Cyber Forensic Services

W+K's AI-powered PII detection service in partnership with Canopy

Canopy

W+K leverages Canopy's advanced Data Breach Response technology to help you meet non-negotiable notification deadlines

W+K is a Canopy partner. Our Cyber, Privacy and Technology team has been trained in Canopy's Data Breach Response software and can meet your breached data assessment, data mining, review and notification needs.

Accurate, timely and cost-effective

When a data security incident occurs, breach response teams need to quickly assess whether it is legally considered a breach. If so, they must meet strict, non-negotiable notification deadlines enforced by data privacy regulations.

By using Canopy's Data Breach Response software, W+K can reduce the time, cost, risk, and effort associated with the defensible detection of sensitive data by streamlining data breach response at every step, from process through to notification. Importantly, engaging W+K to do this work means you will work with experts who understand the regulatory framework and who will maintain legal professional privilege, which can reduce exposures if action is taken later.

"When a U.S.-based online retailer was breached, their response team first employed traditional keyword search methods which flagged 90,000 sensitive documents for review. Comparatively, Canopy's advanced PII detection algorithms accurately flagged just over 10,000 documents, saving the response team 2,000 hours in review."

Case Study

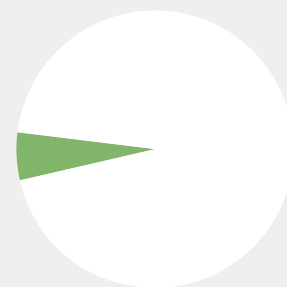Canopy Reduces Review Population by 89%, Saving Response Team 2,000 Hours. Read more **here**.

Original Data Set: **186,479 Documents**

90,000
documents
to review

ediscovery
methods

10,106
documents
to review

Canopy

W+K's cyber forensic solution using Canopy

PHASE ONE **Process**	PHASE TWO **Assess**	PHASE THREE **Review**	PHASE FOUR **Consolidate**	PHASE FIVE **Notify**

Using AI, Canopy quickly identifies different types of personally identifiable information (PII) in any data set – including emails, text documents, spreadsheets, PDFs, and many other file types.

W+K uses Canopy's processing, which is completed in Phase One, to eliminate the need for iterative searches. This means we can immediately flag sensitive documents for review making it faster to assess the scope of the breach response project.

Canopy enables W+K's skilled document reviewers to work even faster, making it easy to connect the identified people and PII detected in your data set. As Canopy learns about a specific project, its AI turns the process of linking PII to entities into a simple 'accept or reject' workflow, eliminating the need to copy-and-paste data into spreadsheets.

Canopy's advanced entity management functionality takes the heavy lifting out of entity resolution, with features including automatic deduplication and suggestions for merging entities.

The ultimate deliverable of any data breach response project is a consolidated list of unique affected individuals and their compromised PII. As the W+K team works, Canopy consolidates this information, which means we can export the list as soon as the review is complete.

Reduce risks by getting faster, more reliable PII assessments

Save time, cost and effort using proven AI-enabled tech solution

Maintain legal privilege by engaging W+K to deliver PII assessment

For more information contact W+K's Cyber, Privacy and Data Protection team leader:

Head of Cyber, Privacy and Tech Liability

Kieran Doyle
Partner, Sydney

T + 61 2 8273 9828
kieran.doyle@wottonkearney.com.au