Legal Data Intelligence

Data Breach Response

Initiate

Scope Project and Set Goals
Some common goals include:
- Gathering information sufficient to notify affected individuals whose personal information was impacted
- Identifying the number of affected individuals by jurisdiction and the information types that were compromised for communication to privacy regulators
- Identifying sensitive information not typically considered personal information, such as business confidential information and financial information of vendors
- Identifying the plaintiff class for a proposed class action arising from the breach

Identify Potentially Compromised Data
Work with data forensics team to identify potentially impacted data

Upload Potentially Compromised Data
Once compromised data has been identified, upload to a review tool for assessment

Tech's Role
Pulls data from sources into a platform for processing

Conduct Initial Assessment
- Identify groups of documents that are not likely to contain personal information (PI) or sensitive information
- Identify key groupings of documents (the "Review Set") that are likely to be rich in personal information

Tech's Role
Provides a variety of functionalities to conduct the initial assessment, including search terms, regular expressions, Boolean operators, AI, and analyses and categorization of document types, titles, sizes, and subject matter

Investigate

Search
Once the Review Set has been narrowed down, create search parameters depending on the specific types of PI, personal health information (PHI), and personal sensitive information (PSI) that are likely to appear in the data set

Tech's Role
Provides a variety of functionalities to conduct the search, including search terms, regular expressions, Boolean operators, and AI

Develop a Review Protocol
Develop a detailed protocol to maximize consistency, accuracy, and efficiency in the data analysis. At a minimum, the protocol should include:
- A description of the affected organization's business and the types of data likely to be included in the Review Set
- A detailed description of each type of personal information that should be recorded
- Coding instructions

Tech's Role
Identifies sample documents from the Review Set to provide as appendices to the Protocol to demonstrate the nature of the information reviewers are likely to come across and how to treat different information types

Review Data
- Identify PI, PHI, and PSI and record the affected individuals
- Associate the PI, PHI, and PSI to the affected individuals

Tech's Role
AI enables the quick extraction of personal information and the association of entities (affected individuals) with linked PI, PHI, and PSI

Implement

Create a Notification List
- Create a report containing the following information:
- Those who are impacted including specific information about what types of information are implicated
- The affected individuals for whom there is no contact information
- Privacy regulators having jurisdiction over the affected individuals

Tech's Role
- AI tools populate the affected individuals in a column and all their associated PI traces in rows
- AI easily normalizes duplicate records belonging to the same individual

Notify Individuals and Regulators
- Inform affected individuals
- Apprise privacy regulators with details on how many individuals were impacted, along with the types of information impacted in the breach

Tech's Role
AI helps prevent duplicate notifications to the same affected individual and consolidates all notifications