COVER

PRIVACY MATTERS

Solving the many challenges of personal information in discovery with AI enhanced privilege review.

WRITTEN BY JOSHUA GILLILAND, ESQ.

PRIVACY LAWS PROTECTING

Every person values their privacy. The European Union, the United States, and many states have enacted laws to protect information that people would not want public. Examples of these laws include individually identifiable health information created by a health care provider that relates to the past, present, or future physical or mental health or condition of an individual. The European Union enacted the General Data Protection Data Regulation (GDPR) in 2016, which stated in Recital 1 that the, "protection of natural persons in relation to the processing of personal data is a fundamental right." California has had data privacy laws for years and is expanding data protection with the California Consumer Privacy Act (effective 01/01/2020). The new CCPA will cover personal information that includes the following that can be associated with a consumer or household:

- Real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Commercial information that includes purchase history;
- Biometric information.
- Internet history
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information that is not publicly available.

This is just a sample of the types of laws that protect personal information. However there are many commonalities between these laws. They are all designed to protect private information from being disclosed and have procedures to follow in the event of a data breach.

A KEY COMPONENT OF EDRM

The Electronic Discovery Reference Model (EDRM™) has anchored privacy rights and control of personal information at each stage of discovery. With these interests in mind, the identification of private or sensitive information early in the EDRM process is critical to understanding the nature of electronically stored information for preservation. Moreover, this realization is a constant reminder on the sensitivity of the ESI throughout the life of the case.

PROTECTING PRIVACY WITH COVER

COVER can help lawyers conducting privilege review by identifying personal identifiable information, protected health information (PHI), and keywords in electronically stored information (ESI) for redaction, while retaining the format of the original file. A production with COVER will include fully searchable PDFs, minus any privilege information, with privileged sections redacted. These features can ***automate*** *privilege review for information protected by privacy laws and help* ***expedite*** *identifying communications protected by evidentiary privileges, saving both time and money. As a key component of eDiscovery workflow, COVER allows user interaction through A) identification, reporting and foldering; B) search and C) mass action redaction.*

IDENTIFY (A)

COVER can generate a report identifying PII (Personally Identifiable Information) and a record count for Rule 26(f) conference negotiations. These reporting capabilities allow attorneys to fully understand the type of PII that can be within a dataset to avoid an inadvertent disclosure of protected information. Furthermore, creating tags or folders which contain each PII type would give project managers and clients a high-level view of potential collection risk,identify any additional steps that might need to be added to the case workflow and would give reviewers a constant visual cue of any special treatment that may need to be part of their review.

SEARCH (B)

Attorneys and project managers can create syntax searches to find known private information, which can be uploaded in COVER, or create saved searches. Boolean searching for keywords has long been the mainstay of a solid eDiscovery investigative workflow. With PII such as Credit Card numbers, the problem is there could be thousands of different credit card numbers in a dataset. Searching for each individual number is neither practical nor easily accomplished. With COVER, the user simply needs to search for 'CreditCard' and documents that contain any credit card number are returned. For example, the system is even smart enough to ignore sixteen-digit numbers that don't meet the CreditCard number algorithm. The same is true for names, dates, places, bank accounts, phone numbers etc, and the ability to search generically for items that you don't know could be a significant time saver on any project.

REDACT (C)

ESI and documents imported into COVER can be scanned for PII along with searching for sensitive information such as financial data, keywords, or phrases as determined by counsel to automate privilege review for information protected by privacy laws by performing mass redactions of any text or phrase in a native file. Trade secrets such as source code can also be identified and readacted. However, while text tables in native files can be redacted, redacting text embedded in Excel files is currently in development.

Once information is identified for redaction, COVER is an automated workflow to identify and redact information from disclosure. Redacted information can have placeholder text such as “CREDIT CARD” or “TRADE SECRET” to identify what confidential information has been redacted. COVER can identify the type of credit cards by their numbers, so text overlays can identify the type of credit card number that is redacted.

Redacting information protected by evidentiary privileges is a highly similar workflow to PII . However, given that privilege logs require a description of the claimed privilege, the workflow is best completed in their review platform. Domain names for law firms, clergy, or medical professionals, can be identified in COVER with highlights for attorneys to review. Using this information in ICONECT, attorneys can identify privilege communications to withhold from production and meet their privilege log requirements.

