

BY ANDREW PERRY

Filling the Privacy Gap: How State Law Applies to Claims Data

The Bankruptcy Code and Federal Rules of Bankruptcy Procedure place a duty on parties filing information on the public docket to protect the personal identifiers of individuals from public disclosure. Filing parties primarily accomplish this duty by redacting personally identifiable information (PII), such as Social Security numbers, birth dates, full financial account numbers and the names of minors before making a public filing. Alternatively, parties may opt to file a sensitive pleading under seal, then seek bankruptcy court approval for the pleading to remain under seal.

Aside from the obligation to redact personal information, the Code and Rules are otherwise silent as to a debtor's protection of personal identifiers maintained as part of the bankruptcy case. Silence is problematic when a large-scale bankruptcy case requires the collection of voluminous amounts of individual data in the claims-resolution process. Because the volume of data and noticing requirements are often beyond the capabilities of bankruptcy courts, debtors often turn to third-party professionals to perform these duties.

However, solutions such as this are not without risk of running afoul of other data-privacy laws. Based on the lack of preemptory federal data-protection laws, several states have enacted data-privacy laws that impact the collection and use of data by private companies. California arguably boasts the most restrictive protections of personal data, although other states have implemented privacy requirements of their own, requiring navigation of a web of data-privacy statutes.

Data Protection Under the Bankruptcy Code and Rules

Section 107 of the Bankruptcy Code generally provides for public access to papers filed with the bankruptcy courts, but expressly authorizes the court to protect access to (1) a trade secret or confidential research, development or commercial information; or (2) a scandalous or defamatory matter involving a person.¹ In addition to these matters, a bankruptcy court may also protect personal information that might subject an individual

to identity theft or unlawful injury, such as personal identifiers.²

Complementing § 107, Bankruptcy Rule 9037 states that unless the court orders otherwise, any filing may only include the last four digits of a Social Security number, the year of a person's birth, a minor's initials and the last four digits of a financial account number.³ It also provides a procedure for filing documents under seal to protect information with leave of the bankruptcy court.

Section 363(b) addresses the sale of estate property that includes the PII of individuals and whether such information may be sold through the bankruptcy case. Generally, if a privacy policy is in place, a debtor may not sell PII unless the sale is consistent with the terms of a privacy policy or, after appointing a consumer privacy ombudsman, the bankruptcy court finds that the sale would not violate applicable nonbankruptcy law.⁴

Nonbankruptcy and State Framework on Data-Collection Nonbankruptcy Law

Federal laws pertaining to data-collection are derived from a patchwork of statutes and regulations that target certain industries and types of harm. For example, the Federal Trade Commission is tasked with enforcing the prohibition on unfair and deceptive trade practices, which often includes the collection and use of data in a manner inconsistent with a company's stated privacy policy or in violation of federal statute.

Specific statutes regulating the collection and use of personal data include the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Health Insurance Portability and Accountability Act and the Family Educational Rights and Privacy Act, which regulate the use and disclosure of personal health information and educational records, respectively. Other legislation that tangentially applies to data-collection includes the Gramm-Leach-Bliley Act (applying to financial institutions), the Children's Online Privacy Protection Act (applying to handling of minors' data) and the Bank Secrecy Act (requiring financial institutions to keep certain customer and transactional data).



Andrew Perry
Foran Glennon
Palandech Ponzi
& Rudloff PC; Denver

Andrew Perry is a partner with Foran Glennon Palandech Ponzi & Rudloff PC in Denver and represents creditors nationwide.

¹ 11 U.S.C. § 107(b)(1)-(2).

² 11 U.S.C. § 107(c)(1).

³ Fed. R. Bankr. P. 9037(a).

⁴ 11 U.S.C. § 363(b)(1).

State Law

Only a handful of states have some form of data-privacy legislation in effect, while several others have passed legislation that will go into effect in the coming years.⁵ The degree of protections and rights of individuals varies greatly by state. Of particular importance is whether the applicable data-privacy law provides individuals with a private right of action to recover damages resulting from a data breach or other statutory violation.

California's laws are currently the only laws that provide consumers with a private right of action to enforce data-privacy rights. The remaining states rely on the state's attorney general to enforce the laws on behalf of consumers.

California's Data-Privacy Laws

In 2018, California enacted the most stringent data-privacy standards through the California Consumer Privacy Act (CCPA).⁶ It gives consumers the right to know the types of data that a company retains about them and the rights to access and delete data. In addition, the CCPA allowed consumers to opt out of data-tracking and the sharing of information with third parties and affiliates.

