AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

Cyber-U

By Elizabeth B. Vandesteeg and Christopher Updike

Public Filings with Private Data?

A Look at Bankruptcy's Conflict with Data-Privacy Laws

Coordinating Editor Elizabeth B. Vandesteeg
Levenfeld Pearlstein, LLC; Chicago

Christopher Updike
Stretto, Inc.
New York

Lisa Vandesteeg is a partner in the Financial Services and Restructuring Group at Levenfeld Pearlstein, LLC in Chicago. She is also a member of ABI's Board of Directors and a 2017 ABI "40 Under 40" honoree. Chris Updike is general counsel for Stretto, Inc. in New York.

In an era when data-privacy laws are rapidly evolving to protect individuals' personal information, the inherently public nature of bankruptcy proceedings presents a clear conflict. By design, bankruptcy cases require transparency, disclosing financial details, creditor lists and service information on publicly accessible dockets. Contrast this with such burgeoning data-protection frameworks as the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) (as well as numerous other state data-privacy laws), which emphasize shielding personal data and allowing individuals to control its use and disclosure.

Since 2018, when some of the first comprehensive data-privacy laws were enacted, bankruptcy rules and regulations have changed very little to address the growing dissonance. Until Congress and the U.S. Supreme Court implement measures to broadly harmonize bankruptcy law with data-privacy laws (which could be a while), courts and their clerks will need to create a patchwork of local rules and general orders to bridge the gap.

Bankruptcy's Transparency by Default Regime

As the saying goes, bankruptcy is a fishbowl. There is a strong presumption and policy in favor of public access to court records. The "right of public access is 'rooted in the public's First Amendment right to know about the administration of justice.'"[1] In fact, "[t]he public interest in openness of court proceedings is at its zenith when issues concerning the integrity and transparency of bankruptcy court proceedings are involved."[2] Section 107(a) of the Bankruptcy Code codifies this general right to inspect and copy judicial records.

Under the Code, there are limited exceptions to this default disclosure rule. For example, § 107(c) protects an individual with respect to the "means of identification," disclosure of which would create "undue risk of identity theft or other unlawful injury," but only "for cause" shown.[3] The burden to prove the need or justification for redaction is on the party seeking it, and the burden is steep. The movant must show that there is a "sufficient basis to overcome the presumption of ready access to legal records and public policy in favor of public access to court records."[4] Even when redaction is authorized, courts generally employ the least restrictive means to do so.[5]

Conflict Between Bankruptcy and Data-Privacy Laws

Bankruptcy's default public-filing regime directly conflicts with evolving state and international data-protection frameworks. The global data-privacy landscape remains highly fragmented, with the GDPR continuing to set the benchmark for comprehensive data-protection standards. In the U.S., effective Jan. 1, 2020, the CCPA and its subsequent amendments established the first broad-based state-privacy regime. Numerous additional individual states have since followed California's example, and to date,

1 *In re Endo Int'l plc*, No. 22-22549 (JLG), 2022 WL 16640880, at *7 (Bankr. S.D.N.Y. Nov. 2, 2022) (citing *Video Software Dealers Ass'n v. Orion Pictures Corp. (In re Orion Pictures Corp.)*, 21 F.3d 24, 26 (2d Cir. 1994)).

2 *In re Celsius Network LLC*, 644 B.R. 276, 288 (Bankr. S.D.N.Y Sept. 28, 2022) (citing *In re Food Mgmt. Grp.*, 359 B.R. 543, 553 (Bankr. S.D.N.Y. 2007)).

3 11 U.S.C. § 107(c)(1).

4 *In re Endo Int'l plc*, 2022 WL 16640880, at *8; *see also In re Celsius*, 644 B.R. at 292 (requiring movants to overcome "strong public policy of transparency and public disclosure in bankruptcy cases" with "strong evidentiary showings").

5 *In re Purdue Pharma LP*, 632 B.R. 34, 38 (Bankr. S.D.N.Y. 2021).

19 states have enacted comprehensive consumer-privacy laws, with several more scheduled to take effect through 2026, thus creating a complex compliance environment for businesses operating across jurisdictions.[6] These state laws, while sharing some common elements with each other and the GDPR, vary significantly in scope, exemptions and enforcement. While a detailed summary of those various laws is beyond the scope of this article, at a high level they require organizations to implement transparency measures, limit data use to specified purposes, and provide individuals with such rights as access, deletion and correction of their personal information.[7]

As a result, debtors are increasingly filing motions to redact broader personal information from public filings, citing their obligations under these privacy laws.[8] Debtors subject to the GDPR have argued that public disclosure of even basic contact information for creditors could run afoul of that statute's data-minimization standards and its requirement for an appropriate lawful basis to process personal information under EU law.[9] While judges squarely presented with this argument have been loath to concede the general applicability of the GDPR in a U.S. bankruptcy proceeding,[10] a number of bankruptcy courts have nonetheless found authority to redact such basic personal information as physical addresses and email addresses, which are routinely publicly disclosed in most bankruptcy cases.[11]

Data-protection concerns are heightened in bankruptcy. Complex corporate restructurings can involve thousands — sometimes millions — of employees, customers, equity-holders and other individuals, thus consolidating an incredible amount of personally identifiable information (PII). Bankruptcy cases become prime targets for cyber criminals deploying increasingly sophisticated technological capabilities to access and abscond with sensitive data. Even when redaction is permitted by the court, security incidents and data breaches have happened and will continue to happen. The question becomes what to do then.

