GREENSFELDER

Between a Rock and a Hard Place

Balancing Privacy Interests and e-Discovery Obligations in Litigation

Julia Voss & Lauren Daming

Greensfelder, Hemker & Gale, P.C.

June 2022

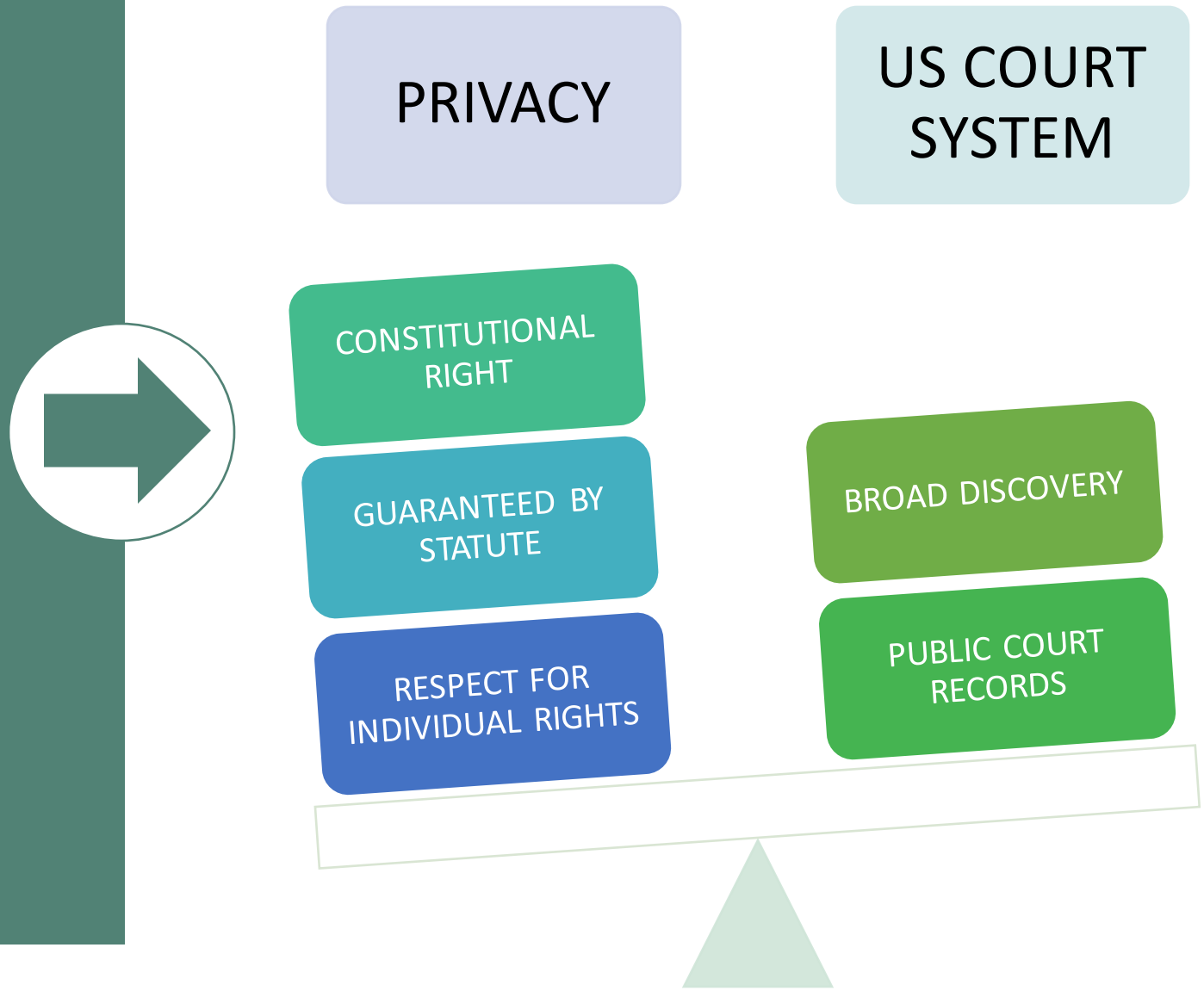
How do you address privacy concerns in discovery?

