (PII), its Cyber team anticipated a lengthy breached document review process. In preparation, they sought out a faster, more accurate way to:

- Narrow their focus to just the sensitive documents in the PSTs
- Speed up the process of linking PII to people

"We saw a real need to be able to more quickly assess the nature of breaches and help organizations meet non-negotiable notification deadlines, all while managing the cost of cyber claims for insureds and our insurance partners," said Kieran Doyle, Head of Cyber, Privacy and Technology at WK. "When we discovered Canopy's Data Breach Response software, I knew that their AI-driven tech was the solution we needed."

AI-Powered Data Mining Hones PII Review Focus

WK's forensics experts were quickly up and running with Canopy's Data Breach Response software. They leveraged their market-leading knowledge of Australia's breach requirements to set up a data processing template, then put the software to work.

Unparalleled Processing Power and Speed

76.77 GB
total size of compromised PSTs

829,000+
documents contained in the PSTs

15
categories of PII detected

©2025 Canopy Software, Inc.

The compromised PSTs totaled 76.77 GB, consisting of 829,422 documents. Canopy's advanced AI and machine learning algorithms detected 15 different categories of PII, including high-risk data like bank account, credit card, and tax file numbers. As soon as Canopy completed processing, it generated a report showing WK's team the findings, including:

- Categories of PII,
- Amount of PII, and
- Where the PII existed.

> "Canopy gives us the ability to target PII with precision, which is the single most effective way to focus our review team's efforts and keep costs low."
>
> **Kieran Doyle**
> Head of Cyber, Privacy and Technology

WOTTON KEARNEY

Without Canopy, WK's team would have engaged the use of ediscovery platforms that are not fit-for-purpose to undertake data mining and review the data set for PII. In contrast, Canopy is purpose-built for PII reviews, as it runs optimized algorithms which accurately detect PII. This makes Canopy a far more efficient and, therefore, cost-effective solution for analyzing compromised mailboxes and setting up workflows for PII reviews.

"Reviewers need to look through every potentially sensitive document for PII. When dealing with large data sets like this, the review is time-consuming and costs can quickly skyrocket," said Kieran. "Canopy gives us the ability to target PII with precision, which is the single most effective way to focus our review team's efforts and keep costs low."

Machine Learning Speeds Up PII Review by 15%

Canopy's workflows gave WK's reviewers additional efficiencies, enabling them to work faster than ever. Before Canopy, reviewers would manually copy-and-paste PII and people from each sensitive document into an Excel spreadsheet.

Canopy's machine learning and intuitive user interface transformed this process into an accept-or-reject workflow. The most time-saving tools were:

Batching: Project leads can run queries, group by file or PII types, and set their batch size; then, Canopy automatically doles out document sets to reviewers.

Suggested Entities: Using natural language processing (NLP) and other machine learning models, Canopy alerts reviewers when it detects PII belonging to an existing entity. Reviewers simply accept or reject the suggestion.

Smart Map: Canopy imports data from spreadsheets in seconds, taking the pain out of dealing with Excel files. Pair your columns with corresponding database fields and preview the mapping, then let Canopy do the rest.

Entity Panel: When reviewing emails, PII is automatically highlighted and classified. Reviewers select an entity and check the boxes next to each related PII element, then see it all populate together in the Entity panel.

"In addition to drawing our focus directly to sensitive documents, Canopy's Data Breach Response software increased our reviewers' speed by approximately 15%," said Jorge Nicholas, Associate at WK. "When it comes to batching, reviewing spreadsheets, and linking compromised PII to people, other tools simply cannot compare."

> "When it comes to batching, reviewing spreadsheets, and linking compromised PII to people, other tools simply cannot compare."
>
> **Jorge Nicholas**
> Associate
>
> WOTTON KEARNEY

WK & Canopy: The Future of Breach Response

WK's market-recognized experts have a deep understanding of the regulatory framework surrounding protected data in Australia, New Zealand, and other jurisdictions across the globe. Pairing this knowledge with Canopy's emerging technology, WK can now deliver faster and more accurate breach assessment and notification services to its clients while simultaneously managing cyber claim costs for its insurance partners.

"WK is shaping the future of insurance law, so it fits perfectly that our firm introduces Australia and Asia-Pacific to this AI-driven technology," said Kieran. "Our Cyber Forensic Services, powered by Canopy, are transforming how the region approaches data breach response."

©2025 Canopy Software, Inc.