Managing Privacy in Data Requests

Technology, Privacy, and eCommerce


DO NOT
DISTURB
PRIVATE
DATA


DO NOT
DISTURB
PRIVATE
DATA

CHEAT SHEET

- ***Data privacy can be burdensome.*** Data privacy standards apply not only to information security and retention policies, but also mediate the transmission of data to third parties.
- ***Not all data requests are made equal.*** Mutually agreed and court mandated discovery requests and government regulatory inquiries must generally be followed, but third-party requests do not always have to be honored.
- ***Privacy as a barrier to disclosure.*** Data requests must be reviewed vis-à-vis the relevant privacy regulations, and privacy considerations may sometimes be justification for moderating the scope of a request or not complying altogether.
- ***Be wary of PII.*** Avoid releasing Personally Identifiable Information by masking, through replacing data values with generic replacements, or simply redacting the data but retaining the original structure.

Data requests are an important and increasingly common undertaking for corporate counsel to manage. Recent regulatory changes in the United States and abroad have resulted in sanctions and litigation arising from violations of individuals' data privacy rights due to mishandlings of data requests. Apart from the standard data privacy control of one's organizational data, similar data privacy processes and considerations should be applied when responding to data requests. This article details considerations of which you should be aware when responding to data requests, as well as several techniques that can be applied to avoid running afoul of industry and regulatory data privacy rules while still effectively responding to these requests.

The data privacy burden

Data privacy issues have been making headlines for several years and legal counsel are increasingly the first and last lines of defense for organizations. You are often responsible for ensuring that private information is not exposed, and managing the repercussions if such an event does occur, whether it involves an employee losing a laptop with sensitive data, a data breach or a violation of consumers' data privacy rights. This data privacy burden requires that you understand all areas of exposure to eliminate or mitigate potential violations.

One new form of concern for general counsel is maintaining control over data privacy in responding to data requests. In January 2015, the US Financial Industry Regulatory Authority (FINRA) reached a settlement with a a brokerage firm over a data privacy violation. The brokerage firm improperly released private customer data to a third party that requested information for a separate litigation matter. The firm was not involved in the litigation, so it did not have the right to send customer information to the third party. As such, the firm violated its customers' privacy rights and was subsequently fined.

This type of incident is becoming increasingly common. The European Union (EU) and Canada have been actively monitoring organizations' adherence to data privacy laws, and various US regulatory

bodies are now following suit. In addition, violations of industry standards and regulations have led to a number of civil litigation cases. Data privacy standards and regulations apply not only to information security and data retention, but also determine how data is transmitted to those outside an organization — including how you manage data and respond to data requests.

This article covers several major considerations for when you respond to data requests and how to ensure that data privacy violations do not occur.

Data requests

Counsel typically respond to various forms of data requests. The most common type is a discovery request, which is a court-ordered or mutually agreed-on request with specific parameters and is usually protected by a confidentiality order. The second type is a request as part of a government regulatory inquiry. These requests, too, can be protected by confidentiality agreements, although new forms of government requests related to the USA PATRIOT Act span multiple industries and privacy standards. The third type is third-party requests, which arrive from clients, suppliers, other business partners and third parties without a preexisting business relationship.

A data request can include data in various forms and from different types of systems and storage, which pose challenges to counsel. Email, document files and transactional data (e.g., database records) are still the most common types of data requested, and requests involving these forms of data can span multiple systems and require collecting data from cloud storage and offline storage (e.g., backup media, near-line systems and archive systems). In addition to managing the retrieval of data, counsel must be aware of what types of information are contained in the data before turning them over. The data may contain privileged information and personally identifiable information (“PII”) for which you should perform reviews to ensure that the information either is not released or is masked or redacted to prevent an improper data disclosure.

Data requests do not always have to be honored, and data privacy presents a possible opportunity for limiting the scope of a request or altogether denying the request. Every data request must be reviewed vis-à-vis applicable privacy regulations and standards, because data requests and data privacy considerations are rarely mutually exclusive for organizations.