- How do you determine what information is sensitive data?
- What should you redact when producing to opposing counsel?
- What should you redact from court filings?
- How do you know when to file a document under seal?

Presentation Topics

- Conflict between privacy and discovery
- Data sources that implicate privacy concerns
- Categories of sensitive information
- Consequences of not protecting sensitive information
- Tools for addressing privacy concerns
- Suggested production framework

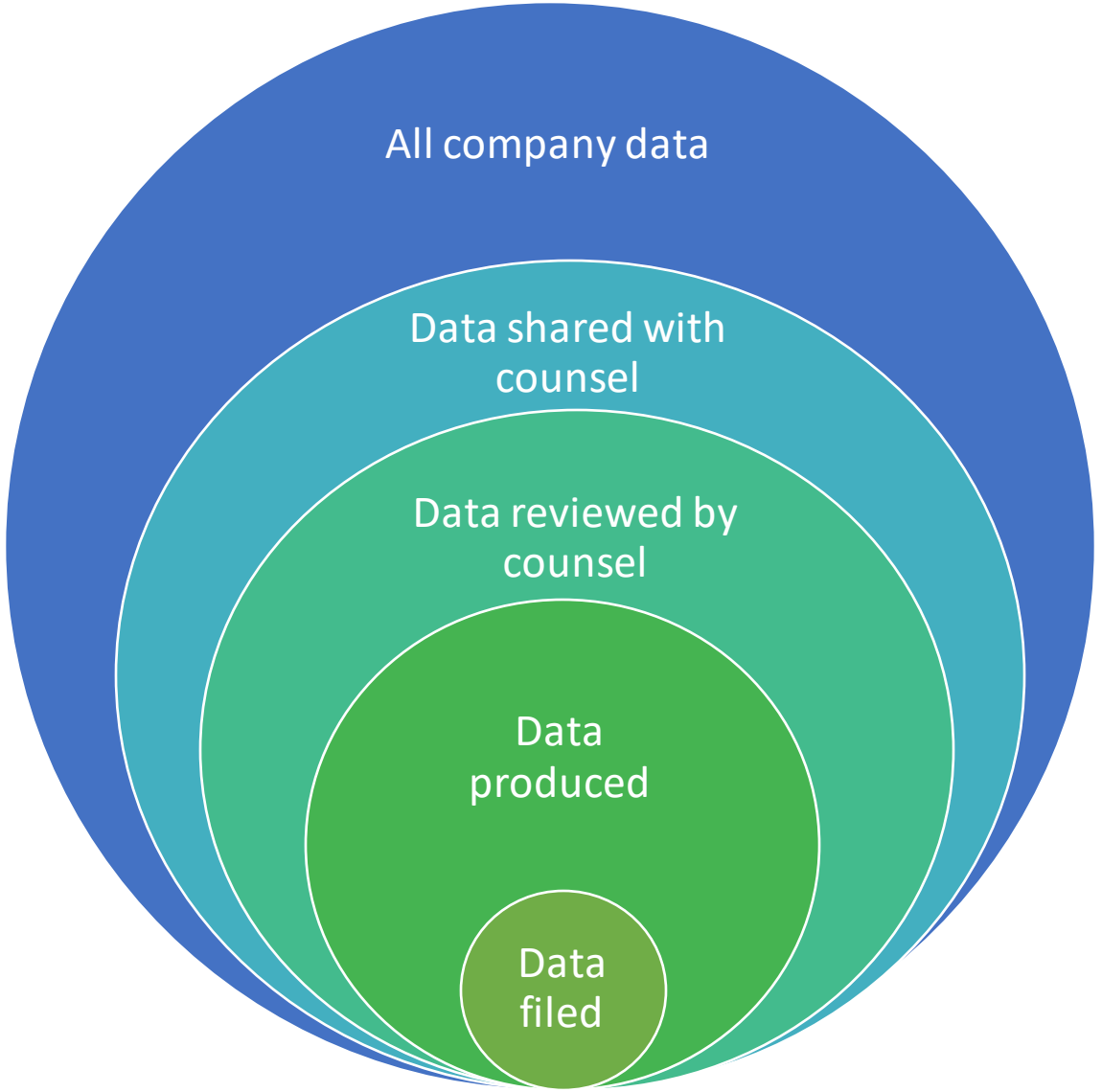
Conflicting Interests



Sources of Private Information in Litigation

- Personal devices
- Social Media
- Email
- Wearables
- Company Document Repositories
- Chat applications

Scope of Data in Litigation



Do we really need to redact everything we produce, or is a protective order good enough?

