

CASE STUDY

ProSearch Privacy Suite Pivotal in Identifying PII

ProSearch leverages Privacy Suite to identify PII in the wake of a critical data breach, protecting the client company's reputation and enabling successful notification under tight timelines.

Cyberattackers Hit Corporate Data

A large organization was victim of a data breach when hackers obtained unauthorized access to company data. On identifying the breach, the company rapidly responded to secure system access and prevent further unauthorized incursions.

As part of the breach response, an equally important concern was to identify any affected personal information belonging to employees, customers, or business partners to aid in notification and remediation. The company turned to ProSearch for assistance in analyzing the at-risk data and identifying personal or sensitive data.

The ProSearch Approach

The company asked us to query all data hosted in ProSearch data centers to locate ~100 data files. ProSearch was able to provide immediate access to a robust tool set for data analysis, information retrieval, and technology-assisted review.

Working closely with the client's outside counsel, ProSearch provided daily reporting and analysis and helped them to pivot as needed—often daily—to accommodate emerging data stories. The ProSearch project team and data scientists have been integral to counsel's efforts to present the clearest possible story about scope and impact, enabling transparency that has reduced reputational damage that otherwise might have occurred as fallout from the breach.

Purpose-built Tools: ProSearch Privacy Suite

IN DEPTH

5 Days

4 Workflows

3 Analytics Tools

2 million documents

1 Platform

ProSearch quickly identified data that represented personally identifiable information or sensitive HR, client, or reputational risk, helping the client to avoid additional costs, time delays, and risks of moving data to another workspace. Within 48 hours, reporting and analysis began.

Based on deep learning solutions for high-precision/high-recall identification of SSNs, the initial scope report provided by ProSearch was significantly more accurate than the best estimate counsel could provide without further insights. This allowed the company to expedite its response and to be transparent from the start, thereby reducing reputational risk. Working with internal stakeholders and key partners of the company, ProSearch established process for continuous improvement and helped streamline communication for efficiency and clarity.

ProSearch Privacy Suite was deployed along with Brainspace, NexLP, and Relativity Analytics to support four concurrent workstreams, all engineered to prioritize and reduce document review:

1. PII Identification for Notification—privacy results returned in 24 hours.

ProSearch Privacy Suite ran over 2M documents and identified 23 categories of PII in 73K documents; the potential PII was highlighted to accelerate review. The population was further reduced to 9K after applying prioritization techniques.

2. Sensitive HR—combined technologies to target 1K docs for review.

ProSearch experts deployed the Medical Information modules of ProSearch Privacy Suite and conducted targeted searching enhanced by Brainspace Concept Search. This led to required review of only 1K documents in a 16K boundary.

3. Client Data Identification for Notification—improved search and prioritized client data review.

Received 150K search terms with syntax errors, stop words, and redundancy. ProSearch's Syntax Inspector allowed us to run an error-free list within 48 hours. Of 1.2M docs containing client names, only 17K were prioritized for review — a reduction of 99% in the review set.

4. Reputation—prioritized 17 negative documents for review.

ProSearch's Reputation Filters targeted files with bad words and emotional language. Paired with Brainspace Concept Search and continuous multimodal learning, 175K documents were reduced to 16 for prioritized review.

150k
SEARCH TERMS

48
HOURS

99%
REDUCTION

Results: Cost-Effective Compliance within a Tight Timeline

- List of 150K search terms executable within 48 hours
- 99% reduction in document review set
- Highly accurate data normalization identifying the true number of affected parties

This cyber incident response brought together an extended team of legal experts and discovery professionals who hadn't previously collaborated. ProSearch partnered with stakeholders from across our client's corporate organization, including IT, legal, and compliance, as well as their trusted advisors in outside counsel and managed review support.

Together we engineered a unified solution that met the immediate needs of the matter while simultaneously laying the foundation for the inevitable "long tail" of investigation and litigation that can follow a data exposure event. Our combined skills, tools, and strengths quickly measured impact and scope, strategically targeted information of interest, compiled data, and provided analysis and QC to ensure accurate reporting for continuous improvement.

Why ProSearch?

ProSearch enables corporations and law firms to meet eDiscovery, fraud investigation, compliance and IG requirements at scale with precision and ease. The ProSearch team of consultants, data scientists, linguists, project managers, attorneys and discovery specialists collaborates with clients to execute their matter strategies and ensure on-target, on-budget, on-time delivery. Because discovery is a business process that can be measured, managed and improved, ProSearch offers an Enterprise solution tailored to align with an organization's business goals by providing operational excellence that transforms its discovery processes. To learn more visit ProSearch.com.

Contact us to talk about our next generation discovery solutions.

www.prosearch.com • 877.477.7291 • press@prosearch.com