PRIVACY ISSUES IN RESTRUCTURING

David Shonka

Matt Rotert

PRIVACY LAW is multidimensional and dynamic. In other words, it's complicated and it changes all the time. For that reason, many attorneys groan any time someone raises a privacy question, especially if other aspects of the pertinent legal landscape are already fraught with complexity. In the high-pressure environment of a bankruptcy, many lawyers simply get up and leave the table when privacy issues are raised.

But it doesn't have to be this way. Privacy law, especially where it conflicts with other rules and practices, should be top of mind for the debtor and acquiring companies. More to the point: they cannot be ignored or abandoned. The more you can be generally familiar with issues like these, the quicker you can raise your hand and get help from a privacy geek. Here are some sample issues:

Debtors Selling Consumer Information

It has long been the case under 11 U.S.C. § 363(b)(1) that companies pursuing Chapter 11 bankruptcy can sell assets, including consumer information, to finance debt repayment. Now more than ever, though, a company's own existing privacy policy may stand in the way.

Specifically, to comply with the California Consumer Privacy Act ("CCPA"), many organizations updated their privacy policies to state that they will not sell consumer data. Under § 363(b)(1), a privacy policy that limits the sale of personally identifiable information in the normal course of business may also limit the sale of such assets through bankruptcy. When a court finds that a debtor's existing privacy policy is at odds with the sale of data through bankruptcy, the court will ordinarily refer the matter to a court-appointed consumer privacy ombudsman to determine the privacy impact of the sale.

Under Chapter 11 § 332, the court-appointed consumer privacy ombudsman is tasked with evaluating:

> (1) the debtor's privacy policy; (2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court; (3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and (4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers.

This analysis will necessarily include an evaluation of non-bankruptcy law, including relevant privacy regulations at the federal level such as the Federal Trade Commission Act, the Children's Online Privacy Protection Act, and the Gramm-Leach-Bliley Act; state statutes such as the CCPA and the Illinois Biometric Privacy Act; and foreign laws such as the General Data Protection Regulation ("GDPR"). The ombudsman will then make a recommendation to the court, and the court will make the final determination as to what consumer data can be sold as an asset. While a necessary protection, the ombudsman's analysis takes precious time and may restrict the type of information available for sale. It may also place additional ongoing obligations on the acquiring company.

Additionally, even if there is no ombudsman, privacy regulators may assert an interest in bankruptcy assets and the potential sale of consumer data may draw additional objections from them. For example, while the court approved the sale of certain personally identifiable information in Radio Shack's 2015 restructuring plan, nearly 40 state attorneys general felt that too much data was included and objected to the sale, forcing mediation. As a result of the mediation, the debtor and acquiring company ultimately agreed to limit the personal data included in the sale as well as the scope of the acquiring company's continuing obligations. The potential for delay in the bankruptcy proceedings can be mitigated with the early involvement of privacy counsel.

The imposition of state-mandated practices can also provide the court with another context in which to assess a debtor's privacy policies. For example, if a state law allows a debtor to sell consumer data but also requires it to provide the consumer the right and opportunity to opt-out of the sales or to provide annual disclosures about those sales, then its failure to meet these requirements could call in to question the validity of its privacy policies. It is not clear at this time whether bankruptcy courts are willing to do this analysis before appointing an ombudsman; however, as state-based privacy statutes become more common place, it may be difficult for the court to eschew the analysis. In any circumstance, the proliferation of state laws is likely to lead to more frequent ombudsman appointments in the future. At the very least, these state-specific privacy protections will provide additional avenues for state attorneys general offices and affected consumers to challenge debtors' bankruptcy plans.

Further, while the overlapping complexities of applying varying privacy mandates to the sale of consumer data through bankruptcy may tempt the debtor and the bankruptcy court to apply vague, generalized privacy policies, the Federal Trade Commission's ("FTC") law enforcement authority allows it to prosecute companies that engage in privacy practices that it deems unfair or deceptive to consumers. And the FTC has shown its willingness to enforce these standards. Therefore, it remains important that privacy policies comply with all legal obligations and accurately reflect the company's actual practices. It is also critical to assess that policy before entering Chapter 11 bankruptcy.

Acquiring Consumer Information

A company that acquires consumer data sets or whole business entities that include personally identifiable information must act quickly to ensure privacy concerns are addressed. While many of these concerns should be addressed during due diligence, the Chapter 11 process may truncate or otherwise accelerate the timeframe and increase risk of exposure for the acquiring company. An acquiring company also must act quickly to confirm ongoing privacy compliance as well as manage risk associated with duplicated or overlapping data, and the risk of subjecting the business to the laws of states where it did not previously do business. Any acquired information must be carefully analyzed:

- First and foremost, if the acquired information is subject to privacy laws such as the CCPA or the GDPR, the acquiring company must confirm that its privacy practices comply with those laws.
- If there is overlap between existing data and the acquired data, its treatment of the duplicative data can be problematic—particularly if the acquired data is subject to additional restrictions—either in continuation of the debtor's privacy policy or as the result of court order risk mitigation.
- Additional complexities can also result from the acquisition of personal information that is subject to foreign laws, such as the GDPR, that limit the processing of such data. For example, even if maintaining a customer list to expedite future order processing is within the scope of the original data collection, it is possible, even probable, that using that same data to develop marketing profiles would not be within the scope of that collection.
- Where the personal information of data subjects in multiple jurisdictions are concerned, the acquiring company may not be able to treat all data equally, even when the collection is based on consent. For example, data subjects in California may opt-out of future sales of their information, EU data subjects may withdraw their consent and demand that it be corrected or deleted, and data subjects in South America or Asia may or may not have such rights, depending on the country in question.
- Finally, where personal information is subject to data localization laws in the jurisdiction where it was originally collected, there will be additional restrictions on the acquiring company's ability to review or move such information.

While many of these conversations should be part of any due diligence prior to the acquisition, the acquiring company will still need to undertake a full analysis after the transfer is complete rather than continue to rely on the

debtor's privacy program and analysis. This analysis must include a review of any prior data breach scenarios, the debtor company's response, and any ongoing notification requirements—particularly if an entire business group is being acquired, not just the affected data; otherwise, the acquisition may create additional exposure for the company. In particular, this should include a careful examination to identify any undiscovered or prior undisclosed data breaches that must be reported to the appropriate data protection authorities and/or impacted data subjects.

For additional information on this topic, please contact the authors **David Shonka** and **Matt Rotert**. For further details on Redgrave LLP's Restructuring Discovery services, please contact **Christine Payne** at cpayne@redgravellp.com or at 312-521-9904.

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*