What information should be protected?

Sensitive Data

Rules/Regulations

- Federal Rule Civil Procedure 5.2
- Federal Rule Civil Procedure 26(c)
- Comprehensive data protection laws:
  - GDPR, CCPA/CPRA
  - CO, VA, CT, UT
- Sectoral guidelines
  - HIPAA, GLBA
  - Bankruptcy
- Contract provisions
  - Nondisclosure agreements
  - Notice requirements

Sensitive Data

Categories of Data to be Protected

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Nonpublic Personal Information (NPI)
- Confidential Data
- Trade Secrets

Sensitive Data

Categories of Data to be Protected

- Non-responsive information
- Information subject to non-disclosure obligation
- Embarrassing information

What happens if you…

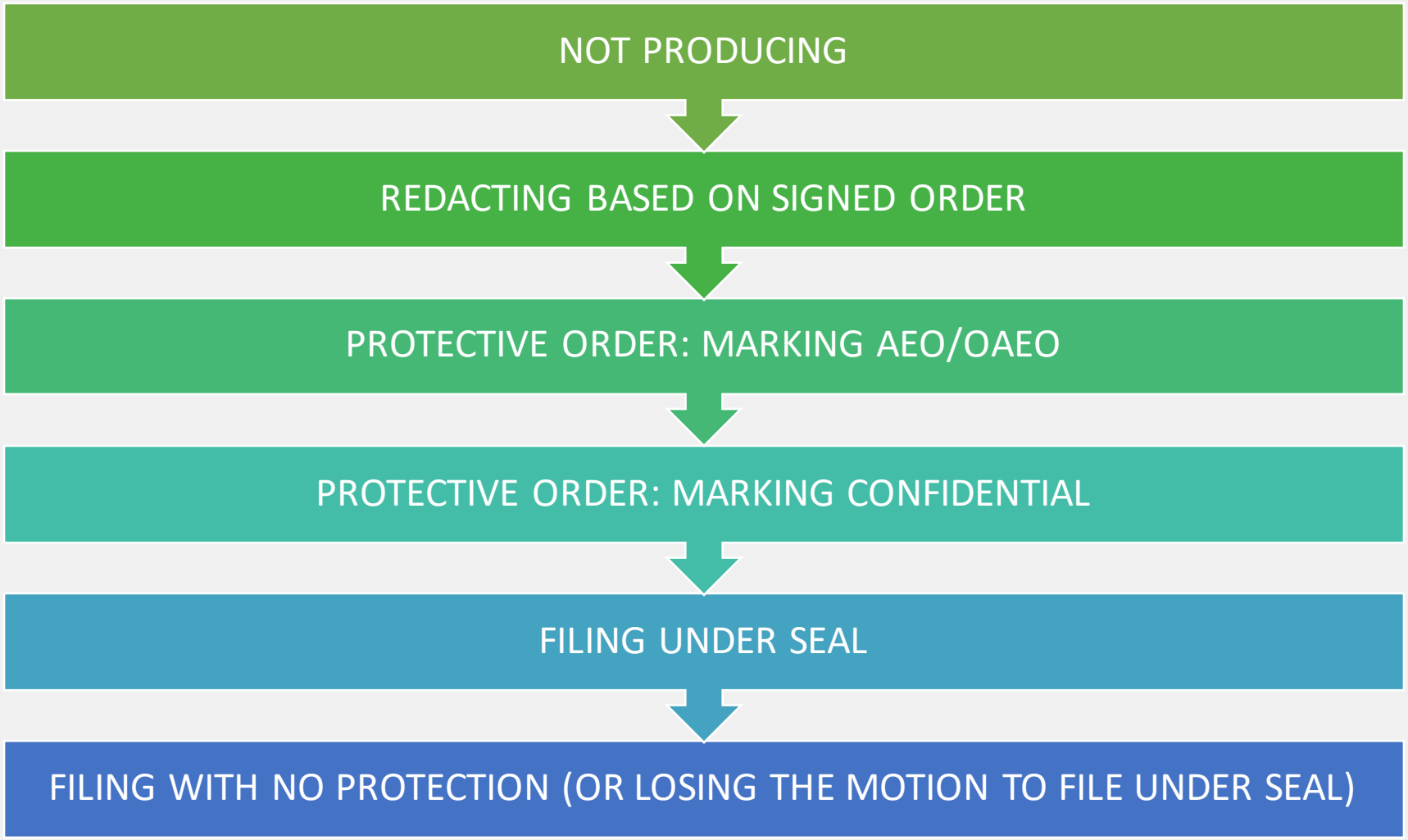
- File a document without redacting sensitive data?
- Redact incorrectly?
- Neglect to file a document under seal?