The CCPA also created a limited private right of action for individuals to recover up to \$750 in damages in the event of a data breach that results in access to nonencrypted and nonredacted personal information. This is defined broadly to include names, addresses, numerical identifiers, personal characteristics that are protected under California or federal law, biometric information, and other data that could potentially identify a consumer or household.

In 2023, California solidified the privacy protections created under the CCPA through the California Privacy Rights Act (CPRA), which adds greater protections. The legislation gave consumers the right to correct inaccurate data and be informed of automated decision-making, and restricted the use of sensitive personal information. The CPRA expands the CCPA's private right of action to allow individuals to recover for damages associated with the breach of nonencrypted email addresses and passwords.

The CCPA and CPRA apply to any business that collects consumers' personal information, does business in California and meets any of the following criteria: (1) has gross revenues exceeding \$25 million; (2) buys, sells or shares the information of more than 100,000 consumers; or (3) derives 50 percent of its annual revenues from selling consumers' personal information. Therefore, regardless of whether an entity intentionally deals in consumer data, many national companies must comply with the CCPA and CPRA if doing business in California.

Other States' Data-Privacy Laws

Other states that have enacted data-privacy laws generally provide consumers with the right to access personal data collected and stored, the right to delete personal data, and the

right to opt out of certain uses of personal data (*e.g.*, targeted advertising). Like California, these states define a business as an entity that deals in the trade of personal information and operates within the state.⁷

Some of these states require businesses to provide notice of any data breach as expeditiously as possible, while others set deadlines of between 30 and 60 days.⁸ The greatest distinction between these states and California is that the enacted legislation does not provide consumers with a private right of action. Instead, the state's attorney general is given the authority to enforce these statutory consumer protections.

The Bankruptcy Code and Rules provide basic safeguards for the protection of personal information.

However, enforcement can prove difficult, because some statutes require the attorney general to provide the violator with notice of potential prosecution before any action has been taken. For example, Virginia's Consumer Data Protection Act provides that prior to enforcing the law, the attorney general must provide a data processor or controller with 30 days' notice of violations, and allow the processor or controller to cure the violations before initiating any action.⁹ Similarly, the Colorado Privacy Act requires the attorney general to provide 60 days' notice, during which a violator may cure the violation.¹⁰ Such provisions arguably limit the deterring effect of punishing violators of data-privacy laws.

Data Collection and Retention in Bankruptcy Cases

The most common reason to collect and retain personal data in bankruptcy cases is the claims process. The information in a proof of claim is fairly standard. In the bankruptcy context, a proof of claim "is a written statement setting forth a creditor's claim" that conforms substantially to the U.S. Court's official proof-of-claim form.¹¹ The official form, approved by the Judicial Conference, requires identification of the claimant, the claimant's noticing address, the basis of the claim, and any account numbers that the debtor may have used to identify a claimant.¹²

Many types of claims (*e.g.*, trade, vendor and professional services claims) do not require the collection and retention of personal data. However, other types of claims — such as claims for personal injury, work performed or personal loans — often do involve the collection of personal data.

5 California, Colorado, Connecticut, Utah and Virginia have laws in effect. Other states have signed legislation that will become effective in the future: Delaware (Jan. 1, 2025), Indiana (Jan. 1, 2026), Iowa (Jan. 1, 2025), Montana (Oct. 1, 2024), Oregon (July 1, 2024), Tennessee (July 1, 2025) and Texas (July 1, 2024). Andrew Folks, "U.S. State Privacy Legislation Tracker," Int'l Ass'n of Privacy Prof'ls (Nov. 17, 2023), available at iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws (unless otherwise specified, all links in this article were last visited on Nov. 27, 2023).

6 Cal. Civ. Code § 1798.100, *et seq.* (2018).

7 Colo. Rev. Stat. § 6-1-1304(1) (2023); Conn. Gen. Stat. § 42-516 (2023) (applying to entities that control or process data of 100,000 consumers, or 25,000 consumers and derive 25 percent of revenue from sale of personal data); Va. Code Ann. § 59.1-576 (2023) (applying to entities that control or process data of 100,000 consumers, or 25,000 consumers and derive 50 percent of revenue from sale of personal data).