In litigation, the meet-and-confer offers counsel an opportunity to discuss concerns and potential limitations in response to a data request. Data privacy is a serious matter that should be discussed in the initial stages. If you believe that data privacy may be an issue, steps should be taken in this stage to limit the scope or agree on a method for masking private information to avoid running afoul of privacy regulations and standards. You may be able to limit the scope by masking PII to provide transactional information without exposing any PII. If the request does not arise from litigation that involves your organization, data privacy can be used as a basis to limit or deny the request.

If PII must or may be produced, then data privacy is a necessity and you should take steps to ensure that safeguards are in place to protect the PII. First, agreements permitting data to be shared in such circumstances and that the data’s confidentiality and security must be protected should be in place with both the PII subject and the party making the data request. Even with those in place, you should discuss the safeguards and privacy controls the requesting party has in place. Basic controls include:

- Internal security controls and encrypted drives that prevent unauthorized access;
- Limiting access to the data to a need-to-access basis;
- Requiring signed confidentiality agreements from every individual who can access the data;

and
- A precise data destruction policy.

Data requests as part of regulatory exams or court-ordered government requests cannot be managed in the same manner as those from private-sector organizations. You cannot negotiate the terms of the data request in the same way when a regulator or government agency with a court order requests the data. Instead, you should proactively review all customer and business-partner data privacy agreements to cover the organization and amend them where necessary to permit required disclosure requests.

Regardless of the type of data request, you should be aware of the data privacy standards and regulations that apply to your industry and the geographic locations of your customers and your operations. Federal or intergovernmental regulations in the United States, Canada and the EU are established but continuously change. For example, the EU has drafted the General Data Protection Regulation ("GDPR"), which it plans to implement in 2015 or 2016. The GDPR will replace EU Data Protection Directive 95/46/EC, which the EU currently believes fails to properly address data privacy issues related to changes in technologies, such as social media and cloud computing.

In addition to those regulations, state and municipality regulations are overlaid to provide specific requirements and protections. States such as California have passed their own laws and regulations that carry penalties if specific consumer privacy rights are not observed. Industry data privacy standards, such as the Payment Card Industry Data Security Standard ("PCI DSS"), also need to be considered. These standards can carry litigation risk if data privacy is violated and your organization claims to be PCI DSS compliant. These regulations and standards are constantly evolving, so you should stay abreast of the current regulations and standards if your role involves these issues.

Regulating privacy

Consider applicable privacy regulations and industry standards when responding to a data request, such as:

- *US federal regulations:* Dodd-Frank, Health Insurance Portability and Accountability Act ("HIPAA"), and Consumer Credit Protection Act
- *US state regulations:* Massachusetts Data Protection Act
- *EU data protection:* EU Data Protection Directive (Directive 95/46/ EC) currently in place with a draft General Protection Regulation under consideration
- *Canadian regulations:* Personal Information Protection and Electronic Documents Act ("PIPEDA")
- *Industry standards:* Payment Card Industry Data Security Standards ("PCI DSS")

Privacy reviews

Identifying and collecting requested data is an important issue, but it is becoming increasingly challenging for counsel to ensure that only proper data are sent as part of the response. Properly identifying and fully collecting requested data can be a challenge — especially if an organization is performing this process alone, without prior experience and without a predefined process. This

challenge will remain and will most likely only increase along with the increasing levels of data storage complexity and data volumes.

The counsel's role in ensuring privilege will also continue to be critical. The heightened focus on data privacy adds a new layer to the review process. Now, counsel must understand and apply the relevant privacy regulations and standards to the review process and ensure that providing such information to a third party is allowed. New and updated jurisdictional privacy regulations require counsel to 1) understand what types of data are in the production set, 2) identify regulations and standards that apply to the production set data, and 3) determine what protections are in place with the third party to safeguard the organization from data privacy risks and exposure.