Consequences

- Admonishment from the court
- Waiver of protection for sensitive data
- Refile documents in redacted form
- Court strikes the document from the record
- Filing party sanctioned
- Pay other party’s costs
- Claims from third parties

How do you protect sensitive data?

Continuum of Protection



Tools of Protection

- In house knowledge
- Negotiate Scope with Opposing Counsel
- Discovery Plan Orders/Protocols
- Redaction
- Protective Orders
- Filing under seal

Protective Tools

In House Knowledge

- Outside Counsel Guidelines (or a white paper)
  - Define and describe company's sensitive data
  - Identify geographical scope of data
  - Specify procedures for protecting sensitive data and consequences

Protective Tools

Security and privacy representations or requirements

- Sample Language
  - "As Client's outside counsel, you may have access to Client's non-public, proprietary, confidential information. Your firm must have in place appropriate procedures for the protection of such confidential information, which including training staff on protection procedures and monitoring the implementation of such protection procedures."
  - "Counsel shall implement and maintain appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of NPI that is provided or obtained respective to the case."

Protective Tools

Define "confidential information"

- Sample Language
  - "Potentially sensitive information includes, but is not limited to, non-public financial data, sales or pricing data and agreements, vendor agreements, contracts, personnel files, employee information, product information, plan information, internal communications, etc."
  - "The Company considers the following information to be highly confidential: internal policy directives, manuals, organizational charts, forms, customer and employee information and other non-public materials, thought processes and work product relevant to the Company's business."

Protective Tools

Describe preferred process for protecting information

- Sample Language
  - "Outside counsel must work with Client Attorney to prepare and seek to obtain court approval of an appropriate protective or confidentiality order before producing potentially sensitive information in discovery or otherwise."