8 Colo. Rev. Stat. § 6-1-716 (2023) (requiring 30 days' notice); Conn. Gen. Stat. § 36a-701b(b)(1) (2020) (requiring 60 days' notice).

9 Va. Code Ann. § 59.1-584 (2023).

10 Colo. Rev. Stat. § 6-1-1311 (2023).

11 Fed. R. Bankr. P. 3001(a).

12 Official Form 410.

For these types of claims, the methods of data protection provided by the Code and Rules are often sufficient.

For example, when an individual creditor files its proof of claim and supporting documentation, the individual will redact Social Security numbers, financial account numbers and birthdates. As is common in mega bankruptcy cases, it can be necessary to collect and store unredacted claims information to process and segregate claims by the appropriate claimant, verify claimant identity, and prevent the filing of fraudulent claims. The very type of information could link data to individuals and allow the identification of individuals.

Although the bankruptcy court is tasked with performing the functions of noticing, maintaining a docket and other administrative services, it “may utilize facilities or services, either on or off the court’s premises,” to provide such services.¹³ However, the “costs of such facilities or services” must be “paid for out of the assets of the estate.”¹⁴ As such, where a debtor seeks to utilize the services of an extra-judicial claims-management team, commonly referred to as claims agents, the debtor generally seeks court approval to retain the claims agent as a professional in the bankruptcy case pursuant to § 327, which requires that professionals must not hold any interests adverse to the debtor and must be disinterested in the case.

Role of Claims Agents in Bankruptcy Cases

The responsibilities of professionally employed claims agents may vary, but these generally include maintaining a registry of all creditors in a bankruptcy case, and processing and maintaining records of all proofs of claim.¹⁵ Bankruptcy Rule 5003(b) requires the clerk of court to “keep in a claims register a list of claims filed in a case when it appears that there will be a distribution to unsecured creditors.”¹⁶

Therefore, when employed as a professional in a bankruptcy proceeding, a claims agent may serve as the official registrar of all filed claims. This entails receiving, reviewing and processing all claims, as well as maintaining a traceable record of claim amendments and objections.

Application of State Privacy Laws to Claims Agents

While claims agents may perform the functions of the clerk of court by keeping the official register of claims filed in the case, claims agents differ in that are generally subject to state data-privacy laws.¹⁷ Despite generally being subject to state privacy laws, claims agents may be exempt when performing aspects of their duties that are required by federal, state and local law.¹⁸ For example, because a claims agent is required to keep the official register of claims, an individual does not have the right to delete personal information contained in the proof of claim available under many state laws.¹⁹ Likewise, an individual would not have the right to correct information contained in a proof of claim where the Code does not allow correction.²⁰

A claims agent is also required to notify individuals of any disclosure of unencrypted or unredacted personal data in the event of a security breach.²¹ This scenario came to fruition in August 2023, when Kroll Settlement Administration LLC was the victim of a security incident that jeopardized the personal information of bankruptcy claimants in the *BlockFi Inc.*, *FTX Trading Ltd.* and *Genesis Global Holdco LLC* bankruptcy cases. Although little information is known about the specific types of personal data accessed by an unauthorized third party, the breach was significant enough to trigger the obligation to notify affected the individuals of the event.²²

Conclusion

The Bankruptcy Code and Rules provide basic safeguards for the protection of personal information. However, when claims agents and other professionals are employed in a bankruptcy case and entrusted with claimant information, the gaps between federal privacy laws and the Code are filled by state privacy laws to varying degrees. **abi**

13 28 U.S.C. § 156(c).

14 *Id.*

15 28 U.S.C. § 156(c); Fed. R. Bankr. P. 5003(b).

16 Fed. R. Bankr. P. 5003(b).

17 Cal. Civ. Code § 1798.105(n)(1) (2023) (explaining that obligations of CCPA shall not apply to government agency).

18 Cal. Civ. Code § 1798.145(a)(1) (2023) (“The obligation imposed on businesses by this title shall not restrict a business’ ability to: (1) Comply with federal, state, or local laws.”).

19 Cal. Civ. Code § 1798.105(a) (2023) (“A consumer shall have the right to request that a business delete any personal information.”).

20 Cal. Civ. Code § 1798.106(a) (2023) (“A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information.”).

21 Cal. Civ. Code § 1798.82 (2023).

22 “Security Incident,” Kroll Settlement Admin. LLC (Aug. 25, 2023), available at kroll.com/en/about-us/news/security-incident.