After the collection has been performed, the first step for counsel to consider is what types of information are contained in the data. Standard methods, such as identifying key custodians and keyword searches, are important for quickly identifying large swaths of specific types of information. If database information is part of the potential production, a review of the database's structure, fields and a set of sample records is vital for knowing the types of information in the system. In addition, database information can be aggregated on key fields to identify jurisdictions (e.g., customer locations) and the types of transactions. Additional methods can be augmented by the use of automated PII discovery tools.

Performing keyword searches is an important part of the initial review. Identifying specific keywords in field names or datasets can save time and reduce risk. Depending on the applicable definition of PII, the searches can be limited to the components of PII. For example, one of the major forms of PII is the social security number or tax ID. Keyword searches for terms such as "SSN," "Social Security Number," "Tax ID," and other variations can more quickly pinpoint the presence or absence of PII. A review of sample data is also required because of possible spelling variations, abbreviations and other terminology to denote this type of information.

Structured and unstructured data require different types of review. Structured data, such as database records, are typically transactional data with field headers that indicate the type of information in each column. The two primary techniques for analyzing structured data for PII are to review the field names and examine sample records. Unless data is improperly labeled or stored, these methods are generally sufficient for identifying the PII — even if the production contains billions of records.

Unstructured data, on the other hand, are files like emails and documents whose contents are not organized into fields. Running keyword searches is one of the primary methods for reviewing these for PII; however, contextual PII may be included. This process can be augmented by reviewing the source of this information. For example, customer feedback or claims emails are typically received through specific channels, such as a Web portal or sent to a specific email address. Reviewing the data sources for unstructured data is useful for identifying possible locations of PII.

Proactive methods or existing documentation can simplify and expedite the privacy review. Large organizations and organizations in certain types of industries regularly receive data requests. You can prepare for data requests by working with other business units within your organization to document the locations of data stores, types of information contained in each, whether PII is stored in the data, business owners of the data and retention schedules. Compliance with the organization's own document retention and destruction policies will reduce the scope of producible documents. If you receive frequent data requests and are subject to litigation holds, clearly documenting holds and the periods of each type of data can simplify the process of data identification. Offline media and cloud data storage may also be in the scope, so having documentation about those data sources can

help reduce effort and complexity in responding to a data request. Proactive organizations maintain documentation of their organizational data stores and the previous data productions in a centralized location maintained by the legal department and other members of the data privacy team (e.g., audit functions and IT system owners).

Pre-production review challenges

Counsel's role in reviewing requested data before production is changing due to the increases in data volumes and data privacy considerations.

- *Data volume:* Organizations are storing much more data across a number of systems. The volumes of emails and document files stored by organizations — the realm of traditional eDiscovery — are continuously increasing in size. The volumes and types of information stored in databases and other large-scale data repositories are also increasing. The increase in volumes and types of data makes the review process more time-consuming and complex.
- *Multijurisdictional privacy considerations:* New levels of data privacy regulations require a multifaceted review process. Each jurisdiction can have its own definition of PII, and different regulations about what constitutes private information complicate the review process.
- *Various industry-based privacy standards:* Several industries have their own privacy standards that can subject an organization to fines or litigation risk exposure.

Considerations when performing an initial review

- *Start with PII:* Identify all locations of PII using the broadest possible definition. Do not exclude fields that loosely define PII (e.g., customer sales locations) at this stage. Only eliminate PII fields when you know which fields are applicable.
- *Consider practical factors:* How much time do you have, and how burdensome is the request? Large data requests can involve hundreds or thousands of data locations, so you need to keep practical limitations in mind. If the request is potentially overly burdensome, note the factors and raise those issues as soon as possible to the requesting party or court.
- *Track your work:* Keep a running log of people interviewed, data sources and type(s) of PII. Data requests are common. Creating documentation of your process can save time and effort in future requests