There is no overarching, universal federal law governing to whom, how and when notification of a data-security incident impacting PII should be provided. Instead, all 50 U.S. states and the EU have enacted their own notification statutes requiring organizations to inform affected individuals (and sometimes state agencies or consumer-reporting agencies) about security breaches involving PII.[12] The specific requirements vary by state, including what type of information triggers a notification obligation, the definition of "breach," the timing of notification and the notice's content.[13] When notification is required, these statutes generally place the burden of notification to impacted individuals on the party that suffered the data breach, but might also require that any third party that could maintain or store — but not own or license — the impacted data must provide notice to and/or cooperate with its applicable owner or licensor.[14] In the context of comprehensive data-privacy laws, the parties that handle the data on behalf of a data controller — known as service providers or data processors — are often contractually[15] or statutorily[16] required to first promptly inform the controller, who then makes the decision regarding notification.

While each law has its own definitions, data-breach statutes generally regulate a narrower subset of PII, such as first and last name *in combination with* at least one "more sensitive" data element such as Social Security number, driver's license, medical history, health insurance information, or biometric information or genetic information.[17] This type of sensitive information would not typically be included in a debtor's schedules or on a claims register (although it can find its way there through careless filings). On the other hand, this information (name, address, claim amount, etc.), which is typically publicly filed and available, would not be of the nature that would implicate or trigger notification obligations under state notification laws.

Notably, under many state data-breach laws, the definition of PII expressly excludes publicly available information that is lawfully made available to the general public from federal, state or local government records (or widely distributed media).[18] Thus, unauthorized access to information that is otherwise available on a public bankruptcy docket would not trigger notification obligations. Even if PII was involved, under certain of these laws, notification often might not be required if, after an appropriate investigation, the entity rea-

---

6 *See, e.g.*, Cal. Civ. Code §§ 1798.100 through 1798.199.100; Colo. Rev. Stat. Ann. § 6-1-1301 through 6-1-1303; Va. Code Ann. § 59.1-575 through 59.1-584; Conn. Gen. Stat. §§ 42-515 through 42-525; Utah Code Ann. §§ 13-61-101 through 13-61-404.

7 *Id.*

8 *See, e.g., In re Celsius*, 644 B.R. at 295 (debtors sought authorization to redact names, email addresses and home addresses of citizens of the U.K. and European Economic Area as required by GDPR); *In re Endo Int'l plc*, 2022 WL 16640880 at *6 (same).

9 *See, e.g., In re Endo Int'l plc*, 2022 WL 16640880 at *6 (debtors argued that public filing of individual litigants' names, addresses and email addresses would violate GDPR). Rather than engage with the question of applicability of the GDPR to a U.S. bankruptcy case, the bankruptcy court instead ordered the redaction of the requested information under § 107(c).

10 *See In re Celsius*, 644 B.R. at 295; *In re Endo Int'l plc*, 2022 WL 16640880 at *12.

11 *See, e.g., In re Celsius*, 644 B.R. at 293-94 (court granted motion to redact home and email addresses of certain parties to protect them from "identity theft, blackmail, harassment, doxing, and stalking" threats); *In re Endo Int'l plc*, 2022 WL 16640880 at *12 (authorizing redaction of names, home addresses and email addresses of certain claimants under § 107(c) as necessarily associating claimants with "unfavorable medical condition" and to protect against identity theft risks); *In re Genesis Glob. Holdco LLC*, 652 B.R. 618, 637-643 (Bankr. S.D.N.Y. Aug. 4, 2023) (authorizing redaction of individual names, mailing addresses and email addresses under§ 107(c) due to heightened risk of identity theft); *In re 2U Inc. et al.*, No. 24-11279-mew, [Doc. 40] (Bankr. S.D.N.Y July 30, 2024) (authorizing redaction of names, home and email addresses, and "any other [PII]" from publicly filed creditor matrix).

12 *See, e.g.*, Ala. Code § 8-38-6 (requiring notification to individuals and attorney general for breaches affecting 1,000 or more residents); 6 Del. C. § 12B-102(d) (requiring notification to individuals and attorney general for breaches affecting 500 or more residents); Ind. Code §§ 24-4.9-3-1(c) and 24-4.9-3-3 (requiring notification to individuals and attorney general for all breaches).