Protective Tools

Negotiate with Opposing Counsel

- Rule 26 conference topics
  - Preservation of discoverable information
  - Proposed discovery plan
- Rule 16 conference topics
  - Extent of discovery
  - Disclosure, discovery, or preservation of ESI
  - Agreements between parties for asserting claims of protection

Protective Tools

Discovery Plan/Order

- Get any agreements limiting scope of preservation/production into the Discovery Plan, PO, or ESI Order signed by the judge

Protective Tools

Protective Orders

- Protective Orders can limit who sees documents that are produced
  - AEO/OAEO
  - Confidential
- Include categories that may be redacted
- Include procedures for challenging designations/redactions
- Be aware: Court may not allow them or may limit beyond what parties agree to

Protective Tools

Redaction

- Very few regulations specifically discuss redactions
  - HIPAA = produce without redactions if a Qualified Protective Order
  - FRCP = redact limited sensitive data before filing
  - FINRA = redact before filing with FINRA but specifically states the rules on redaction do not apply to exchanges between parties (although encourages agreements on redactions)
- Proportionality Considerations
  - Volume, burden, evidentiary value
- Methods
  - Manual, search terms, assistive technology + QC, RegEx
  - Native format redaction

Protective Tools

Filing Under Seal

- Rule 5.2 categories do not need a motion to file under seal
- Can be cumbersome, especially in MDL
- Judges may not grant the motion
  - Standard: good cause v. compelling reason

Minimizing Data Transfer Risks

- Limited collection of data/limited access
- Quality control measures
- Data transfer protections (encryption, FTP, etc.)
- Give notice/authorizations for release (law, NDA, etc.)
- E-discovery vendor due diligence and contract provisions

Suggested Framework

Disclaimer: the following generalities must be evaluated for your matter's specific circumstances. There is no one size fits all answer when it comes to weighing the risks of producing private information.

Framework

Small Case

- Redact everything. If the time to redact is not that great, take the safest course.

Framework

Larger/Complicated Cases

- Redact anything that can be automated or easily defined for reviewers
- Isolate sensitive data that you consider higher risk and manually redact
- Designate lower risk documents containing sensitive data as confidential or AEO and produce without redacting
- If opposing party wants to file a designated doc, must either:
  - Give producing party notice prior to filing and allow time to redact, or
  - File as a slip sheet and allow producing party to replace it with a redacted version

Framework

Common Examples of Private Data	Considerations even if you have a HIPAA QPO
Social Security Numbers/Tax ID numbers/DL numbers, Passport numbers, etc.	The damage to reputation for releasing SSN is high.
Credit Card Numbers	The damage to reputation for releasing a CCN is high.
Trade Secrets	They can't be unseen and are the lifeblood of the business. They are worth fighting about in court if there are objections.
Financial Account Numbers	Business accounts are given out to more people in the normal course of business, so may not be as concerned with business accounts.
Biometric Identifiers	These cannot be changed, so should be protected.
Very Personal Pictures	The people in the pictures are often not involved in the litigation. Let them stay that way.
Minor's Names	Always redact when filing, but it's difficult to do effectively during production.
Customer Lists	In many cases, these are considered trade secrets.
Health Information	Consider redacting anyway if highly personal, not relevant in a business dispute, and there is not a lot of it so it does not substantially add to the cost of review to redact it.
Passwords or Security Questions	You will need to provide passwords for relevant password protected documents.
Confidential Business Plans	Most business data is outdated by the time it's been collected for litigation. It's very difficult for reviewers to draw the line on just general business talk and confidential business strategy.
Sexual Orientation/Religion/Political Beliefs/Race or ethnicity/trade union membership	Consider the source and the jurisdiction. These are GDPR protections.
HR/Resumes/Salaries	Court more likely to think PO will protect this, But consider jurisdiction.
Date of Birth	Lower priority - can be found online in most cases.
Address	Lower priority - can be found online in most cases.
Phone Numbers/email address	Lower priority - can be found online in most cases.

* These considerations are generalities. The circumstances of any given matter must be evaluated for that matter to determine the level of risk for various types of data.

TAKEAWAYS

- **Know the scope of data in your company**
- **Know the scope of data in the case**
- **Address privacy issues early with opposing counsel and the court**
- **Customize data tools to case**

Questions?

GETTING IN TOUCH

Julia Voss
314.345.4745
jms@greensfelder.com

Lauren Daming
314.345.4768
ldaming@greensfelder.com