Techniques for managing privacy

If data containing PII has to be provided, the PII can be managed in several ways to avoid releasing private information. The most common method for managing private information — outside of not providing it — is to mask the PII. Masking PII involves replacing or redacting the private information but retaining the original data's structure. PII replacement entails modifying the data to substitute each PII value with a specific replacement value. For example, if database information contains a customer name PII field, each customer name can be replaced with a numeric value. All instances of a customer name value of "John Smith" can be replaced with the numeric value of "1," "Jane

Smith” can be replaced with “2,” and so on. The responding party should maintain a copy of the unmodified version and an index that contains the names and corresponding replacement values should any questions arise. Another form of masking is to redact the PII. In the previous example, rather than replace the customer name values with sequential numeric values, the field could be made blank or blacked out (manually or electronically). This is an effective method if the customer’s name is not material but the original data structure is required, such as if the requesting party needs to see the original database’s structure and confirm that there was, in fact, a customer name field.

Other techniques should be applied if PII does need to be produced. PII must be protected from falling into the hands of an unauthorized third party. Unauthorized access can occur in a number of ways. Drives can be lost, so if a data production is being delivered by postal service, you should maintain a backup copy and encrypt the drive with the decryption key provided in a separate delivery. This will protect the data should the drive be lost in transit. If the data is being delivered electronically, use a secure protocol (e.g., SFTP) with strong user-access protections and nontrivial passwords. Electronic files should be encrypted and the encryption key provided separately to add an extra layer of protection.

All PII that leaves the organization can be tracked to create an audit trail and document that outside organizations have received PII and the details about which PII they were provided. The PII log can either contain the PII values that were provided or provide aggregate-level details with information about how to identify the individuals if questions about the PII arise later. If PII is lost or a privacy claim is made by your customers or regulators, you should be prepared to answer questions about what was provided, the justification for why it was provided, and steps you and the requesting party took to protect your customers’ privacy.

Conclusion

Data requests are an increasingly common part of a general counsel’s job, and data privacy regulations and standards add another layer of responsibility that you must account for before producing data. The amount of data generated and stored in virtually every organization is growing at a rapid rate, resulting in larger volumes of data that might be part of data productions and may contain PII. Both US-based and global organizations are faced with everchanging data privacy regulations and standards that require your awareness and adherence as part of responding to data requests. Data privacy will continue to be an important issue for individuals and government agencies, and regulations and standards will continue to be updated with the constant change in technologies. Practical steps can be taken to ensure that you do not run afoul of data privacy regulations. Starting from the initial steps, data privacy concerns can be raised to the requesting party. The review process offers you opportunities to locate all PII and take steps to safeguard the privacy of your customers’ information.