13 *Id.*; *see also, e.g.*, Ala Code § 8-36-2(6); O.C.G.A. § 10-1-911(6); Idaho Code § 28-51-104(5); Md. Code Ann., Com. Law § 14-3501(e).

14 *See, e.g.*, Ala. Code § 8-38-6 ("covered entities" that are not "third-party agent[s]" must provide required notices); Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(A) (notices are required for all "person[s] who own ... license ... or maintain ... computerized data"); Neb. Rev. St. § 87-803(1) (commercial entities that "own ... or license ... computerized data" are required to provide notices); *see also* Ala. Code § 8-38-8 (third-party agent experiencing breach must notify "covered entity"); Conn. Gen. Stat. Ann. § 36a-701b(c) ("Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery."); Neb. Rev. St. § 87-803(3) (individual or commercial entity "that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach").

15 For example, the clerk of Court for the U.S. Bankruptcy Court for the District of Delaware has promulgated a service-level agreement (SLA) that claims and noticing agents must execute to qualify to provide services in that venue, which contains certain notification requirements to be given to the clerk of court.

16 Article 33(2) of the GDPR requires data-processors to "promptly" notify a data controller of a data breach.

17 *See, e.g.*, Conn. Gen. Stat. Ann. § 36a-701b(a) (setting forth multiple specific data elements for definition of "personal information" that would trigger notification requirements); Cal. Civ. Code § 1798.82(h), (i) (same); Fla. Stat. § 501.171(1)(g) (same).

18 *See, e.g.*, Ala. Code § 8-38-2(6) (personal information excludes information that was "lawfully made available to the general public from either federal, state, or local government records or widely distributed media"); Idaho Code § 28-51-104(5) (same); 815 Ill. Comp. Stat. 530/5 (personal information does not include "publicly available information that is lawfully made available to the general public in federal, state, or local government records").

sonably determines that the breach will not likely result in harm to the individuals.

A complicated new wrinkle then arises in the wake of any increasing use of redaction and sealing orders: In the event of a data-security incident or data breach involving such information as names and addresses, which would not otherwise trigger any state law notification obligations, but in which a sealing or redaction order has hidden that information from the public eye in the bankruptcy forum, when is notification of the incident required, and to whom? There does not appear to be any written answer to this tricky question in the existing rules, standing orders or guidelines.[19] Thus, with the exception of potentially applicable state breach notification laws, parties grappling with a data-security incident have nothing more than their own best judgment (and potentially advice of counsel advising them on incident response) to follow to determine what notification should be provided to whom and when.

Proposed Solutions

To reduce the risk of PII misappropriation or misuse from publicly filed documents, courts could implement local rules or general orders that require redaction by default for filings that typically include more sensitive information, such as certificates of service and creditor matrices, and instead require interested parties to seek unreacted copies only as necessary or upon entry of a court order. While at least providing clearer guidance in their respective jurisdictions, bespoke approaches at the local level will no doubt lead to inconsistencies across the numerous judicial districts and circuit courts of the bankruptcy world.

A better solution would be to implement a consistent, universal and nationwide framework to address notification requirements related to data breaches arising in the context of bankruptcy cases. At a minimum, such a notification framework should include the following: (1) definitions of what data would be covered and what would constitute a "breach" triggering notification; (2) clarity as to who may constitute mandatory or discretionary notice parties; and (3) clarity as to the timing and content of notifications to be provided to mandatory notice parties.[20]

Conclusion

The clash between bankruptcy's "fishbowl" transparency and modern privacy rights is intensifying. Courts and practitioners must grapple with thorny questions about individual data rights, redaction duties and privacy liability in an area of law designed for openness — not privacy. The time is ripe for meaningful discussion by various participants in bankruptcy proceedings — clerks of court, judges, U.S. Trustees, legal and financial professionals, and claims and noticing agents, to name a few — to develop and implement some uniform, clear and practicable guidance to holders of personal information in bankruptcy cases. Until Congress or the Supreme Court squarely addresses these issues, the burden will fall on these parties to navigate this complex and evolving intersection. abi

Reprinted with permission from the ABI Journal, Vol. XLIV, No. 11, November 2025.

19 The SLA issued by the clerk for the Delaware Bankruptcy Court is a limited exception to this general rule, as the SLA contains certain notification requirements applicable to claims and noticing agents. However, this service-level agreement does not apply to any other stakeholders, such as counsel or financial advisors, who might be compromised with respect to the data that they are entrusted with as estate professionals.

20 The authors are members of a working group composed of certain claims and noticing agents and clerks of bankruptcy courts who are discussing and drafting a proposed universal framework of rules and guidelines around reporting and notification requirements in the event of a data security incident involving PII in the context of a bankruptcy proceeding.