BENEFITS OF USING COVER

- REDUCE RISK
- AVOID SANCTIONS
- E-DISCOVERY
- WORKFLOW INTEGRATION
- SAVE TIME
- SAVE MONEY
- EASY TO USE
- COST EFFECTIVE

PROTECTING PRIVACY IN DISCOVERY

We live in an age where a person literally carries vast quantities of personal information on their smartphones. The proliferation of digital information raises many challenges for only producing what is both relevant and non-privileged in a lawsuit. When it comes to conducting privilege review, there are twin goals for protecting privileged information: safeguarding personal information protected by privacy laws, such as medical information, addresses, phone numbers, and credit cards; and keeping information protected by evidentiary privileges such as attorney-client or spousal from disclosure. There are substantial more to include protected by both evidentiary rules and privacy laws, but these all boil down to the same fundamental truth for attorneys: effective privilege review, redaction, and creating a privilege log.

EVIDENTIARY PRIVILEGES PROTECTING CONFIDENTIAL COMMUNICATIONS

Privilege communicates exist to encourage people to speak freely with those who have a fiduciary or statutory duty to protect their professional advice given to those seeking it. The traditional example in a lawsuit is attorney-client communications or work product, but can include doctor-patient, psychological, clergy, and other privileges identified in state evidence codes. The key elements of these communications is an exchange with a person seeking a professional opinion from an individual licensed to provide such a professional opinion, or the professional in turn providing advice, in a secure manner that is not disclosed to others.

PRIVILEGE LOG REQUIREMENTS

A producing party that withholds relevant information from production must explain why in a "privilege log." The basic privilege log requirements include 1) expressly making the privilege claim and 2) describing the nature of the information that will enable the other party to assess the claim without revealing the privileged or protected information. Moreover, privilege log requirements apply implicitly to documents produced with redactions. However, courts have not required a "redaction log" for the redaction of confidential information such as personal identifiable information, because such redactions are common practice and can comply with local rules for protecting personal identifiable information.[6] While that implies that privileged logs are required for information redacted pursuant to an evidentiary privilege, saying that information redacted based on privacy law does not require a privilege log as a maxim, would be a risky rule statement. Such a determination of whether a redaction log for private information could vary based on local rules, ESI Protocols ordered by the court, agreement by the parties, or determined by the needs of a case.

[1] *Riley v. California, 134 S. Ct. 2473, 2485 (2014).*
[2] *42 U.S.C. § 1320d.*
[3] *Cal. Civ. Code § 1798.140(o)(1).*
[4] *Fed. R. Civ. P. 26(b)(5)(i)-(ii).*
[5] *H&L Assocs. of Kan. City, LLC v. Midwestern Indem. Co., Case No. 12-2713-EFM-DJW, at *14-15 (D. Kan. Oct. 25, 2013).*
[6] *Henry v. Ocwen Loan Servicing, LLC, Case No.: 3:17-cv-688-JM-NLS, at *3-4 (S.D. Cal. Apr. 17, 2018).*

CREATING REDACTION LOGS WITH COVER

Redactions in COVER are logged, which can be exported as a redaction log with the number of each redactions for personal information protected by privacy laws. The redaction report can also be used during meet and confers with opposing parties or for reporting to the court.

EFFICIENTLY PROTECTING PRIVACY

Privilege review can be a time consuming process, especially if there is personal identifiable information in addition to privileged communications. Leveraging COVER, attorneys can automate redacting personal information protected by privilege laws. Attorney time can then be focused on expressly claiming privilege communications to comply with evidentiary rules, while also ensuring personal identifiable information is not inadvertently produced.

ABOUT ICONECT

iCONECT Development, LLC develops the innovative iCONECT eDiscovery review software platform. iCONECT raises the bar by delivering intelligent, easy-to-use tools that help hosting providers, law firms, and legal departments optimize workflows and manage some of the world's most complex legal cases more efficiently. Leading AI and auto-redaction capabilities combined with a user's ability to search, sort, analyze, categorize and produce documents and multi-media files recently led industry publication 'Silicon Review' to name iCONECT as one of the '30 Fastest Growing Tech Companies' of the year.

ABOUT THE AUTHOR

Joshua Gilliland
Twitter: @bowtielaw
Josh@bowtielaw.com

Joshua Gilliland is a California attorney creator of the eDiscovery blog Bow Tie Law and has presented at over 400 eDiscovery seminars and webinars. Josh is co-creator of The Legal Geeks blog and podcast, which has made the ABA Journal as one of the top 100 blogs for lawyers from 2013 to 2018. Josh grew up in Silicon Valley and is a graduate of UC Davis with a degree in Political Science and earned his law degree from McGeorge School of Law, University of the Pacific. Josh enjoys organizing panels and mock trials at comic conventions, photography, and volunteering in Scouting.

iC10008

FIND OUT MORE

Contact iCONECT for more information.
www.iconect.com | info@iconect.com | 1-855-915-8888

Copyright© 2018 iCONECT Development, LLC. All rights reserved. iCONECT and XERA are registered trademarks of iCONECT Development, LLC. 20180511

LEARN MORE