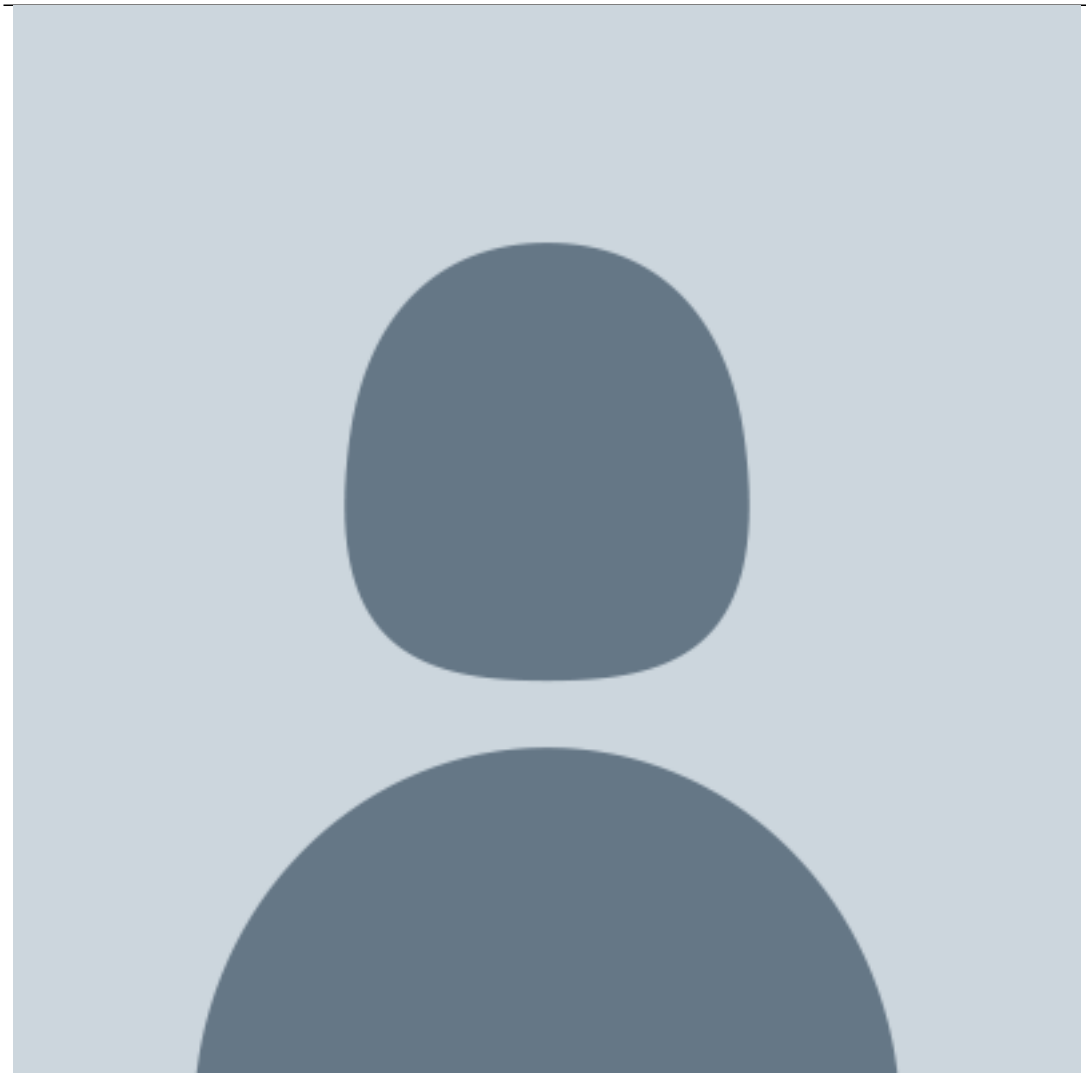
Best practices

In June 2015, ACC updated its Leading Practices Profiles series by publishing “Leading Practices in Privacy and Data Protection: What Companies Are Doing.” This resource examined the data security and privacy practices of six companies with operations spanning the globe. The article provides practical information on the types of privacy and data security practices corporate counsel should consider implementing. These practices include internal and external privacy practices and compliance and risk mitigation efforts on an international spectrum. The participants in the Profile described their incident response programs for privacy and data breaches; the personnel structure for

privacy and data security; vendor-facing programs; concerns arising from cloud environments; and leading practices. Participants in the Profile articulated what they considered to be their leading or best practices:

- Have a clear mission statement in light of the ethical
- framework and values of the organization.
- Train on privacy and data security at all levels of the organization.
- Obtain support throughout the organization, including management and employees.
- Manage vendors.
- Cloud control.
- Develop rules for BYOD use.
- Follow the strictest jurisdiction’s rules when operating across jurisdictional lines.
- Base data security compliance programs on established privacy directives. Participants built their privacy programs and policies around the principles set forth in the EU Data Protection Directive or other high-level privacy directives.
- Keep consumer trust by taking a permissions-based approach.
- Develop a formal incident response program for breaches or leaks.
- Focus on developing a comprehensive privacy policy that is also readable and understandable by everyone.
- Establish a detailed internal system of processes and procedures for employees to handle privacy/data security matters.

Laura Dorman

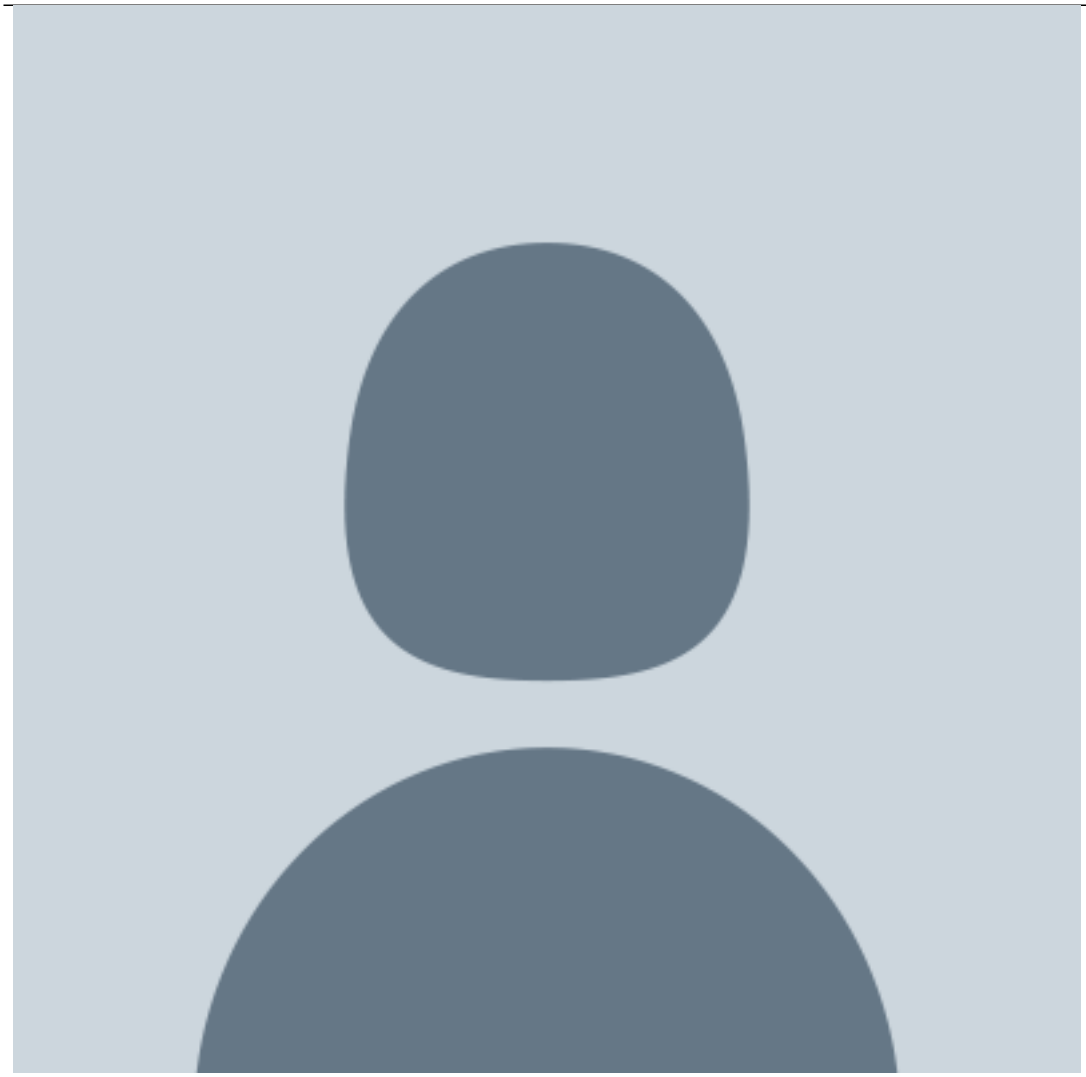


Managing Director and Associate General Counsel

Berkeley Research Group

Berkeley Research Group is a global consulting firm specializing in economics, finance, statistics, public policy and business strategy.

Joe Sremack



Berkeley Research Group

Joe Sremack is a director in Berkeley Research Group’s technology services practice in Washington, DC, where he provides advisory and expert services related to information governance, e-discovery and complex data analytics.